Go to Contents

COUNTER TERRORISM POLICING
HEADQUARTERS

THE COUNTER-TERRORISM CASE OFFICER GUIDE

'One-Stop-Shop' for CTCOs & CTCO Supervisors

Abstract

This document is a guidance tool to assist CTCOs & CTCO Supervisors in the management of Subjects from receipt of the initial referral through all aspects of PREVENT Case Management (PCM).

This document highlights policy & best practice for CTCOs & Supervisors from across the PREVENT network.

Professional judgement by CTCOs & Supervisors will be needed to establish the best course of action with each unique Case, in line with their assessment of the Case as part of the National Decision Making Model.

This document should be read in conjunction with the latest version of CONTEST and the CTPHQ PREVENT Policy document.

CTPHQ - PREVENT

I&S

Go to Contents

Version Control

Protective Marking	OFFICIAL – SENSITIVE
Title	Counter-Terrorism Case Officer (CTCO) Guide
Summary / Purpose	Guidance for Police PREVENT Practitioners
Owner	CTPHQ PREVENT – National Co-ordinator's Office
Organisation	Counter Terrorism Policing HQ
Unit	CTPHQ-PREVENT
Contact Details	I&S
Version	3.5
Publish Date	25 / 08 / 2020
Review Date	Yearly from above date & after each official CTP-Prevent Policy update.
Author	Marek HUBERT
Approval	CTPHQ PREVENT – National Co-ordinator's Office

Version	Date	Changes / Description	Author
1.0 Draft	**01/06/2018**	In draft	Mark BEBBINGTON
2.0 Draft	**06/07/2019**	Complete re-draft & extension, with updates, corrections & additional guidance.	Marek HUBERT
2.1 Draft	**16/08/2019**	Feedback from CTPHQ, corrections & additional guidance.	Marek HUBERT
3.0 Draft	**21/04/2020**	Complete reformat & overhaul. PLP process added. Draft for network feedback.	Marek HUBERT
3.1 Draft	**15/06/2020**	OSCT PLP Panel feedback	Marek HUBERT
3.1 Draft	**22/06/2020**	SLT feedback, profiles & DPIA information.	Marek HUBERT
3.2 Draft	**10/07/2020**	Further SLT feedback.	Marek HUBERT
3.3 Draft	**30/07/2020**	Final checks before "CTCO Webinar" sessions & feedback	Marek HUBERT
3.4 Draft	**13/08/2020**	RPC Policy feedback	Marek HUBERT
3.5 Publish	**25/08/2020**	Foreword & hyperlinks inserted	Marek HUBERT

USING THIS DOCUMENT

This document should be used in conjunction with the CTP-PREVENT Policy and the Channel Policy.

Use the Contents page to select the topic heading that you wish to explore.

Left click on the heading to jump to the relevant section.

Topics are arranged in the order of how a case enters and moves through Prevent Case Management.

You can also use the "Find" function by entering the keyword that you are searching for.

To return to the Contents page, click on the "Go to Contents" link in the top right hand corner of every page.

Any words or sentences in this document that are blue and underlined are internet hyperlinks to further guidance outside of the document.

CONTENTS

1 FOREWORD 9
2 INTRODUCTION 10
3 STRATEGIC OBJECTIVES FOR CTP PREVENT 11
4 PREVENT CASE MANAGEMENT (PCM) 11
5 BASIC PCM PROCESS MAP 13
6 CTP PREVENT – OVERVIEW & PRINCIPLES 14
6.0.1 CTP PREVENT – Overview 14
6.0.2 CTP-PREVENT – Principles 14
6.0.3 CTP PREVENT – Specified Police Authorities 15
7 CTP PREVENT – ROLES & RESPONSIBILITIES 16
7.0.1 CTP PREVENT – CTCO Role in PCM 16
7.0.2 CTP PREVENT – CTCO Supervisor Role in PCM 20
7.0.3 CTP PREVENT – Further Role Considerations for CTCOs & CTCO Supervisors 22
8 PREVENT RELEVANCE – WHAT SHOULD POLICE LOOK FOR? 23
9 FULL PCM PROCESS MAP 27
10 PREVENT REFERRALS 28
10.0.1 PREVENT Referrals - How Information Enters PREVENT (Diagram) 28
10.0.2 PREVENT Referrals – CTCO Responsibilities 28
10.0.3 PREVENT Referrals - What IS a Referral? 28
10.0.4 PREVENT Referrals - What is NOT a Referral? 28
10.0.5 PREVENT Referrals – Processing Referrals 29
10.0.6 PREVENT Referrals – I&S 29
10.0.7 PREVENT Referrals – Other CTCO Actions 29
11 FIMU DE-CONFLICTION 31
11.0.1 FIMU De-confliction – Overview 31
11.0.2 FIMU De-confliction - PURSUE / RADO Assessment vs. PREVENT Assessment 31
11.0.3 FIMU De-confliction - Process Diagram 32
11.0.4 FIMU De-confliction – Process Explained 32
11.0.5 FIMU De-confliction – Handover to PREVENT CTCOs 32
11.0.6 FIMU De-confliction – Not Suitable For PREVENT / FIMU Retains the Case 33
12 PCMT – THE PREVENT CASE MANAGEMENT TRACKER 35
13 PGA – PREVENT GATEWAY ASSESSMENT ("INITIAL ASSESSMENT") 35
13.0.1 Completing a PGA – Timeframe 36
13.0.2 Completing a PGA - Contacting the Initial Referrer 36
13.0.3 Completing a PGA – Background Checks 36
13.0.4 Completing a PGA – Further Checks & Additional Biographical Information 37
13.0.5 Completing a PGA – Contacting / Visiting the Subject or Partners 38
13.0.6 Completing a PGA – Using the DIF 40
14 AFTER THE PGA 40
14.0.1 After the PGA – Overview 40

14.0.2 After the PGA – Outcomes on the PCMT (non-Dovetail) 40
14.0.3 After the PGA – Subject Deceased 41
14.0.4 After the PGA – CTCO Supervisor Responsibilities 41
15 INFORMATION GATHERING 43
16 S.36 DECISION 45
17 CHANNEL – DOVETAIL & NON-DOVETAIL 48
17.0.1 Entering Channel (non-Dovetail Flowchart) 48
17.0.2 Channel – CTCO General Information 48
17.0.3 Channel – CTCO Duties (Dovetail & Non-Dovetail) 49
17.0.4 Channel – CTCO Duties (Non-Dovetail) 50
17.0.5 Channel – CTCO Duties (Dovetail) 50
17.0.1 Channel – Exiting & Outcomes for the Programme 51
17.0.2 Channel – Police Withdrawing Subjects from the Programme 51
17.0.3 Channel – Completing the VAF 52
17.0.4 Channel – Sharing the DIF with Partners (Dovetail & Non-Dovetail) 52
18 PLP - POLICE-LED PARTNERSHIP & PANELS 54
18.0.1 PLP – Basic Flowchart 54
18.0.2 PLP - General Information 55
18.0.3 PLP – Entering Police-led Partnership 56
18.0.4 PLP Case Management – Prioritising Cases 57
18.0.5 PLP Panels – Terms of Reference (Expanded) 59
18.0.6 PLP – PLP Panel Detailed Guidance 60
18.0.7 PLP Panels – Case Management Plans (CMPs) 63
18.0.8 PLP Panels – Case Resolutions 64
19 DIF - THE DYNAMIC INVESTIGATION FRAMEWORK 66
19.0.1 DIF – Background 66
19.0.2 DIF – Overview 68
19.0.3 DIF – Making Assessments 69
19.0.4 DIF – Breaking It Down: What to Write 71
20 CMPs – CASE MANAGEMENT PLANS & INTERVENTIONS 75
20.0.1 CMPs - Overview 75
20.0.2 CMPs – Protective Factors (Potential Issues) 76
20.0.3 CMPs – Introducing Interventions 76
20.0.4 CMPs – Types of Interventions 77
20.0.5 CMPs - Interventions: General Goals 77
20.0.6 CMPs – Interventions: Individuals 78
20.0.7 CMPs – Interventions: Institutions 79
20.0.8 CMPs – Interventions: Ideologies 80
20.0.9 CMPs – The Problem Solving Approach 82
20.0.10 CMPs – Tactical Options for Interventions 82
21 CASE OUTCOMES, CLOSURES, TRANSFERS & REVIEWS 83
22 INTELLIGENCE CYCLE 85
ANNEX 1: COMPLETING THE DIF 87
SUMMARISING THE ISSUE 87

COMPLEX NEEDS & VULNERABILITIES 87
GRIEVANCE NARRATIVES 89
ENGAGEMENT FACTORS, INDICATORS & DRIVERS 89
IDEOLOGICAL CONCERNS 90
INDIVIDUALS, GROUPS & INSTITUTIONS OF CONCERN TO PREVENT 91
CAPABILITY TO OFFEND OR CAUSE HARM 91
INTENT TO COMMIT OFFENCES OR CAUSE HARM 93
OPPORTUNITY TO OFFEND OR CAUSE HARM 93
INTERNET & SOCIAL MEDIA "LEAKAGE" 94
SUSPICIOUS TRAVEL OR DESTINATIONS 94
PREMISES OF INTEREST OR CONCERN 95
ESCALATIONS, TRIGGERS & WARNING BEHAVIOURS 96
MOBILISATION, FINISHING OR "LAST RESORT" BEHAVIOURS 97
ANNEX 2: COMPLETING THE VAF 99
ANNEX 3: EXTREMISM – OVERVIEW FOR CTP PREVENT 101
Extremism – 2011 PREVENT Strategy 101
Extremism - Disrupt, Deter & Prosecute 102
Extremism – Offences & Unlawful Extremist Conduct 102
ANNEX 4: LEGISLATION RELEVANT TO PREVENT 104
TACT 2000 - Terrorism Act 104
CTSA 2015 – Counter Terrorism & Security Act 105
CTBS 2019 – Counter Terrorism & Border Security Act 108
TPIM 2011 – Terrorism Prevention & Investigation Measures Act 109
EQUALITY ACT 2010 109
ANNEX 5: INFORMATION SHARING WITH PARTNERS 111
Information Sharing - PREVENT Purposes 111
Information Sharing - Necessary & Proportionate 111
Information Sharing - Case Merits 111
Information Sharing – Consent 112
Information Sharing – Types of Personal Information 112
Information Sharing – What is "Power to Share?" 113
Information Sharing - Legislation & Guidance 113
Information Sharing - Gateways, Exemptions & Explicit Powers for Police 114
ANNEX 6: TRANSFERRING PREVENT CASES 118
ANNEX 7: DECISION MAKING 119
Decision Making – National Processes & Guidance Manuals 119
Decision Making – Authorised Professional Practice (Risk) 119
Decision Making – National Decision Model (PREVENT) 120
Decision Making – CTCO Supervisors 120
ANNEX 8: I&S 122
ANNEX 9: PREVENT & PUBLIC ORDER (ACTIVISM – TERRORISM THRESHOLDS) 123
ANNEX 10: UK MILITARY PERSONNEL & PREVENT 128
ANNEX 11: PROSECUTING RACIST & RELIGIOUS HATE CRIMES 131

Go to Contents

ANNEX 12: RADO ASSESSMENT OUTCOMES & PREVENT 139

4) ANNEX 13: GLOSSARY OF TERMS & CONTENTS 140

Baseline Beliefs & Behaviours 140
Capability 140
Data vs. Information vs. Intelligence in PREVENT 141
DDP – The Desistance & Disengagement Programme 142
Dynamic Investigation Framework 142
Engagement Factors & Indicators 143
Exposure to Extremism & Radicalisers 144
Extremism – CTP PREVENT Operational Guidance 145
Fixation & Fixated Behaviours 146
Force 147
Grievance Narratives 147
Freedom of Information (FOI), Subject Access & Media Requests 148
Hate 149
"Have Due Regard..." 150
Hostility 150
Ideology (relevant to PREVENT) 152
Immigration Enforcement 154
Individuals & Institutions (of Concern to PREVENT) 154
Intent (to Commit Offences) 156
Intervention Providers 156
Interventions 156
Investigations within Channel 157
Leakage 157
MAPPA – Multi-Agency Public Protection Arrangements 158
Mobilisation Behaviours, Signals & Activities 158
Mobilisation Identity 158
Opportunity (to Plan or Commit Offences) 159
Othering People – "In-Group" vs. "Out-Group" 159
Pathways Towards Terrorism 161
Prevention 161
PREVENT Subjects – Individuals, Institutions & Ideologies 161
Prisons 163
Probation & Youth Offending Services 163
Proscribed Organisations & Hate Groups 164
Protective Factors 164
Radicalisation 165
Reasonable Suspicion vs. Reasonable Belief 166
Referring to Alternative Forms of Support 167
Reviewing Closed Cases 167
Relevant Offences 168
Risk Within PCM 168
Risk Factors & Indicators 169
Safeguarding 169
Sensitive Cases 170

Go to Contents

Terrorism 170
Terrorism-Connected Offences 171
Transferring Cases 171
Triggers & Tipping Points 171
Unlawful Extremist Conduct 172
"Vulnerable to being drawn into terrorism..." 172
Vulnerabilities & Complex Needs 172
Vulnerability Support Hubs 173

1 FOREWORD

2020 saw the onset of a global COVID-19, which has changed the way we function as individuals and as a network. We were dynamic in our response to this, rapidly evolving early intervention and support in response to changing threats and risks. The UK terror threat is likely to remain high with the main threats to the UK continuing to come from Islamist (groups such as Daesh and Al-Qaeda), RW and LASIT terrorism.

We listen constantly to our own intelligence experts, academics, front-line practitioners and our growing CT Advisory Network to understand the changing face of terrorist propaganda, narratives and messaging. This continues to shape our understanding of how terrorist groups adapt their tactics: increasing online activity (digital technology is a feature of almost every investigation), and using narratives that exploit fear, anxiety, hate, grievances, and conspiracy theories.

The success of Prevent in tackling radicalisation lies in our ability to innovate, learn and improve how we respond to terrorism risks and vulnerabilities in an ever changing world. To maintain legitimacy, trust and confidence we must ensure our interventions are fair and consistent, robust but caring, and underpinned with evidence and skilled professional judgement. I am proud of the systematic and enthusiastic way we have responded to reviews and feedback. This has enabled us to improve the sharing of information, challenge and support Prevent partners and front-line policing to play an increased role, be more robust and consistent in the assessment of risk, and provide more structured support to families to enable them to better support loved ones.

The CTCO Guide is designed to support all specialist CTP-Prevent officers and staff to identify, assess and manage terrorism vulnerability and risk effectively. The guide is designed to be easy to navigate and is presented with a hyperlinked Index and Glossary. It endeavours to provide step-by-step guidance on practically every task that CTCOs and CTCO Supervisors are expected to undertake in the course of their duties, and includes details on where to find additional relevant information, including other useful documents available on CTnet.

This new guidance, along with training and support, is designed to help you perform your role to a high standard. CTPHQ colleagues have listened and responded to extensive feedback throughout a pilot phase and numerous changes have been made in response to feedback. Good guidance adds value when it is used consistently and continuously evolves. It is therefore vital, not only that everyone takes personal responsibility for developing the knowledge, skills and experience necessary to deliver the processes and activities outlined in the policy, but that you also feedback ideas and opportunities to make future improvements.

I am thankful to both the CTPHQ team who have developed this product and to all those working in vital front-line Prevent roles who have contributed.

Nik Adams

National Co-ordinator for CTP-Prevent
Counter Terrorism Policing Headquarters

2 INTRODUCTION

1) UK Policing has a specific requirement under of the **Counter Terrorism and Security Act (CTSA 2015)** to *"pay due regard to the need to prevent people from being drawn into terrorism"*[1]. The Police are required to identify and help manage the risks and vulnerabilities around Individuals, Institutions and Ideologies (or more specifically, extremist ideological expressions such as leafleting campaigns) identified as having a possible PREVENT-relevant concern. UK CT Policing delivers on this requirement through Regional and Force based **Counter Terrorism Case Officers** (**CTCOs**) who are responsible for managing and mitigating the PREVENT-relevant threats, risks and vulnerabilities of Subjects referred to them, generally far "upstream" of actual terrorism offending.

2) **PURPOSE OF THIS DOCUMENT**

   a) This document seeks to help ensure that all Cases within PCM are managed by CTCOs and Supervisors in a consistent manner across the entire UK CTP PREVENT network.

   b) It guides CTCOs & CTCO Supervisors through every step of their roles:

      i) Referrals, FIMUs & background checks,

      ii) The initial PREVENT Gateway Assessment process (first use of the DIF),

      iii) Ensuring consistency of language & improving inter-rater reliability,

      iv) To provide guidance on the risk and vulnerabilities relevant to PREVENT,

      v) Using CTP-PREVENT's bespoke risk & vulnerability assessment tool, the **Dynamic Investigation Framework**,

      vi) Developing **Case Management Plans** in the **Police-led Partnership** process and how the **Prevent Case Management Tracker** supports and enables this process.

3) **SCOPE OF THIS DOCUMENT**

   a) This document is intended primarily for CTP-PREVENT CTCOs and their Supervisors involved in the management of PREVENT Subjects. It will also prove useful to RPCs and other CTP-PREVENT officers and staff.

   b) Although this document builds upon the requirements set out in the CTP-PREVENT Policy, if there are any direct conflicts between this document and the policy document, the **policy document** should be taken as the authoritative source and the conflict should be raised as a matter of urgency with CTPHQ PREVENT.

[1] Counter Terrorism and Security Act (CTSA 2015), Part 5, Chapter 1, Section 26 (1).

3 STRATEGIC OBJECTIVES FOR CTP PREVENT

1) The CTCO Guide and the Policy it stands behind are key parts of delivering the strategic objectives for PREVENT policing: to safeguard and support those vulnerable to radicalisation and to stop them from becoming terrorism offenders or supporting terrorism offenders. This is achieved by:

   a) **Enabling our People:** Our success relies on the trust and confidence of every community. We will achieve this through our people, who are well led, well equipped, and well trained. We take pride in the service we provide, we value each other and we support our people to be the best they can be.

   b) **Identification:** We will work in partnership to better identify and refer those vulnerable to being drawn into terrorism, and those who pose a radicalisation risk to others. We will work with communities, local policing, CT policing, public sector, businesses and charities.

   c) **Safeguarding:** We will work collaboratively across policing and wider partnerships to safeguard people and divert those who are vulnerable to radicalisation or being drawn into any terrorism related offending.

   d) **Managing Risk:** We will use our unique skills and powers, together with internal and external partners wherever appropriate, to assess, manage and disrupt those individuals who pose a CT or extremism risk. This includes diverting or disrupting those who seek to radicalise the vulnerable.

   e) **Professionalism and Consistency:** This updated policy draws upon two years-worth of feedback from the PREVENT network in order to refine and improve the overarching CTP-PREVENT framework, providing a clear step-by-step process for staff and officers, and promoting a consistent approach to PREVENT work.

4 PREVENT CASE MANAGEMENT (PCM)

1) PREVENT Case Management, or PCM, is the catch-all term used in this document to describe all case management within Prevent, whether it is by Police or the Local Authority. We identify the core activities of PCM as follows:

   a) **PREVENT Referrals:** This is the initial receipt of a referral potentially suitable for PREVENT Case Management. It may arrive with PREVENT directly or via an Intelligence Management Unit (IMU). The policy details the requirement to record referrals on the PCMT at the earliest possible opportunity as well as the necessity for de-confliction and assessment of cases by IMUs before any activity is undertaken locally by CTCOs. This also covers issues such as case responsibility where a subject is active across multiple CTUs or CIUs.

   b) **PREVENT Gateway Assessment (PGA):** Or simply the "Gateway Assessment", this is the term given to the initial screening & triage phase that CTCOs must complete on all de-conflicted PREVENT referrals. Coming after FIMU de-confliction and drawing upon Policing databases, the Gateway Assessment is the first use of CTP PREVENT's dedicated threat, risk and vulnerability assessment tool, called the Dynamic Investigation Framework (DIF). Whereas PGA used to be the name of a separate assessment tool, now PGA is just the name of the step/phase.

   c) **The Intelligence Cycle:** Intelligence Management Units (IMUs) are the only part of the CTP Network that have the potential to see the whole intelligence picture. It is essential that intelligence obtained through PCM is passed back to a Fixed Intelligence Management Unit (FIMU) to allow for proper assessment of any risk/threat and identification of escalation of risk. It is also critical that Channel Panels and Chairs are fully cited on all intelligence held by Police that is necessary for them to be able to make effective decisions, alongside Police, regarding risk.

   d) **Channel Cases:** Channel is the Local Authority led, multi-agency PREVENT programme, designed to support and safeguard people who are at risk of being drawn into terrorism offending within the UK. It is the primary mechanism for managing and supporting individuals entering into Prevent, after FIMU de-confliction and the Gateway Assessment phase.

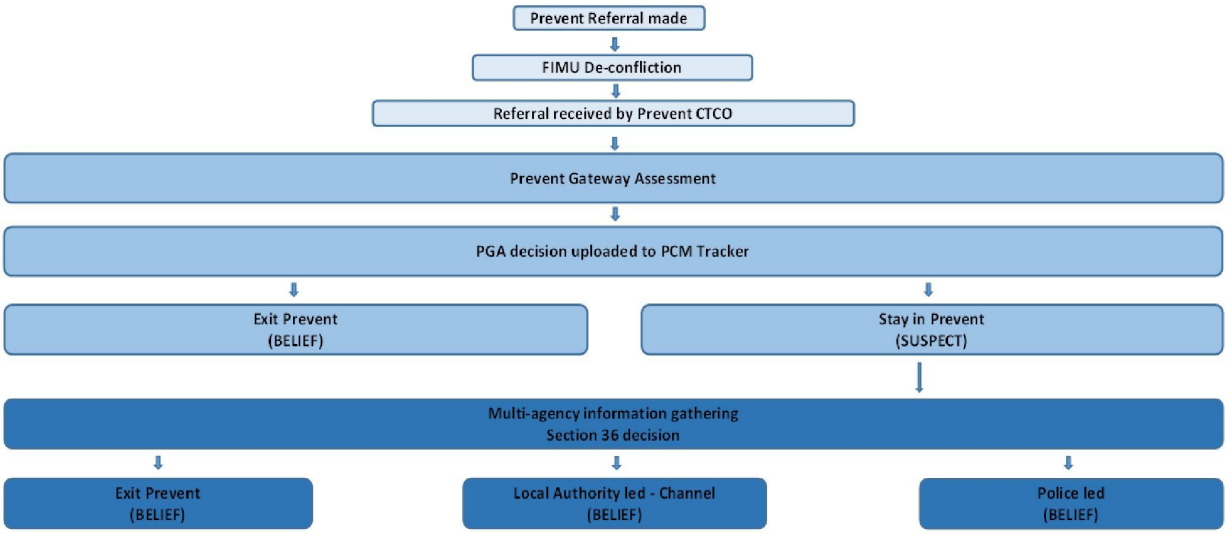
e) **Police-led Partnership Cases:** Led by Police but working in partnership with other agencies, the Police-led Partnership (PLP) process concerns the management of individuals, groups, institutions or ideological expressions that, although not suitable for Channel, still have identified Prevent-relevant issues that require support and/or mitigation. PLP was formerly known as just "Police Led".

f) **Outcomes, Case Closure and Case Transfer:** Decisions around case closures should be made solely upon the basis of the CT risk present, not simply whether interventions have been made or attempted.

g) **Supervision:** CTCO Supervisors have clear responsibilities at each stage of the PCM process, whether a case is managed within Channel or PLP. Proper supervision of Police activity is a golden thread that runs throughout the entire methodology.

Go to Contents

5 BASIC PCM PROCESS MAP



6 CTP PREVENT – OVERVIEW & PRINCIPLES

6.0.1 CTP PREVENT – Overview

1) The purpose of PREVENT is to safeguard and support vulnerable people within the UK in order to stop them from becoming involved in terrorism offending or supporting such offending. PREVENT work also extends to supporting the rehabilitation and disengagement of those already involved in terrorism. PREVENT works in similar ways to programmes designed to safeguard people from gangs, drug abuse, and sexual abuse, and indeed the "public health approach" to combatting violence. Success means an enhanced response to combat the activities of extremist groomers; tackle the causes of radicalisation, in communities and online; continued effective support to those who are vulnerable to radicalisation; and disengagement from terrorist activities by those already engaged in or supporters of terrorism.

2) The Police play a critical role in delivering PREVENT, developing local partnerships and bringing together a wide range of organisations in communities to support the local delivery of projects to protect individuals from radicalisation. The Police provide specialist support and capabilities to manage risk and disrupt those who are of interest to the authorities due to their extremist views, or who have links to those engaged in terrorism-related activity.

3) The **PREVENT Duty Guidance**[2] describes the following:

- **a)** For cases outside of Probation / MAPPA[3], Police will **always** have a responsibility to mitigate identified risks and threats around the breadth of terrorism offending, at least within the PREVENT pillar of CONTEST.
- **b)** Police hold information which can help assess "radicalising" behaviours and to disrupt people engaged in drawing others into the breadth of terrorism offending, violent and non-violent. The Police work alongside other sectors to play a galvanising role in developing local PREVENT Partnerships and bring together a wide range of other organisations to support local delivery of PREVENT. The Police are uniquely placed to tackle terrorism offending, and whilst it is acknowledged that the Police Service will designate dedicated PREVENT roles within Policing, a key objective for the Police is to ensure that PREVENT is embedded into all aspects of policing including patrol, neighbourhood and safeguarding functions. CTCOs and CTCO Supervisors are encouraged to help implement this.

6.0.2 CTP-PREVENT – Principles

1) Counter Terrorism Policing from PREVENT must ensure that PREVENT is embedded into all aspects of policing, including patrol, neighbourhood and safeguarding functions. Police officers often come into contact with vulnerable people in society, including those linked to counter-terrorism investigations, and are therefore well placed to identify those who are vulnerable to being drawn into terrorism and refer them on to appropriate support. The Police are also uniquely placed to engage and where appropriate disrupt radicalising activity, in partnership with other agencies, and using the full range of their powers and resources.

2) **CONTEST** is at the heart of everything PREVENT Police, every CTCO & CTCO Supervisor, do. The CONTEST strategy describes the three overarching objectives of PREVENT in the following terms[4]:

- **a)** Tackle the causes of radicalisation and respond to the ideological challenge of terrorism,
- **b)** Safeguard and support people most at risk of radicalisation through early intervention, identifying them and offering support,
- **c)** Enable those who have already engaged in low level terrorism offending, or those who have served custodial sentences for terrorism offences, to disengage and rehabilitate.

3) For our purposes in CTP PREVENT, we unpack the above key terms as follows:

- **a)** **Radicalisation:** refers to the process by which a person comes to defend, support, or take part in extremism or any offences under the breadth of UK terrorism legislation.

---

[2] PREVENT Duty Guidance, S.137 – 138.

[3] For cases within MAPPA for serious offending that is **not** terrorism related, these may still be eligible for PREVENT support if certain conditions are met. See the MAPPA entry in this document's glossary for further details.

[4] CONTEST, 2018, p.31.

b) **Terrorism:** for this we mean "terrorism offending", so any criminal offences under the breadth of UK terrorism legislation.

c) These terms and others are explored in more detail in the **Glossary Annex** of this document.

6.0.3 CTP PREVENT – Specified Police Authorities

1) The specified Police Authorities that are relevant to PREVENT, listed in Schedule 6 to the CTSA, are as follows:

a) Police forces in England and Wales.

b) Police and Crime Commissioners.

c) Civil Nuclear Police Authority.

d) The British Transport Police.

e) Port Police forces.

7 CTP PREVENT – ROLES & RESPONSIBILITIES

1) As per the PREVENT Duty Guidance, Channel Guidance and CTP PREVENT Guidance, in the fulfilment of their duties, CTCOs are expected to take action in the following areas, either directly or by linking in with other relevant authorities or policing units:

7.0.1 CTP PREVENT – CTCO Role in PCM

1) The wording of the following will be slightly different from that which appears in the Policy. This is not a contradiction. This chapter breaks apart and provides more granular detail on what is included in the Policy, it does not add anything that is no already stated in the Policy. Please also refer to the CTP PREVENT POLICY and the CHANNEL GUIDANCE in relation to "Channel Case Officers".
2) A Counter Terrorism Case Officer (CTCO) is a Police member of staff or warranted officer designated to enact the Police PREVENT statutory duty under the CTSA 2015. Police staff and officers performing the CTCO role will have comparable roles, with the key difference being the ability of an officer to utilise warranted powers where necessary. CTCOs, along with their CTCO Supervisors, are CTP leads for individuals, institutions and ideologies under management within Prevent, regardless of whether the case is managed as PLP or Channel. CTCOs have direct responsibility for the management of a cases under the PREVENT Case Management methodology detailed in this document. They are distinct from CTCO Supervisors and 2nd Line Managers. CTCOs may be referred to locally as PREVENT Officers, PREVENT Practitioners, Channel Officers, PREVENT Staff, Local Operations Officers or by another name entirely.
3) **Basic Requirements**
    a) **CTCOs will:**
        i) Be vetted to at least Security Clearance (Enhanced) (SC(e)).
        ii) Have current force led safety and first aid training (or equivalent) for staff and officers.
        iii) Have current access to the PCMT, CMIS & all required local force intelligence & crime systems.
        iv) Complete the National PREVENT Foundation Course (NPFC) as soon as practicable from starting role or complete online course, and attend any required refresher courses if already in post.
4) **Case Referrals**
    a) **CTCOs Must:**
        i) Create a PCMT record whenever a referral or potential referral is received.
        ii) Submit all referrals to (F)IMU for de-confliction and "PURSUE Assessment" before any dedicated "PREVENT Assessment".
5) **Gateway Assessments**
    a) **CTCOs will:**
        i) Upon receipt of a de-conflicted referral from a FIMU, conduct all required background checks and contact the referrer.
        ii) Find out whether the case subject is under investigation for any non-CT offences.
        iii) Use the DIF to complete the screening & triage of the PGA phase in order to identify any Individuals where there are reasonable grounds to suspect vulnerability to being drawn into any terrorism related activity. Such cases must then be marked to remain within PREVENT & forwarded into the Information Gathering phase for further development.
6) **Information Gathering**
    a) **CTCOs will:**
        i) Utilise and liaise with the **Vulnerability Support Hubs** (**VSH**) to assess vulnerability of referral Subject.
        ii) In **non-Dovetail** sites, request relevant information from the Local Authority / other Statutory Partners about the identified Individual.
        iii) Combine this information with the results of the PGA to generate a more developed assessment on the nature & extent of the identified Individual's vulnerability and risk.

iv) Use this more developed assessment to establish whether there is reason to believe a Case should be referred to a Channel Panel, placed within Police-led Partnership processes, or closed from PREVENT. This is the **Section 36 Decision** (**CTSA 2015**).

v) In **Dovetail** sites, both the Information Gathering & S.36 Decision is made by the Local Authority Channel Coordinator (LACC), **not** the Police.

7) Channel

a) CTCOs will:

i) See section **Channel – Dovetail & Non-Dovetail** for more detail.

ii) In **all Channel** sites, attend all Channel Panels and fulfil the Police role as statutory partner as CT Subject Matter Expert (SME), disclosing Police held intelligence necessary to make effective risk management decisions. CTCOs must take an **active** part in the Panels, advising & holding to account the Channel Chair in relation to all aspects of CT risk within the case management of the Panel, as presented within the Channel Duty Guidance and the CTSA 2015. Note that other, non-Prevent, Police **may** also be invited to attend as necessary and requested by the Channel Chair.

iii) In **Dovetail** sites, where the PGA phase presents a reasonable suspicion that an Individual may possess a Prevent-relevant vulnerability, provide all relevant information & intelligence to the Local Authority Channel Coordinator (LACC) to allow them to complete the VAF. See the section on Prevent-relevance in this document for details.

iv) In **non-Dovetail** sites, create & maintain the CMISv2 record, & record the S.36 CTSA 2015 referral justification on that system & the PCMT.

v) In **non-Dovetail** sites, complete the initial VAF after Information Gathering.

vi) In **all Channel** sites, attend every Channel Panel as a mandatory statutory partner, fulfilling the Police role articulated within the Channel Guidance.

vii) In **all Channel** sites, regularly update the Panel on the Case's potential risks in relation to **any** terrorism related activity (not solely extreme violence & murder), & ensure the Panel is fully cited on all intelligence held by Police that is necessary for them to be able to make effective decisions in relation to the case.

viii) In **all Channel** sites, risk assess deployments of Intervention Providers (IPs).

ix) In **all Channel** sites, actively monitor & identify if risk has escalated to the point where a case could be considered a potential IHM lead or Priority Operation, & refer them back to a FIMU for re-assessment. CTCOs must bear in mind that in most instances they are **the** experts present at all Channel Panels concerning the risks of escalation towards terrorism.

8) Police-led Partnerships:

a) CTCOs will:

i) See **Police-led Partnerships and PLP Panels** for more detail.

ii) Attend all Police-Led Partnership Panels (PLP Panels) meetings where their cases are being discussed.

iii) Create agendas for Panel meetings, as per directions from PLP Chairs, and compile all other documentation required to take a Case to each PLP Panel meeting. Disseminate any other appropriate information to relevant Partners.

iv) Advise PLP Chairs as to which Partners may be relevant and useful to the Case are present at the PLP Panel.

v) Take any findings or recommendations from the Vulnerability Support Hubs to the Panel meeting and refer any new concerning behaviours or circumstances back to the Hubs, as relevant.

vi) Decide on the priority banding of the case and develop CMPs, in conjunction with Partners (where relevant), and to be discussed at PLP Panels. Every case at Panel will require a CMP.

vii) Identify and engage approved Intervention Providers (IPs). Risk assess any deployment of IPs to a Subject, paying particular attention to who is best suited to enact each intervention in each context.

viii) Identify any potential travel risks and ensure that appropriate markers are placed on PIW, PNC and Local Intel Systems, as appropriate to the Case.

ix) Regularly use the DIF and apply feedback from the Panel (and VS Hubs) to re-assess vulnerabilities and risks posed by (and to) Subjects at regular intervals, or whenever there is a significant event in the Individual's life.

x) Throughout PCM, identifying if risk has escalated to the point where a case could be considered a potential IHM lead or Priority Operation and referring them to an IMU for re-assessment.

xi) Determine, along the CTCO Supervisors, the most suitable route for a Case should it no longer be suitable for the Police-led Partnership.

xii) Support Local Authority PREVENT co-ordinators, regional further and higher education co-ordinators, regional health PREVENT leads and regional NOMS PREVENT co-ordinators in carrying out their work.

9) Disruptive Activity:

a) CTCOs will:

i) Throughout the PCM process, disrupt extremism using problem solving approaches and activities to investigate and prosecute all ASB and offences by PREVENT Subjects, not just terrorism offending. Wherever necessary, this should be done in conjunction with safeguarding activities.

ii) Divert, deter, desist & where possible prosecute extremist "groomers", extremism-related offending & all other extremist activity by Individuals within the PLP process. To achieve this, officers should consider the full range of lawful & proportionate investigation, disruption & prosecution options available to them, paying due regard to the operational guidance on "extremism" provided in this CTCO Guide document..

iii) Work with partners to utilise their unique powers to divert, deter or desist extremists and other persons involved in extremist activities, including events which support or promote extremism.

iv) Compile evidence and build files to support the Local Authority to take safeguarding action, up to and including Wards of Court procedures.

v) Provide disruptive capacity to CT investigations and other PURSUE operations by completing tasks as directed as an overt response option.

vi) Officers should consider the full range of investigative and prosecution options when it comes to disrupting extremist material and activities. I&S

(1) I&S

(c) College of Policing: Menu of Tactics,

I&S

10) Outcomes and Closures

a) CTCOs will:

i) Ensure the correct closure code is recorded on the PCMT / CMIS.

ii) Ensure any flagging used during management (PIW, PNC, NCIA, and local systems) is removed.

iii) Ensure all policing activity has been accurately recorded on the PCMT / CMIS including the use of activity flags to show specific interventions.

iv) Ensure closure of cases only occurs when the identified case priorities around risk and vulnerabilities have been addressed and CT risk has been mitigated, or at least evidence that management options have been exhausted.

11) Partnership Working Outside of the Police

a) **CTCOs will:**

i) Support existing Intervention providers & help identify potential new ones.

ii) Provide to Local Authority Partners, where appropriate, details of the Police Counter Terrorism Local Profile (CTLP).

iii) Work with Partners to develop a common understanding of roles & responsibilities, thus empowering specified agencies & other Partners to fulfil their PREVENT Duty.

iv) Support PREVENT co-ordinators, regional further & higher education co-ordinators, regional health PREVENT leads & regional NOMS PREVENT co-ordinators in carrying out their work.

v) Wherever possible, support Partners with targeted engagement in order to help improve their processes and increase the quantity and quality of referrals into Prevent.

vi) Work with Partners within multi-agency boards driving the PREVENT program, (e.g. Contest boards, PREVENT boards, PREVENT steering groups).

12) **Partnership Working Within the Police Family**

a) **CTCOs will:**

i) Work with Police partners to assess and monitor community tensions particularly after executive actions and CT consequence management.

ii) Support CTP Partners outside of PREVENT in the management of their cases where they intersect with PREVENT policing.

iii) Provide support in the production of Counter-Terrorism Local Profiles (CTLP) and assist partners with action plan development and the delivery of objectives and activities outlined.

iv) Coordinate the delivery of Prevent (activities, awareness and training) with police staff and officers across the force or region (Prevent Champion / SPOC network, training etc.) to fulfil its obligations under the CTSA 2015.

v) Develop strategies to support PURSUE Operations, acting as a PREVENT subject matter expert and tactical advisor around wider PREVENT safeguarding issues for families and RSOIs.

vi) Deploy as a PREVENT Contact Officer at the time of executive action (where relevant training has been completed).

13) **Community Engagement**

a) **CTCOs will:**

i) Identify, engage and maintain relationships with key individuals, institutions and groups within the community to:

ii) Promote and support the delivery of PREVENT at a local and national level,

iii) Support community resilience building, to challenge extremist and terrorist ideologies,

iv) Invite carefully selected (and 'vetted') community members, where appropriate, to join Regional CT Advisory Groups (R-CTAG).

14) **Additional Training**

a) **CTCOs may require additional specialist skills or training. As such, they are encouraged to seek the following where possible:**

i) **PND.**

ii) **COSII.**

iii) **NCIA.**

iv) **Contact Officer.**

v) **Consequence Management.**

7.0.2 CTP PREVENT – CTCO Supervisor Role in PCM

1) CTCO Supervisors are any officer or member of Police staff who are in a supervisory rank and who have direct line management responsibility for CTCOs. Non-supervisory ranks (e.g. constable or lowest band Police staff) should never undertake the role of CTCO Supervisor. Acting and temporary ranks are acceptable, providing it has been officially sanctioned by the local force. Police-led Partnership Panels must be chaired by CTCO Supervisors, or a PREVENT officer of higher rank, as per the Police-led Partnership Panel Terms of Reference (details are contained within this document). Supervision is **MANDATORY** for all uses of the DIF (so for Gateway Assessments and during PLP cases), Closure Reports, any other mandatory assessments (inc. VAFs), Case Management Plans, PGA Decisions, S.36 Decisions and Closure Decisions associated with the Case. Updates to CMPs **MUST** be supervised, and these updates **MUST** be completed at least as frequently as the bare-minimum defined in the Policy Document (every 4 weeks for **High Priority** Cases, every 8 weeks for **Standard Priority** Cases). Although a CTCO Supervisor can transfer a Case to a different Region, this **MUST** be communicated and agreed with the destination Region beforehand.
2) **Basic Requirements.**
    a) **CTCO Supervisors will:**
        i) Be vetted to at least Security Clearance (Enhanced) (SC(e))
        ii) Complete the National Prevent Foundation Course (NPFC) as soon as practicable of starting role or complete online course (in development).
        iii) Have supervisory access to the PCMT and CMIS, an open source terminal (where possible) and NCIA (where possible).
        iv) Have current force-led officer safety and first aid training (or equivalent) for staff and officers (if working in a public facing role).
        v) Ensure that all members of the team have received the required training to effectively risk assess, manage cases and access appropriate systems.
3) **General Duties**
    a) **CTCO Supervisors will:**
        i) Support & manage CTCOs day-to-day.
        ii) Bear joint responsibility for CTCO decisions within PCM.
        iii) Supervise and quality check all CTCO PCM work & ensure its timely completion.
4) **PCM Basics**
    a) **CTCO Supervisors will:**
        i) Allocate all received referrals, ensuring that regular updates on all PCM action or decisions are recorded on the PCMT.
        ii) Supervise DIFs completed for PGAs, ensuring they are completed within 5 working days of receipt from FIMU.
        iii) Ensure all referrals received by CTCOs directly from Partners or members of the public are submitted to the FIMU for de-confliction and "Pursue Assessment" prior to any CTP-Prevent work commencing.
        iv) Supervise Gateway Decisions and their rationales, assess the suitability to close a case and apply the appropriate closure code from drop down boxes.
5) **Channel**
    a) **CTCO Supervisors will:**
        i) Supervise CTCO decisions around suitability for Local Authority led management and ensure the prompt referral such cases to Channel Coordinators (or non-Dovetail equivalents).
        ii) Ensure at least one CTCO attends each and every Channel Panel meeting as CT SME and fulfil the Police role as statutory partner, disclosing Police held intelligence necessary to make effective risk management decisions.
        iii) Risk assess deployment of Intervention Providers (IPs) to a Subject.

iv) Identify risk escalation in Channel cases with potential IHM lead or Priority Operation. Refer to FIMU for urgent assessment.

v) **Non-Dovetail:**

(1) Supervise rationale for S.36 for Local Authority led management of referral within 20 days of FIMU de-confliction.

(2) Supervise CTCOs completed VAFs.

vi) **Dovetail:**

(1) Ensure CTCO provides all relevant data / information / intelligence to LA Channel Coordinator (LACC) in a timely manner for their ongoing management of the case.

6) **Police-led Partnership:**

a) **CTCO Supervisors will:**

i) Quality assess and supervise every completed DIF.

ii) Ensure all paperwork is uploaded to the PCMT in a timely manner, including PLP Panel minutes and actions. This means either copying the relevant information into the relevant case notes (marking them clearly), or, once the facility to store documents on the PCMT has been added to the system, physically uploading the relevant documents into the relevant casefile for storage.

iii) Supervise rationales for S.36 Decisions leading to PLP management, within 20 working days of FIMU de-confliction.

iv) Ensure continual reassessment of cases throughout the PLP process, including:

(1) CTCOs assessment of Prevent relevant risks.

(2) Agree the priority banding for the case.

(3) Oversight & approval of PLP Case Management Plans (CMP).

v) Chair PLP Panels and ensure that:

(1) Findings and recommendations of VSH are considered

(2) Approved Intervention Providers are risk assessed before deployment

(a) Activities/interventions within the CMP are to reduce Prevent relevant risks and vulnerabilities, and to safeguard Subject.

7) **Disruptive Activity:**

a) **CTCO Supervisors will:**

i) Ensure appropriate disruptive activities are considered throughout the PCM process.

ii) Coordinate with Partners to utilise their unique powers to disrupt and deter persons believed to be extremists[5] or people who escalating towards extremism, including events which support or promote extremism.

iii) Ensure CTCOs capture evidence and build files to support the Local Authority to take safeguarding action, including Wards of Court.

iv) Support CTCOs to explore opportunities to investigate and prosecute individuals of interest for non-TACT offences to undermine their status/credibility and limit their activity.

v) Provide disruptive capacity to Pursue-led operations by completing tasks as directed as an overt response option.

8) **Outcomes and Closures**

a) **CTCO Supervisors will:**

i) Ensure the correct closure code is recorded on the PCMT / CMIS.

ii) Ensure any flagging used during management (PIW, PNC, NCIA, and local systems) is removed.

iii) Ensure all policing activity has been accurately recorded on the PCMT / CMIS including the use of activity flags to show specific interventions.

[5] As per the CTP-Prevent operational definition of "extremism" and "extremists" provided within the Glossary of this Guide.

iv) Ensure closure of cases only occurs when the identified case priorities around risk and vulnerabilities have been addressed and any risk has been appropriately mitigated, or at least evidence and justification that all management options have been exhausted.

9) Partnership Working Outside of the Police

a) CTCO Supervisors will:

i) Support existing Intervention Providers & help identify potential new ones.

ii) Provide to Local Authority Partners, where appropriate, details of the Police Counter Terrorism Local Profile (CTLP).

iii) Work with Partners to develop a common understanding of roles & responsibilities, thus empowering specified agencies & other Partners to fulfil their Prevent Duty.

iv) Support Prevent co-ordinators, regional further & higher education co-ordinators, regional health Prevent leads & regional NOMS Prevent co-ordinators in carrying out their work.

v) Wherever possible, support Partners with targeted engagement in order to help improve their processes and increase the quantity and quality of referrals into PREVENT.

vi) Work with Partners within multi-agency boards driving the Prevent program, (e.g. Contest boards, Prevent boards, Prevent steering groups).

10) Partnership Working Within the Police Family

a) CTCO Supervisors will:

i) Work with Police Partners to assess and monitor community tensions particularly after executive actions and CT consequence management.

ii) Support CTP Partners outside of Prevent in the management of their cases where they intersect with Prevent policing.

iii) Provide support in the production of Counter-Terrorism Local Profiles (CTLP) and assist Partners with action plan development and the delivery of objectives and activities outlined.

iv) Coordinate the delivery of Prevent (activities, awareness and training) with police staff and officers across the force or region (Prevent Champion / SPOC network, training etc.) to fulfil its obligations under the CTSA 2015.

v) Develop strategies to support CT Operations and act as a Prevent subject matter expert / tactical advisor.

vi) Deploy as a Prevent Contact Officer at the time of executive action (where relevant training has been completed).

11) Community Engagement

a) CTCO Supervisors should:

i) Identify, engage and maintain relationships with key individuals, institutions and groups within the community to:

ii) Promote and support the delivery of Prevent at a local and national level,

iii) Support community resilience building, to challenge extremist and terrorist ideologies,

iv) Invite carefully selected (and 'vetted') community members, where appropriate, to join Regional CT Advisory Groups (R-CTAG).

12) Additional Training

a) CTCO Supervisors are encouraged to seek the following additional training wherever possible:

i) PND.

ii) COSII.

iii) NCIA.

iv) CT / Prevent Contact Officer.

v) CT / Prevent Consequence Management.

7.0.3 CTP PREVENT – Further Role Considerations for CTCOs & CTCO Supervisors

1) Maintain the Intelligence Loop

a) **CTCOs & CTCO Supervisors:**

i) During the lifecycle of a Case, the "Golden Thread" of intelligence must be considered. There MUST be a continual regard to feeding back relevant intelligence to the FIMU, starting at de-confliction and continuing throughout the lifecycle of the Case.

ii) Monitor local policing for PREVENT-relevant issues.

iii) Identify all activities and incidents involving an Individual (e.g. missing person reports, crime allegations, etc.) and ensuring the relevance of all intelligence is assessed and submitted to an IMU where appropriate.

iv) Be careful to not openly identify Individuals on wider Police criminal systems just for being vulnerable within PREVENT, it is vital to **avoid vulnerable Individuals showing up on criminal background checks solely for being involved in PREVENT safeguarding**. If this cannot be achieved, **do not** put any overt flags around the Individual on PNC.

v) Ensure open source research is completed and I&S referrals are actioned where appropriate (see flow chart in I&S Annex).

vi) Monitor world and local events to maintain an awareness of potential CT issues, radicalisation "trends" and community impact.

2) **Community Engagement & Resilience**

a) **CTCOs & CTCO Supervisors should:**

i) Identify, engage and maintain relationships with key individuals, institutions and groups within the community to:

(1) Promote and support the delivery of PREVENT at a local and national level.

(2) Support their Local Authority and local Police PREVENT leads in developing PREVENT-related projects and action plans.

(3) Where relevant, supporting the Charity Commission with guidance to avoid money being inadvertently given to organisations which may endorse extremism or terrorism and enforcing legislation where fraud offences are identified.

(4) Identify relevant groups in the community & develop corporate understanding of their needs & vulnerabilities in accordance with CTLP and ERT prioritisations, developing Key Individual Networks to support PREVENT activity.

3) **Partner Liaison & Support**

a) **CTCOs & CTCO Supervisors will:**

i) **Intersect with Wider Safeguarding & Law Enforcement:** If any non-CT criminal or safeguarding concerns are identified, CTCOs have a duty to ensure that they are referred onward for suitable management by the most relevant agency **at the point** of closure from PREVENT and **before** relinquishing responsibility.

4) **Support PURSUE Investigations**

a) **CTCOs & CTCO Supervisors will:**

i) Help ensure that PREVENT considerations are fully embedded into counter-terrorism investigations within the PURSUE space.

5) **Delivery of Police Training**

a) **CTCOs & CTCO Supervisors will:**

i) The CTSA 2015 outlines that specified agencies should train their **own** staff in matters pertaining to their PREVENT Duty. Therefore CTP PREVENT is expected to provide training to local Police colleagues. PREVENT concerns and safeguarding awareness needs to be embedded in every type of operational policing, as is the Case with the safeguarding awareness around Child Abuse.

8 PREVENT RELEVANCE – WHAT SHOULD POLICE LOOK FOR?

1) This section looks at what contexts and behaviours we might consider relevant for PREVENT.

2) **What Should PREVENT Look For?**

   a) PREVENT legislation requires us to identify and manage (alongside our Statutory Partners) anyone who is "vulnerable to being drawn into terrorism". This means that PREVENT must consider Individuals who are "upstream" of **any** terrorism offending, as defined within the breadth of UK terrorism legislation. (see the legislation annex for more details)

   b) This includes a lot more than the murder and massacre of high visibility terrorist attacks. For example it includes:

      i) Obtaining information likely to be useful to terrorism, including terrorist material that is downloaded, viewed or streamed over the internet.

      ii) Inviting support for a proscribed organisation, including expressions of support that are **reckless** as to whether they will encourage others to support the organisation.

   c) So PREVENT must look to support and/or divert people who are vulnerable to being drawn towards these and **any other** terrorism connected offences contained within any UK terrorism legislation. Hence PREVENT must, by necessity, take a relatively broad and contextual view in terms of relevance.

3) **Consider PURSUE**

   a) If a Case appears to have PREVENT relevance, particularly if it may involve weapons, explosives or their precursors, attack planning or planning any other extremist violence, high level aggravated activism[6] or terrorism related activity, **always** ensure that you have updated the FIMU with this information and always record on the PCMT their response about why the case is **not** relevant for PURSUE.

4) **Importance of Context**

   a) PREVENT relevance can be very contextual. Specific behaviours that may be indicative of escalation towards terrorism offences in one Individual in one set of circumstances, may **not** be indicative of the same with another Individual in a similar circumstances. The following should be regarded as **guidance** and not a rigidly prescriptive account of PREVENT relevance. Professional judgement, CTCO Supervisory oversight and where relevant Vulnerability Support Hub input around the Subject, context and circumstances of any potential Case is required.

5) **"Extremism":**

   a) Anything sent to PREVENT must be considered with a critical eye and within its context. Consider:

      i) Vulnerable people who commit "lower level" non-violent terrorism offences, or offences where they are victims as well as offenders (people who are coerced or groomed, for instance), these may be relevant for PREVENT support in addition to any measures that may be necessary from a PURSUE perspective.

      ii) **Providing PURSUE does not want the case**, anyone who appears to fall within our operational guidance around "**extremist**" and "**extremism**"[7], or who has concerning personal connections with anyone fitting this description, may be relevant for PREVENT consideration (although they *may* be weeded out by FIMUs or at the PGA stage).

6) **PREVENT RELEVANCE:**

   a) The presence of any factor that appears within the DIF may designate PREVENT relevance.

   b) Consider the Subject's ideology, hostility, grievance narratives, extremist connections, and any concerning or fixated behaviours, as these are explored within the glossary of this document and the DIF.

   c) In the context of an Individual's exposure to or behaviours around extremism, consider:

      i) High Level Aggravated Activism.

      ii) Someone with previous membership or desired membership in a proscribed organisation or known "hate group".

      iii) Someone who appears to have a "fanatical" or an otherwise **concerning** obsession with extremists or extremism, as opposed to a fascination around legitimate academic study or a lawful hobby.

[6] See the Counter Terrorism Policing (CTP) Terminology and Thresholds Matrix Annex of this document.
[7] See the CTP-PREVENT operational definition of "extremism" provided in the Glossary of this document.

iv) Someone exposed in a **repeated** or **deeply personal** or **traumatic** manner to extremist Individuals, groups, institutions or activities, or has shown a repeated or strong desire to associate with any of these.

v) Someone engaging in a strongly sympathetic or supportive manner with extremism. This might include writing, re-posting or 'liking' extremist material online, or having concerning extremist friends or online / social media contacts.

vi) Someone planning travel to active warzones (not as part of legitimate armed forces or a recognised aid agency or for some other clear and lawful reason), where there is a **significant** likelihood of **direct** contact between the Individual & terrorists and/or proscribed organisations.

vii) Someone who commits or intentionally causes hate offences, or who uses explicitly dehumanising, demonising or threatening language towards someone due to the target's perceived "otherness", particularly around any protected characteristics, as per the **2010 Equality Act,** and certainly if there is an apparent political, racial, religious or other single-issue ideology dimension connected to this behaviour (like "InCel" inspired hatred towards women, etc.).

viii) Someone who seems to be obsessed with, or who has apparently fantasised about, committing murder or mass murders (like school-massacres, rampaging shooter attacks or similar).

- **(1)** This is particularly concerning if they have also made notes drawn up a "hit list" or diagrams of attack plans, even if on the face of it these lists seem sketchy or juvenile, and even if on the face of it the person concerned does not appear physically capable of acting on these lists / plans.
- **(2)** For PREVENT, what a Subject **believes** they are capable of is often just as relevant as what we **perceive** them to be physically capable of.

ix) Someone with **extremist tattoos** or who owns known extremist or proscribed organisation or "hate group" memorabilia, flags or icons, and particularly if this ownership seems furtive or secretive.

- **(1)** Consider flags / emblems of proscribed groups like Al-Muhajiroun (and derivatives), ISIL, National Action, Al-Qaeda, Boko Haram, Continuity IRA, Orange Volunteers, etc..
- **(2)** Consider flags / emblems of known (non-proscribed) "hate groups" or other high-concern groups, like the British Nationalist Party (BNP), English Defence League (EDL), English Democrats, National Front, Proud Boys, Generation Identity, Ku Klux Klan, Combat 18, Hizb ut-Tahrir, Third Reich or Swastika flags or memorabilia, etc..

x) Someone who owns **illegal** offensive weapons (like illegal firearms, explosives or some kinds of bladed weapons), or who tries to acquire any weapons illegally online. Consider the context and surrounding behaviours and attitudes:

- **(1)** What makes this PREVENT relevant as opposed to gangs policing or any other form of criminal behaviour or public safeguarding?
- **(2)** Is there an apparent political, racial, religious or other single-issue ideology connected to this weapon ownership?

xi) Someone who **carries** any sort of weapon **illegally**, even if the ownership of the weapon is legal in itself within the UK. This could be on the street, in an educational establishment or in any public space. Think about the context and surrounding this weapon carrying, as with point above (e.g.: is it gang related, other crime related or extremism related, etc.).

xii) Someone who intentionally seeks out or shares real 'beheading', murder or torture videos, particularly if they are also religious, political or racially / hate-based connected videos.

- **(1)** This can include other extremist, terrorist, or egregious and graphic (or "real") violent content, particularly if this material has not been produced by a lawful news-media outlet.

xiii) Someone with close family members or close friends who are SOIs[8] or under investigation for anything that would be an offence under **UK** terrorism legislation.

[8] Although this is a discussion to be had between any Contact Officers or Family Liaison Officers, the FIMU, the investigating PURSUE officer, PREVENT CTCO Supervisors and CTCOs.

(1) Note that this **may** not be as relevant if the family member concerned is estranged or some sort of distant third-cousin living thousands of miles away, although consider each circumstance and the surrounding attitudes on their own merits in their contexts.

xiv) Someone who downloads, without a lawful or reasonable explanation as to why:

(1) Unlawful material produced by proscribed organisations.

(2) 3D printing plans for firearms or other unlawful weapons alongside any other PREVENT-relevant concerns.

(3) Restricted material falling under UK terrorism legislation, e.g.: terrorist or guerrilla training manuals, bomb making manuals, the "Anarchist's Cookbook", etc..

(4) Other very concerning or illegal material, irrespective of whether it appears to have a connection in extremists or extremism, if the Subject is also exhibiting behaviours that seem concerning within a PREVENT context.

xiii) Potentially, depending upon the contexts, any activity of a **political**, **religious**, **racial**, or of another single-issue **ideological** nature, either individually or as a part of a group (or a movement or a cause), where the Subject committed:

(1) Deliberate hate offences,

(2) Violence related-offences,

(3) Stalking or harassment offences,

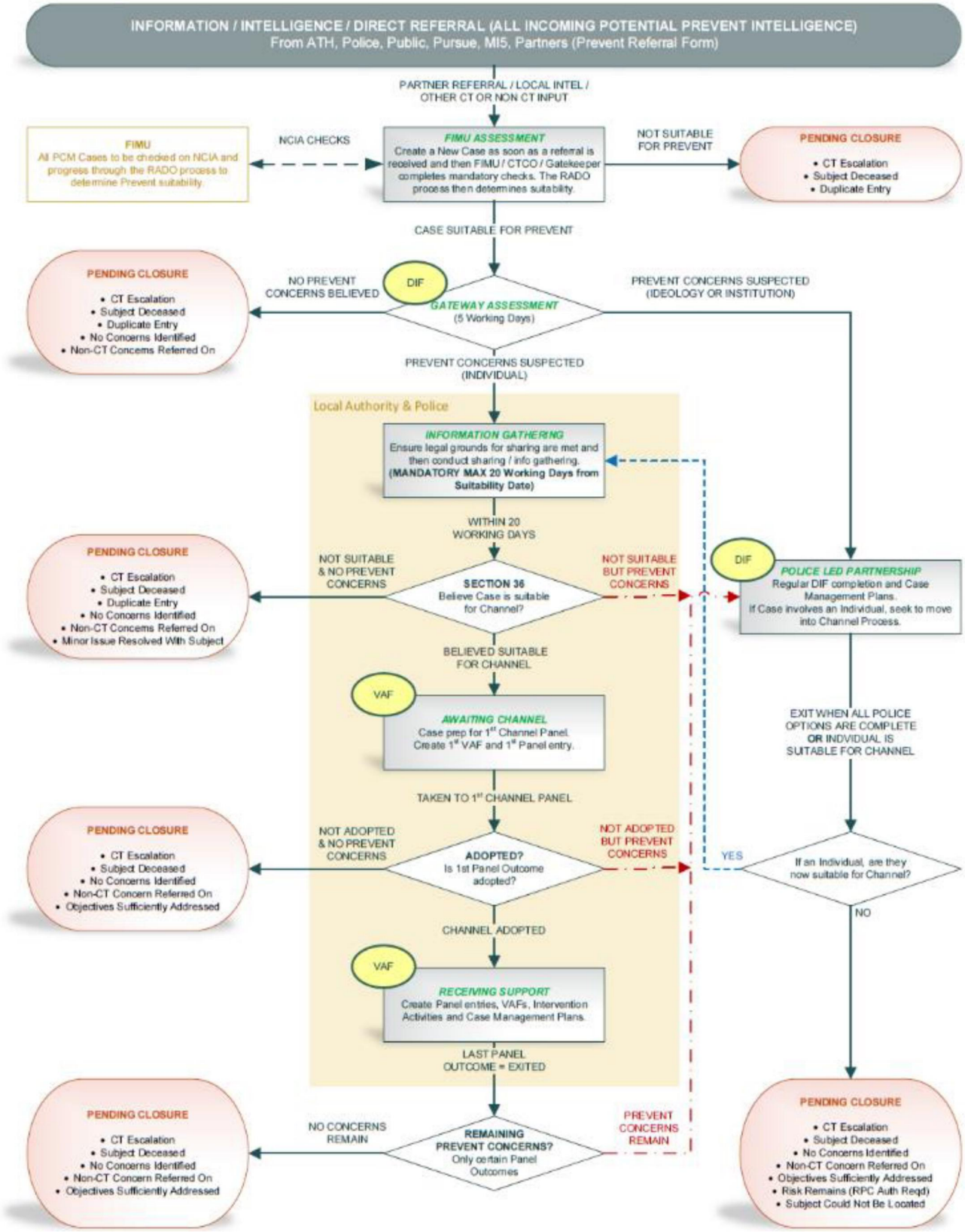
(4) Riot or Violent Disorder offences,

(5) Aggravated and/or serious and widespread criminal damage or arson.

7) ANY combination of the above factors and indicators should be considered very strongly as a potential PREVENT referral, *after* de-confliction with a FIMU to ascertain PURSUE relevance.

Go to Contents

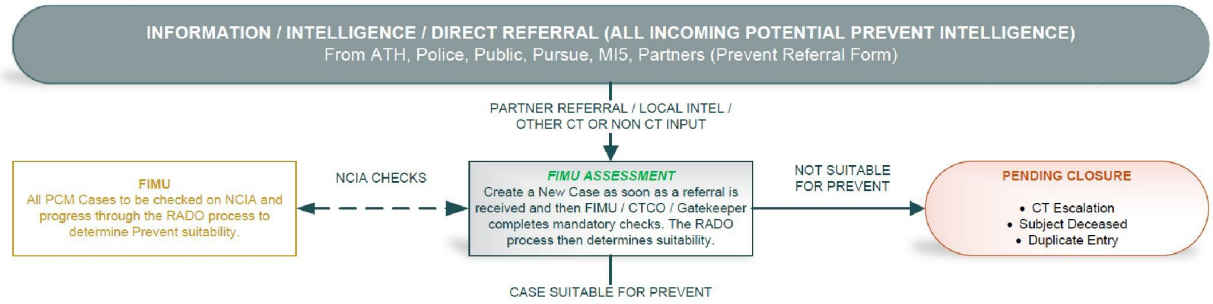
9 FULL PCM PROCESS MAP



10 PREVENT REFERRALS

1) In this section we look at how information enters into the PREVENT space, how it is assessed and how it is progressed.

10.0.1 PREVENT Referrals - How Information Enters PREVENT (Diagram)



10.0.2 PREVENT Referrals – CTCO Responsibilities

1) After de-confliction and the 'PURSUE / RADO Assessment' completed by the FIMU, CTCOs are required to log the referrals they receive on the digital **PREVENT Case Management Tracker** (PCMT).

2) CTCOs are then responsible for conducting the Gateway Assessments on **all** these referrals. Through this, CTCOs will determine (along with their CTCO Supervisors) whether the referral should:

- **a)** Be closed on the PCMT and the Subject exited from PREVENT.
- **b)** Be forwarded into the Information Gathering Phase.
- **c)** Be forwarded straight to a LACC (in Dovetail sites).
- **d)** Be forwarded straight into the PLP space (for Institutions, Ideologies or, in exceptionally rare circumstances, an potential SOI requested and approved by the FIMU / PURSUE, providing no active PURSUE investigation is going on around that SOI).

10.0.3 PREVENT Referrals - What IS a Referral?

1) For ease of use, we often call **any** concerns passed to CTCOs about a Subject a "PREVENT Referral".

- **a)** However, a "PREVENT Referral" is only formally classified as being such when an **Intelligence Management Unit** (**IMU**) – usually a **Fixed Intelligence Management Unit** (**FIMU**) has assessed intelligence using the **National Standards of Intelligence Management** (**NSIM**), and if applicable the **Intelligence Handling Model** (**IHM**), and has decided that a Case should be passed to PREVENT.

2) Prior to de-confliction, concerns sent to PREVENT can include any direct or indirect information or intelligence that indicates any possible PREVENT relevant concerns or vulnerabilities around an **Individual** or **Institution** (i.e.: the '**Subject**'). This information can come from any source where a concern has been raised that a Subject is:

- **a)** vulnerable to being drawn into terrorism related activities,
- **b)** is a risk of radicalisation,
- **c)** is engaged in radicalising others.

3) Any information suggesting any of these, prior to de-confliction, should be treated as a **potential** PREVENT referral and should be entered on the PCMT.

10.0.4 PREVENT Referrals - What is NOT a Referral?

1) Contact with CTCOs by Statutory Partners and the public is not automatically PREVENT referral.

2) As part of the **NOTICE**, **CHECK**, **SHARE**, process, a Partner or member of the public could call a CTCO to CHECK whether something they have identified really is an issue that should be referred to PREVENT. This is not automatically PREVENT referral and CTCOs are free to provide advice, using their professional judgement, around informal conversations of this sort. However, if a CTCO intends to advise that there is no concern to send to PREVENT formally, but there are **any** uncertainties at all, these must be discussed with a CTCO Supervisor before the advice is given **not** to refer a case to PREVENT.
3) **Everything** that arrives with PREVENT on a PREVENT Referral Form, and everything that is sent **in writing** to PREVENT from a statutory Partner or the Public – especially anything that is formally sent and/or is recorded by a Partner in their own systems as a PREVENT referral – **MUST** be recorded as a referral by CTCOs on the Tracker, and sent for de-confliction is it has not already been.

10.0.5 PREVENT Referrals – Processing Referrals

1) Referrals made directly to PREVENT that have not been through a FIMU, **must** be registered by CTCOs on the PCMT with the Subject's basic details **as soon as** they received, even if it hasn't been through the FIMU yet, (i.e.: open a 'skeleton' Case).
2) No further work should be completed on these 'skeleton Cases' until they have been de-conflicted by a FIMU.
3) If the referral has come straight to CTCOs on a **National Referral Form**, note that this is the basic document that you will use to record a new Case on the PCMT & it is a document that you can pass on to the FIMU.
4) In any referral, whether it is on a National Referral Form or not, there will need to be at least a basic summary of what the **"PREVENT Concerns"** are:
   a) These are the concerning issues themselves: the specific vulnerabilities around radicalisation and/or the risks of being drawn into terrorism offending that suggests a Subject may be suitable for support through PREVENT.
   b) Refer to the **PREVENT Relevance – Considerations** section above for the sorts of circumstances that might suggest a PREVENT Concern.
5) **A referral should have the:**
   a) Contact details for the referrer,
   b) Basic personal-identifying information of the Subject,
   c) A description of the potential PREVENT concerns and their contexts.

10.0.6 I&S

1) I&S

10.0.7 PREVENT Referrals – Other CTCO Actions

1) Relevant policing systems and email accounts should be checked regularly for incoming referrals or information / intelligence that could be deemed as being a potential referral.
2) The PCMT should be checked daily to see if there are new Cases awaiting allocation on the Dashboard.
3) Where a request is received from any part of the CT network for Police to manage (***manage*** being the key word here) any aspect of vulnerability or risk towards terrorism offending, then this should be treated as a referral and Subject to the same process. The only exceptions to this should be:
   a) Where it is clear from a JOT or similar that risk management is being undertaken by other parts of the CT network and Police have a clearly defined, usually singular, role to play or action to complete.

b) Where CTCOs receive a tasking package which includes a relevant risk assessment carried out by the instigating agency allowing them to own the risk assessment process on the CTCOs behalf.

4) If there is an identified piece of intelligence or a direct referral suggesting any kind of CT issue or vulnerability, checks should be made on the PCMT to determine if the Subject of the intelligence is already being managed.

5) The system will safeguard against creating a Case for an existing Subject by requiring a search to be carried out before providing a New Case option.

6) If a Subject is already being managed as an open Case on PCM, then the user assigned to the current open Case on the PCMT should be contacted and informed of this new piece of intelligence.

11 FIMU DE-CONFLICTION

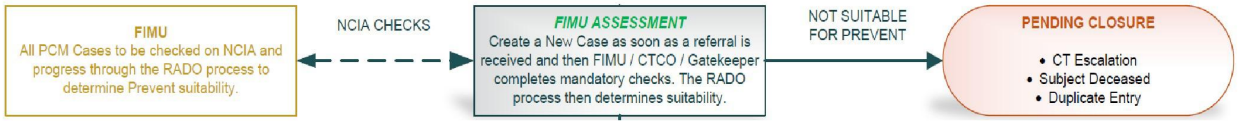
11.0.1 FIMU De-confliction – Overview

1) See NSIM Guidance for FIMUs.
2) **All** referrals **must** be assessed by a FIMU a RADO assessment, to check for "**PURSUE Relevance**" & to be **"de-conflicted".**
3) De-confliction checks whether the Subject of the referral is **already an active investigation** within the "PURSUE Space", & whether the Subject is in fact an active CT **Subject of Interest** (**SOI**) undergoing a PURSUE investigation.
4) The RADO assessment looks for **Counter Terrorism** (**CT**) relevance, predominantly from a PURSUE perspective, although they are required to give due consideration to PREVENT matters too. See the NSIM PREVENT Guidance for full details (particularly its Annex B).
5) FIMU assessments consider whether the referral has a CT concern that is **explicit, implied** or **inferred,** but not yet **mitigated**:
   a) **Explicit:** the referral states directly that a Subject is engaging, or is intending to engage, in activity of CT concern.
   b) **Implied:** although not stated directly, the content of the referral is strongly consistent with a Subject engaging in, or intending to engage in, activity of CT concern.
   c) **Inferred:** when it could be deduced from the referral reporting that a Subject is engaging, or is intending to engage in, activity of CT concern.

11.0.2 FIMU De-confliction - PURSUE / RADO Assessment vs. PREVENT Assessment

1) The FIMU de-confliction and assessment does not automatically replace the necessity of the CTCO's PREVENT initial assessment (the Gateway Assessment)**.**
2) Very generally speaking, the differences in the styles of assessment can be summarised with the following:
   a) **PURSUE / RADO Assessment =>**
      i) Completed by **FIMU**s.
      ii) Assigns **RADO Number (1-6)**.
      iii) "De-conflicts" the Case with ongoing CT investigations by other agencies / units.
      iv) Looks for leads & existing terrorism threats & risk factors closer to the PURSUE space.
      v) Looks for Subjects who are mobilising rapidly, or planning, attempting or committing any terrorism offences or terrorism-connected offences.
   b) **PREVENT Assessment =>**
      i) Completed by **CTCO**s through the screening & triage process we call the **PREVENT Gateway Assessment** (**PGA**).
      ii) Looks for vulnerability & risk factors "upstream" of PURSUE considerations.
      iii) Looks for initial "push" & "pull" indicators that may suggest Subjects are at risk of being drawn into terrorism offences, e.g.:
         (1) Concerning "signalling" behaviours,
         (2) Direct / indirect coercion of a Subject by extremists,
         (3) Early grooming or exploitation of a Subject by extremists,
         (4) Other forms of exposure or engagement that cause Subjects to defend, identify with, or become fixated upon, known extremists or terrorists, or extremist positions on any political, religious, racial or other ideological causes.

11.0.3 FIMU De-confliction - Process Diagram



11.0.4 FIMU De-confliction – Process Explained

1) CTCOs **cannot** use the DIF to commence a Gateway Assessment on a Case until **after** it has been de-conflicted through their FIMU. No PREVENT assessment work should be carried out until the result of de-confliction is known and logged.

2) Where FIMU de-confliction and assessment has not yet been completed, the Referral details **MUST** be submitted to the FIMU before proceeding.

3) Depending on local processes, this will either be by direct entry on the NCIA or via an Intelligence Log.

4) If entering directly onto the NCIA, CTCOs must be aware of the requirement to carry out the Mandatory NSIM Checks before registering the Intelligence Log.

5) Some regions may have CTCOs embedded within the FIMU, and it is these officers who commence the Gateway Assessments whilst the Case is still *technically* "with the FIMU". This is acceptable, but note that all Cases need to be de-conflicted with ongoing PURSUE investigations prior to PGA commencement and/or before the Case is forwarded out from a FIMU.

6) In situations where there is no specific **Individual** or **Institution** identified, advice should be sought from the FIMU to determine if there is any relevant information surrounding the Referral context (locality, leaflet / poster distribution, graffiti marks, etc.).

7) These Cases, which can be classified as **Ideologies** on the PCM TRACKER, still require processing through the FIMU as they may be linked to Individuals or Institutions of interest to PURSUE.

8) Where additional relevant information is received by CTCOs about a referral that is still with the FIMU, officers must make the FIMU aware of the new information as a matter of urgency.

11.0.5 FIMU De-confliction – Handover to PREVENT CTCOs

1) FIMUs will pass to CTP PREVENT any of the following:

- **a)** Cases that are assigned **RADO 5** or **RADO 6**, but where the cases are not obvious clerical errors or administrational mistakes, entered in error or duplicating existing cases.
- **b)** Any cases that arrive at the FIMU on a PREVENT referral form, or otherwise marked for PREVENT, and where the FIMU has not decided that the case should remain in the PURSUE space.
- **c)** Some cases at **RADO 4** (see RADO Annex for details) where there is **no PURSUE investigation** around the Subject and the FIMU is satisfied that the referral's information can be developed adequately by CTCOs through the Prevent Gateway Assessment. If the result of the CTCO's gateway assessment is that there is nothing that requires the case be re-escalated back to PURSUE, and the CTCO and Supervisor believe that the Subject's risk can be managed adequately by PREVENT, the RADO 4 Subject may be forwarded straight into the Police-led Partnership process.

2) The FIMU submission back to CTCOs should include:

- **a)** A list of all checks that have been carried out. Any official reference numbers that have been discovered pertaining to the Subject. For example:
  - **i)** PNC / PND,
  - **ii)** NCIA Entity,
  - **iii)** OIMU references,
  - **iv)** Crime Numbers for relevant offences, etc..

b) ***No Trace*** **at FIMU:**

i) Results of FIMU checks that indicate *No Trace* after the checks were carried out mean that there was no trace of the Subject, **not** no trace of PREVENT relevance.

ii) The CTCO will determine whether non-terrorism offences are relevant or not to PREVENT.

3) A de-confliction result from the FIMU should, wherever possible and practicable, include:

a) FIMU observations around the Case - although the final decision for whether the Case is relevant for PREVENT management lies solely with CTCOs and their CTCO Supervisors.

b) NCIA / NSPIS reference or Action Number.

c) Summary of any checks carried out and the result:

i) NCIA / NSPIS check results (Mandatory)

ii) PNC check results (Completed / Not Completed)

iii) PND check results (Completed / Not Completed)

iv) Local Crime and Intelligence System check results (Completed / Not Completed)

v) Open Source check results (Completed / Not Completed)

vi) CT Homes check results (Completed / Not Completed)

vii) CTP-NOC check results (Completed / Not Completed).

4) The above details **MUST** be logged on the PCMT in the Notes section. Any NCIA reference number returned should be entered in the de-confliction reference field. If the Case is suitable for PREVENT then the date of suitability should be completed. A Case can only move to Pending Closure until a Suitability Date has been entered. If a Case is deemed suitable for PREVENT but the FIMU has identified that the Case has a larger footprint in a different Force Area, then the Case may be transferred to that Force Area or Region. A discussion with a CTCO Supervisor in the destination Force Area **MUST** be carried out prior to transferring a Case. A Case should **NEVER** be closed just to re-open a new Case in the destination Force. The Case transfer functionality should be used by a CTCO Supervisor.

11.0.6 FIMU De-confliction – Not Suitable For PREVENT / FIMU Retains the Case

1) Where there is no conflict with an open PURSUE Investigation, or where the FIMU does not wish to retain the Case as a potential lead for PURSUE, FIMUs must **always** pass Cases to CTP PREVENT. This applies in particular where the referral was already marked as potentially relevant to PREVENT **prior** to being sent to the FIMU.

2) If a CTCO receives information from the FIMU that a Case already on the Tracker is not suitable for PREVENT, due to its relevance for PURSUE, then the Case should move to Pending Closure with an outcome of CT Escalation.

3) Due to the necessity of a sterile intelligence corridor between PURSUE and PREVENT investigations, FIMUs may not always be in a position to explain in great detail why a referral sent to them is being retained / not forwarded back to PREVENT. However, other than an administrational issue (like the referral being an identical duplicate of an existing one), the only reason a FIMU will not forward a case to PREVENT is if they assess that case as having direct PURSUE relevance.

4) If the referral was **entered in error** from the outset, this should be explained in the FIMU handover.

5) A brief summary of why the Case was not suitable must be added to the closure rationale on PCMT – bearing in mind that that not all information from the FIMU for this type of closure will be suitable for entering on an Official-Sensitive system and should be redacted as necessary. No suitability date should be entered.

6) If a decision has been taken to not refer a case back to CTP PREVENT but the case already exists on the PCMT (perhaps because it arrived with CTCOs prior to being sent for de-confliction), then the CTCO **MUST** ensure that all Case Details are fully completed. This should include:

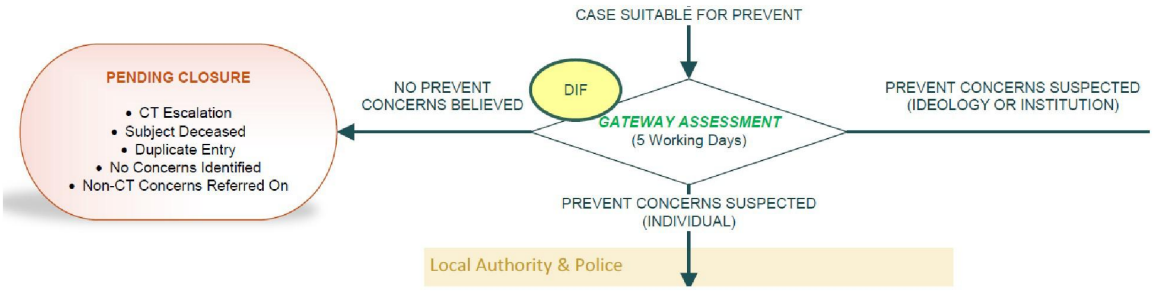
a) **Subject Bio-Data -** First & Last Name, Date of Birth, Addresses, Telephone Numbers, Additional Info and Social Media Information.

b) **Case Information -** Summary, Primary Influence, Primary Activity, ERT Theme, De-confliction Information (if any), Actions Closed and All Relevant Activities Are Selected.

12 PCMT – THE PREVENT CASE MANAGEMENT TRACKER

1) Please refer to the PCMT guidance document (available under the PREVENT tab on CTNet), and the in-programme help functions for detailed guidance.
2) The PCMT is a Prevent-specific web based case management application, accessible to all CTIUs and CTUs via their normal IT platform. Everything CTCOs do within the PGA, Information Gathering and PLP phases, including PLP Panels and any interventions, must be recorded within the digital PCMT. Although CMISv2 is the system used for the management and recording of case information within Channel, detailed around acceptance of a case into Channel, escalating risk and Channel outcomes must be recorded on the PCMT as well.
3) The security marking for the system is Official Sensitive, which means it is accessible via the PNN/PSN network and also works on work laptops and tablets, providing they are operating within PNN/PSN. As the platform is Official Sensitive any intelligence obtained that is Secret or above must not be recorded on PNN and instead recorded on the appropriate system as per local force guidance.
4) Use of the PCMT has been mandatory from July 2018. Plans are underway to combine CMIS with the PCMT, making the proposed new system the only system upon which PCM activities will be recorded and from which CTP PREVENT performance data will be collated. The PREVENT network and this Policy document will be updated as progress is made on the proposed combined system.
5) **IMPORTANT:**
   a) On creation of a case involving an Individual, leave the Priority field blank – this is only used for PLP cases.
   b) When using any element of the PCMT, if you do not know what to put in a field and cannot find out at the time of writing for whatever reason, leave it blank – **DO NOT** select other and enter Unknown, N/A or similar.

13 PGA – PREVENT GATEWAY ASSESSMENT ("INITIAL ASSESSMENT")



1) The **PREVENT Gateway Assessment** (**PGA**), or simply the "**gateway assessment**", is just the name given to the **initial screening** & **triage** phase that CTCOs must complete on **all** de-conflicted PREVENT referrals. It is the **first use** of our dedicated threat, risk & vulnerability assessment tool, the **Dynamic Investigation Framework** (**DIF**). The PGA step comes after FIMU de-confliction and draws upon Policing databases, hence it **must** happen before any further triaging or assessments by Local Authorities.
2) We used to refer to it as the **Police** Gateway Assessment. This was because at the time it was uncertain whether CTCOs would be handling MAC and DDP cases in addition to being PREVENT officers. Now it is clearer that the first Police assessment is the FIMU assessment, and the Gateway Assessment is purely for cases that are being forwarded to assess whether they are suitable for management within PCM – within PREVENT.
3) A referral should not continue within PREVENT if:
   a) It is clearly malicious or misguided;
   b) It is clear the person is not vulnerable to being radicalised or drawn into any terrorism related activity, or;

c) The person is already being managed through **Multi-Agency Public Protection Arrangements** (**MAPPA**) for a terrorism-related offences.[9]

4) Only **one** PGA, **one** Gateway Assessment, is ever completed in the lifetime of a single Case, **after** de-confliction**.** It must be completed even for cases where the FIMU has designated the referral as containing no CT relevance**.**

5) **Once uploaded to the PCMT, a Gateway Assessment is final. It cannot be altered or revisited.**

13.0.1 Completing a PGA – Timeframe

1) Gateway Assessments must be completed within **5 working days** of receipt from a FIMU, following de-confliction, or as close to 5 working days as is reasonably practicable within the unique circumstances of the Case. The PCMT starts a timer when a Case moves into Initial Assessment and will highlight expiry of the 5 day period on the Dashboard. CTCOs and CTCO Supervisors should be aware of Cases that have exceeded this **5 working day** period and update them accordingly.

13.0.2 Completing a PGA - Contacting the Initial Referrer

1) CTCOs should **always** endeavour contact the Initial Referrer and wherever possible also the last person or organisation that handled the referral prior to in arriving with CTP PREVENT, **before** the gateway DIF is finalised and the PGA Decision is made. The Initial referrer is the source of the information sent to CTP PREVENT, i.e.: person who first sent details of the Subject and the potential PREVENT concern. If (as with a school teacher on holiday) an initial referrer cannot be reached, then the CTCO should speak with the PREVENT point of contact (or head-teacher, etc.) wherever possible, or the last person who handled the referral before it arrived with CTP PREVENT. If there is no-one related to the referral whom the CTCO can speak to speak to. This contact allows CTCOs to build up a fuller picture of the Subject and their activities, and also to reassure the Initial Referrer that their concerns are being taken seriously and reviewed appropriately.

2) **CTCOs should:**

a) Check and confirm the details of the information originally sent by the referrer.

b) Ensure that full information from the referral is added to the referral page, including the original text and all contact details available.

c) Corroborate any matters that may need corroborating. Check claims about the Subject wherever possible, e.g.:

i) Is the initial concern valid for PREVENT or another agency?

ii) Did he/she really do what has been described, as described?

iii) Does Subject really have an MH condition, or is it just a suspicion?

d) Where possible, explore the context and wider circumstances of the concerns – find if there is anything relevant that the Initial Referrer may have missed first time around. CTCOs can draw inspiration from the DIF for any follow-up questions, although any such considerations and questions should be broached diplomatically and an eye on time constraints. Attempts / successes to fulfil these duties by CTCOs should also be recorded in the Notes section on the Tracker.

13.0.3 Completing a PGA – Background Checks

1) Background checks are not a separate process from the Gateway Assessment step. They feed directly into the completion of the DIF form for your Gateway Assessment. In order to complete a Gateway Assessment, CTCOs must complete background checks within local crime and intelligence systems for relevant information relating to the Subject. Many of these should hopefully be

[9] For cases within MAPPA for serious offending that do not fall under terrorism legislation, these may still be eligible for PREVENT support if certain conditions are met. See the MAPPA entry in this document's glossary for further details.

already answered for CTCOs in the initial referral, or in the FIMU handover, or through your contact with the Initial Referrer. All information gathered must be recorded on the PCMT in the notes.

2) To complete these checks, consideration should be given to use of the following systems:

a) **NSIM Mandatory:**

i) PNC.

ii) PND.

iii) NCIA.

iv) CT Holmes (where available).

v) Local Crime & Intel Systems – CTCOs must also be aware of any non-CT criminal investigations that are underway around a potential PREVENT Subject.

b) **Necessary for PREVENT:** where deemed necessary, proportionate and possible within the unique circumstances & timescales, the following need to be checked for relevancy and accuracy:

i) PCMT

ii) CTP-NOC.

iii) Open Source.

iv) Voters Register.

v) Missing Persons.

vi) Briefing Systems.

vii) Relevant Local Authority – this can be obtained from: https://www.gov.uk/find-local-council using the correct postcode.

viii) Check all biographical information for accuracy – first & last name, DoB, home addresses, telephone numbers, any social media information provided (do any accounts cited in the referral actually belong to the Subject?).

b) **Where possible, <u>try</u> to ascertain at PGA stage:**

i) Is the Subject aware of the current PREVENT Referral?

ii) Has the Subject been visited by Police for this or any previous PREVENT / CT matter? Include dates, reasons & outcomes (if known). Previous contact may influence intervention tactics & their success.

iii) Where the subject is a foreign national then consideration must be given to contacting the Foreign and Commonwealth Office (FCO), the Criminal Records Office (CRO) and Immigration Services to identify whether subject has any convictions abroad or whether other intelligence about activities outside the UK is held.

c) **IMPORTANT:** When using any element of the PCMT, if you do not know what to put in a field and cannot find out at the time of writing for whatever reason, leave it <u>blank</u> – **DO NOT** select other and enter Unknown, N/A or similar.

13.0.4 Completing a PGA – Further Checks & Additional Biographical Information

1) These are details that the FIMU and CTCOs may not already have ascertained, not been checked but which may be useful in order to assess vulnerability and risk, and also to help Partners complete their checks once they become involved. Some or all of these additional background checks can be completed **after** a PGA Decision has been made and uploaded onto the PCMT, specifically for Cases where the Decision is to keep them within PREVENT (either Local Authority led or Police-led Partnership).

2) These are **<u>not mandatory</u>** checks during the PGA phase, and in most cases a Gateway Assessment can be completed without them. However, they are checks that will be useful for the rest of the case, and will have to be completed during the Information Gathering phase if not already done so.

3) **Partners outside the Police (other than the initial referrer) should <u>not</u> be consulted prior to a PGA Decision to keep a Case within PREVENT for further information gathering.**

4) Sensitivity and due diligence are required whilst attempting to ascertain these details on a case-by-case basis:

a) Is the Subject 'On License'?

b) Immigration / Asylum Status?

c) Current & Previous Workplace?

d) Disabilities, Disorders or MH Issues?

e) Family Makeup / Who Lives with Subject?

f) Do they have a National Insurance Number?

g) Nationality / Country of Origin / UK Citizenship?

h) Current & Previous Educational Establishment(s)?

i) Where they are currently staying / residing (if different from their registered address)?

j) Wherever they are impactive upon the vulnerabilities and risks of the Case, what are the ideology, religion or politics of the Subject?

13.0.5 Completing a PGA – Contacting / Visiting the Subject or Partners

1) Overview:

a) Visits to Subjects **should not** be necessary in order to complete the PGA phase. Best practice is for gateway assessments to be completed and uploaded to the PCMT with a decision **prior** to any visit.

b) The PGA step is **not** a comprehensive, intrusive, "wrap-around" risk-assessment. It is a *screening* and *triage* – a "detailed snapshot" – to decide whether:

i) There is a **Reasonable SUSPICION** that a PREVENT issue is present (however minor), or,

ii) A **Reasonable BELIEF** that there is no PREVENT issue present at all.

c) Once CTCOs establish, (and can justify and explain) a reasonable suspicion that there is a PREVENT issue, they do not need to dig any deeper at the PGA stage, **if** the PGA Decision will be to keep the Case within PREVENT. A PGA Decision to close a Case from PREVENT completely requires a higher standard of justification – hence a **reasonable belief**.

2) Pre-FIMU De-confliction:

a) There should be no contact between CTCOs and the Subject of the referral prior to FIMU de-confliction and "PURSUE Assessment". This is notwithstanding any tasking from a FIMU to clarify specific information (such as necessary biographical information) during their de-confliction and Pursue Assessment processes.

3) After FIMU De-confliction, During the PGA Stage:

a) Contact with Individual Subjects or Partner agencies prior to the PGA Decision being made is not categorically 'prohibited' within the operational necessities of the case. However these Cases are an **exception** to the rule and must be in the minority, and cannot be treated as commonplace or 'routine' Case management activity.

b) If there is an exceptional operational necessity for a visit, CTCO Supervisors must provide written explanation and authorisation on the PCMT, in the Case's notes section.

c) The vast majority of Cases will not require Partnership engagement to complete the first DIF and make a PGA Decision. However if that a Partner holds vital relevant information to the initial screening and triage of the PGA but which cannot otherwise be obtained, early engagement **may** be permitted. In such cases, it must be discussed with CTCO Supervisors in advance, then the decision and rationale must be recorded by the Supervisor on PCMT prior to the contact. Again, this is only for exceptional circumstances and must not be viewed as routine.

4) Relevant Exceptional Circumstances:

a) It may be appropriate to contact or visit a Subject if there is a suspected immediate **risk to life or limb**, or another very **urgent and acute** safeguarding risk, or the Subject seems likely to be about to leave the country – although in these circumstances, consideration should first be given to whether the Subject needs to be referred with urgency out of PREVENT into another

unit or agency. If not, then it is still possible to make a PGA Decision to forward the case urgently into PCM (Channel or PLP) on the basis of a reasonable suspicion.

b) The CTCO and CTCO Supervisor may feel that there is really is not enough detail to make an assessment, but something in the referral raises their concerns that NOT contacting the Subject risks losing contact with the Subject completely. Where a travel risk is present then consideration should be given to placing the Subject on **PIW** (**Ports Intelligence Watch-list**) at the earliest opportunity. If a PIW is raised then the corresponding Action should be activated on the PCMT.

5) Visits:

a) If you are visiting a Subject due to a justifiable operational necessity, the first judgement CTCOs should make will be to draw upon basic Police safeguarding considerations, used for all other forms of ad hoc operational visits to potentially vulnerable members of the public. Before anything else, CTCOs should note the following:

i) Appearance: What can be observed immediately about the person and their demeanour prior any detailed conversation? Is there something about their appearance that is unusual or gives rise for concern? Do they look ill, injured, unsettled, anxious? Are they in distress? Do they possess any apparent disabilities? Do they appear injured or "out of sorts", e.g.: bleeding or bruising, do they appear under the influence of any intoxicating substances, etc.?

ii) Behaviour: Is there something about their behaviour that is unusual or gives rise for concern? What are they doing physically and is it in keeping with the situation? Is their behaviour excitable, irrational, manic, or it is slow and furtive? Do they appear to be suffering from a panic attack? What is their body language telling you? Are they displaying any subtle (or acute) signs of stress or fear, if so, is it towards you, someone else in the house or does it seem to be just in general?

iii) Communication & Mental Capacity: Is there something about the way that they communicate that is unusual or gives rise for concern? Is their speech slurred, slow or fast? Are the babbling or meandering aimlessly in what they are saying? Are their eyes glazed and dilated or large and staring? Do they understand what you are saying / asking?

iv) Danger: Are they taking a deliberately intimidating or aggressive posture towards you or anyone else present? Is there a risk of danger or any kind of harm to themselves, to anyone else in the vicinity, to someone not physically present with you, or to yourself?

v) Environment/ Circumstances: Is there something about the environment that is unusual or gives rise for concern? Is the premises / home in good order or chaotic? Are there any other people present who might be vulnerable (like children) or a risk to the Subject or yourselves? Are there any extremist signs or memorabilia in view? Are there weapons or drugs in view? Does anything at all give rise to concern?

6) A Strong Word of Caution:

a) Besides not being best professional practice, an early visit by "Counter Terrorism Police" may also deter particularly vulnerable or worried Subjects from engaging. If a Subject's PREVENT issue involves belief in conspiracy theories around the State or Police, an early visit by CT Police may serve to convince a Subject that they are indeed being "watched" and are right to be paranoid. In acute cases a visit might make the Subject a flight risk.

b) For **mistaken**, **misinformed** or **malicious** referrals to PREVENT, a visit from CT Police may be perceived as unnecessarily intrusive by the wrongly identified Subject.

c) If early contact is deemed absolutely vital, then our Partners in Local Authorities may have an existing relationship with the Subject or family, and may well provide a better means by which any additional required information can be obtained.

d) It is extremely bad practice to attempt to obtain consent for Channel prior to a PGA Decision being uploaded to the PCMT. Matters of consent should be discussed with Partners to identify which agency is best placed to make such an approach to an Individual and their family. This discussion may occur prior to, or even as part of, the first Channel Panel.

13.0.6 Completing a PGA – Using the DIF

1) Please refer to the "**Completing the DIF Form**" section of this document.

14 AFTER THE PGA

1) This section explores what happens immediately after CTCOs have completed their PGA.

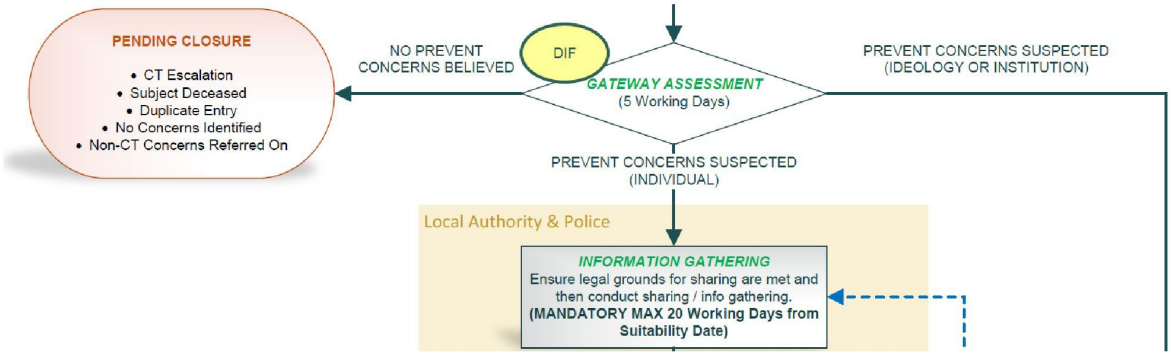
14.0.1 After the PGA – Overview

1) Other than the few cases that will go straight into the PLP process from the PGA phase, the majority of Cases involving Individuals that CTCOs have decided need PREVENT support, should be directed into the Information Gathering phase with the view of presenting them to a Channel Panel for adoption, if a reasonable belief of a PREVENT relevant vulnerability can be ascertained during Information Gathering. This applies in both Dovetail and non-Dovetail sites, except that in Dovetail sites it is the LACC who takes responsibility for multi-agency Information Gathering and making S.36 Decisions.

2) It is possible at the PGA Decision for CTCOs to suggest a final destination for cases staying within PREVENT (Channel or Police-led Partnerships), but any suggestions recorded onto the PCMT are not final until confirmed through the Information Gathering phase.

3) Where the CTCO and CTCO Supervisor cannot reach a decision to close a Case, perhaps due to lack of information, but where they suspect that there may well be PREVENT-relevant vulnerabilities and/or risks, then the case should still be moved into Information Gathering to develop the case, unless there are other indicators to suggest that this is not appropriate (the Subject is an SOI).

14.0.2 After the PGA – Outcomes on the PCMT (non-Dovetail)



1) The outcomes of a PGA are what the CTCO and CTCO Supervisor think the onward progression of the Case should be. Based upon all you have learned you will decide whether a Case should:

- **a)** Close & be exited from PREVENT:
  - **i)** CT Escalation,
  - **ii)** Duplicate Entry,
  - **iii)** Subject Deceased,
  - **iv)** No Concerns Identified,
  - **v)** Non-CT Concerns Referred On.
- **b)** Kept within PREVENT and forwarded straight into the PLP process – for Institutions & Ideologies.
- **c)** Kept within PREVENT and forwarded into the Information Gathering phase, building towards a S.36 decision (CTSA 2015).

d) **Non-CT Concern Referred On**: Note that a referring an Individual BACK to a school (for example) after a PGA, for the school to address what has been established through the gateway assessment as a non-CT concern, this still counts as a positive outcome.

14.0.3 After the PGA – Subject Deceased

1) It goes without saying that should anyone die whilst they are being assessed for PREVENT, or whilst they are within any element of PCM, the circumstances must be looked at by the CTCO and CTCO Supervisor. In the vast majority of cases, death whilst "in" PREVENT will likely be of natural causes or via accident, and will have no direct connection to PCM itself. That said, for **all** potentially suspicious deaths and suicides, the CTCO and Supervisor must consider, along with any relevant partners (Police and otherwise) whether involvement in PREVENT played any part in the death. People within PREVENT often have a cocktail of complex need and vulnerabilities, and they may have contacts or relationships with people who are coercive or actively dangerous. All these must be considered very carefully after any deaths.
2) The SOPs for deaths after Police contact may well apply for cases involving Police disruptive activities and similar non-Police procedures may well apply for deaths after contact with social workers or IPs as part of a Channel support package. Suffice to say these need to be explored by CTCOs and Supervisors in the first instance, and escalated through second Line Managers and up through appropriate channels to PREVENT policing leads in the relevant area, and their opposite numbers within the Local Authorities wherever necessary. Where a death appears to have a connection to any PREVENT activities, or where PREVENT is mentioned as potentially a causal factor by relations of the deceased (or the deceased in a suicide note), this should also be reported to CTPHQ-PREVENT as soon as possible.
3) Wherever possible within any restrictions imposed by the investigation, the contexts around any seemingly suspicious or self-inflicted deaths of PREVENT Subjects must be written up in detail by CTCOs and their Supervisors on the PCMT, and full co-operation must be provided to any other officers or agencies investigating the deaths. In any event, after the investigation has been completed the details should be recorded on the PCMT, or at least a case number, summary and location.

14.0.4 After the PGA – CTCO Supervisor Responsibilities

1) Once the Gateway Assessment is completed, it must be uploaded onto the PCMT with "PGA" selected from the appropriate drop-down menu. On the PCMT, cases should be moved from Initial Assessment at this point, and generally also at the expiration of the 5 working day period.
2) Cases can be closed directly after the Gateway Assessment if the CTCO believes that there are no PREVENT concerns. Cases pending closure status can only be managed by a CTCO Supervisor. A CTCO Supervisor should regularly check the Pending Closure queue to quality assure those Cases that have been submitted for closure by system users.
3) **Quality Assurance:**
   a) A CTCO Supervisor must open each Case in the **Pending Closure** queue to examine:
      i) **Case Details:**
         (1) Ensure that all the correct drop-down fields have been chosen.
         (2) Gateway Assessment completed – incl. mandatory background checks, contacting the Initial Referrer and/or the last person or organisation that handled the referral prior to in arriving with CTP PREVENT, etc..
      ii) **Case Notes:**
         (1) The most appropriate PGA Decision Closure Outcome has been suggested, along with supporting rationale.
         (2) To ensure that as fully as possible, all suitable activities and enquiries have taken place and have been recorded and (where necessary) justified sufficiently well.
      iii) **Case Actions:**
         (1) To ensure that all relevant Actions have been selected.

4) If the CTCO Supervisor agrees that the Case is ready for Closure, and is happy that all of the above details and activities are correct and have been completed with adequate diligence (in line with policy), the CTCO Supervisor will then select and appropriate status to move the Case on to as well as enter their rationale for the change of status. Refer to the PCMT Guidance for the closure process and Outcome Codes.

15 INFORMATION GATHERING

1) **Multi-Agency Information Gathering:**

   a) This is the stage that comes after a PGA Decision to keep a case within PCM. Police and Statutory Partners are involved to gather wider information relevant to the Individual and the Case, in order to decide whether there is **Reason to Believe** that the Individual is vulnerable to being drawn into terrorism related activity. Please refer to the Channel Guidance for additional information and examples around appropriate information sharing.

   b) **The DIF & More:** Information Gathering should be structured around exploring more of the DIF questions and further developing DIF questions that have already been answered during the PGA Phase. Also, this is the time to establish any other relevant background or biometric information that has not already been established during the PGA phase.

   c) **Dovetail:** In Dovetail sites, Information Gathering is completed by the Local Authority, the LACC, not the Police. However, CTCOs **must still** complete and provide Police-specific information relevant to this process. These are questions that only Police and they require answers either before the handover to the Local Authority, or during the Information Gathering phase. This includes reviewing Police crime and intelligence records, both national and local, and providing to the LACC any information that may be relevant to the concerns of Prevent, either directly or as aggravating factors to other issues. This includes tactics such as I&S or feedback from the **Vulnerability Support Hubs** – once a case has passed a PGA Decision to remain in PREVENT (Dovetail, non-Dovetail, Channel or PLP), open source checks and Police-specific elements of information gathering must still be completed in order to give a rounded picture of risk and vulnerability to any subsequent panels. The LACC may commence the first VAF at any time after receiving a referral from a CTCO after the PGA phase.

   d) **Non-Dovetail:** In non-Dovetail sites, once the DIF with the gateway decision to keep a case within PCM is uploaded to the PCMT, the Case *de facto* enters the Information Gathering phase. The Case remains the responsibility and ownership of Police throughout this process, right up until it is either closed from PREVENT altogether or accepted into Channel. The first use of the VAF occurs after a S.36 Decision has been made to refer the case to a Channel Panel and the Channel Chair has agreed to take the case to a Channel Panel. This first VAF should contain all the relevant information discovered through all uses of the DIF so far, from both the PGA and information gathering phases.

2) **Co-operation with Partners**

   a) In non-Dovetail sites, CTCOs may request Local Authority partners comprising Channel Panels to provide information about an Individual during the information gathering stage. In Dovetail sites it is the LACC who does this. It is considered good practice to draft a local data sharing agreement (DSA) to expedite the appropriate sharing of relevant and proportionate information. If a DSA is in place, as long as the request for information conforms to the stipulations of that DSA, little further legal justification should generally be needed. A template, for local adaptation is available on the CTNet.

   b) Section 38 of the Counter Terrorism & Security Act 2015 requires the partners listed in Schedule 7 (repeated in Annexes of this document) to co-operate with the Panel and the Police in providing any relevant information so that it can determine whether an Individual is vulnerable to being drawn into terrorism. Partners are expected to respond to the Channel Case Officer within five working days of receipt of any information requests.

3) **Information Sharing**

   a) The partners of a Panel cooperate with the Panel and the Police in carrying out their functions for Channel. The duty to cooperate extends as far as is compatible with the partners' legal responsibilities in respect of their functions; compliance with the duty does not automatically require or authorise the making of a disclosure that would contravene the Data Protection Act 2018 (DPA 2018) or the General Data Protection Regulation (GDPR). Further detail on information/data sharing is available in the Annexes to this document. It is important that local organisational information governance leads, and legal teams are consulted on the principles of information sharing within the Panel. Police are expected to also share all

relevant Police-held information wherever possible, and this must be provided whether or not it is requested by the Local Authority.

4) **GDPR:**

   a) The GDPR, DPA 2018 and human rights law are not barriers to justified information sharing, but instead provide a framework to ensure that personal information about individuals is shared properly. Under the GDPR and DPA 2018 information may be shared where there is a lawful basis to do so, such as for example when fulfilling a statutory function such as that set out in section 36 of the CTS&A 2015. A list of lawful bases for sharing can be found in the Annexes of this document.

5) **Requesting Information:**

   a) When you are requesting information from, or sharing information with, statutory partners, you should be clear of the basis upon which you are doing so, and the request should be stated clearly. When responding to a request to share information, you must ensure the grounds for doing so must be on which you might do so are legitimate and in accordance with the law (see the information sharing Annex for details). Further detail about GDPR and DPA 2018 in relation to information sharing can be found in the information sharing Annex. Information should only be used in line with for the purpose upon for which it was requested. You should consult your information governance officer and legal team for your organisation before sharing information. Information shared for the purposes of Channel may include special category personal data. When sharing special category personal data, you must identify a lawful basis under Article 9 supplementary to that under Article 6 GDPR.

6) **Consent:**

   a) Consent to share information is distinct from consent to receive support (Section 36, Part 5, CTSA 2015). These two issues should not be conflated nor treated as a single consent. Processing authorities must be aware of the individual rights of the data subject. Whilst consent is not necessarily required for information sharing, the data controller must take steps to ensure the subjects' individual rights are met. If a Panel Partner has any concerns about the appropriateness of sharing the requested information, they should consult with the CTCO, the Local Authority Channel Panel Chair, legal advisers and their own data policy officials to ensure all are satisfied that the information requested is lawful, proportionate and necessary.

7) **Panel Partners**:

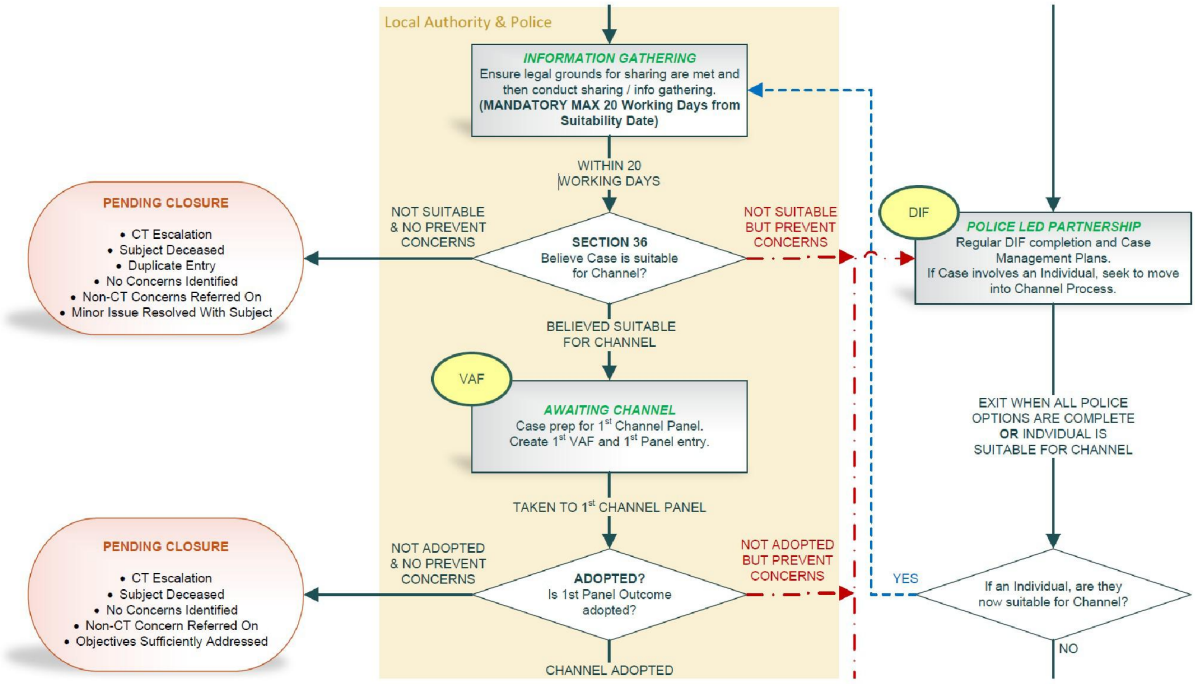
   a) If a statutory Partner provides information to the Channel Panel, or for a VAF assessment, it is likely that they will be invited to attend the meeting to discuss the case. Panel Partners invited to meetings should attend to ensure that the full range of an Individual's vulnerabilities can be discussed, and expert advice sought from attendees.

8) **Visiting the Subject:**

   a) Whilst it is not absolutely prohibited to make contact with a Subject **after** the PGA Decision during the Information Gathering phase, it should also be regarded as a rare exception, not the rule. See the next section for further details on contacting Subjects.

16 S.36 DECISION

1) This section explores what happens in after CTCOs have gathered information from Partners and need to decide what happens to the case going forward.



2) This is refers to decisions made under **Section 36** of the CTSA 2015, which legislates the process of identifying Individuals who there is reason to be believe are *"vulnerable to being drawn into terrorism"*[10], and therefore be suitable for PREVENT support, most notably Channel support.

3) The S.36 Decision is the culmination of the Information Gathering phase.

4) Police only make S.36 Decision in **non-Dovetail sites** on behalf of *"the Chief Officer of Police"*[11] in the CTCO's Force area, and only for Subjects that should not be referred directly from the PGA phase into the PLP process (Institutions and Ideologies).

5) After FIMU de-confliction, a S.36 Decision **must** be made for a referral within 20 working days.

6) **Overview:**

a) In a non-Dovetail site, after a PGA Decision that a Case involving an Individual is not suitable for Closure, the case should be forwarded into the **"Information Gathering Phase"**. This is a multi-agency process involving Statutory Partner agencies (Local Authority, Probation, Social Services, Health, Education, etc.), assisting Police in moving the Case forward towards a S.36 Decision.

7) **Section 36 Decision:**

a) In **non-Dovetail** sites, if after gathering and assessing relevant information through the information gathering phase, the CTCOs **Reasonable Suspicion** of the PREVENT vulnerability articulated in the PGA Decision has solidified into a **Reasonable Belief** of the same (and does not need to be escalated into PURSUE), then the CTCO & CTCO Supervisor must make a decision

[10] CTSA 2015, S.36, 1a.
[11] CTSA 2015, S.36 (3).

whether to refer the Case to a Channel Panel[12], or to close the case from PREVENT, or to forward the case into the PLP process.

b) Minor Issue Resolved with Subject:

i) If the Information Gathering phase has demonstrated to CTCOs and CTCO Supervisors that the Case can be closed from PREVENT within **20 working days from de-confliction**, then a visit to bottom-out the very minor issues **may** be appropriate. This, however, is a post-S.36 Decision action resulting in a closure outcome *"Minor Issue Resolved with Subject"*.

8) Cases Submitted to Channel (Dovetail Sites):

a) **Straight after making a PGA Decision** that there is a reasonable suspicion that an Individual has a Prevent-relevant issue, officers **must** refer Cases to the LACC, who will then commence the information gathering phase, the first VAF and make a S.36 Decision regarding the suitability to adopt the Case into Channel.

b) The LACC is expected to provide all relevant information gathered during information gathering to Police and Police must provide all relevant Police-specific information around the case, as well as providing advice and assistance on how best to proceed.

c) CTCOs must record the LACC's / Channel Panel's S.36 on the PCMT. Refer to the PCMT Guidance for the closure process and Outcome Codes.

9) Cases Submitted to Channel (non-Dovetail):

a) For Cases submitted towards Channel, they must be submitted to the Panel no later than 20 days after receipt of the de-conflicted referral from the FIMU into PREVENT.

b) There is no requirement to seek the Subject's permission (nor that of their parent/guardian or appropriate adult – if otherwise required) to share information with the Channel Panel / Channel Chair, as this is covered within the various legislative frameworks to share PREVENT safeguarding concerns (see the Information Sharing annex of this document for more detail). Consent is required from the Subject (or the parents / guardians / appropriate adults) only for the support package offered by the Channel Panel. Consent is not required to enter into Channel per se.

10) Case Ownership Prior to S.36:

a) In **non-Dovetail** areas, prior to a S.36 Decision and before acceptance into Channel, the Case ownership, management and risk still rests with the Police. Case management, ownership and direction is only transferred to the Local Authority if the S.36 Decision is to refer the Case to Channel and the Case has been accepted by a Channel Panel.

11) Contact with the Subject:

a) Whilst it is not absolutely prohibited to make contact with a Subject after the PGA Decision during the Information Gathering phase, it should also be regarded as a rare exception, not the rule. If there are operational reasons that require contact with the Subject after the PGA Decision but before Channel Panel acceptance, this remains a decision for the CTCO, although this also requires agreement and authorisation from the CTCO Supervisor.

b) Following a S.36 decision (though prior to the first Channel Panel meeting) consideration for contact with the Subject should be brought to attention of the CTCO Supervisor who may consider discussion with the Channel Chair. In this case the information disclosed and any decisions reached should be recorded and logged on CMIS as an extraordinary Channel Panel.

c) In either of these Cases, contact with the Subject must be expressly for the purpose of discovering vital information that can only be attained through direct contact with the Subject and which cannot therefore be ascertained through any other lawful and proportionate means.

d) Discussion with Subjects prior to Channel runs the risk of their refusal and therefore hindrance to future Partner engagement. At Channel Panels, Cases should be discussed and the Chair should agree an action plan to determine the best progression

[12] This is the default position for the majority of Cases involving Individuals within PCM

for the Case, including which is the best agency / sector to make the initial approach to Subjects to seek their consent for Channel interventions.

e) Any and all contact should be agreed in advance with CTCO Supervisors, planned and on the Tracker (or CMIS), with dates, times and reasons, and with the results recorded on the Tracker after each meeting.

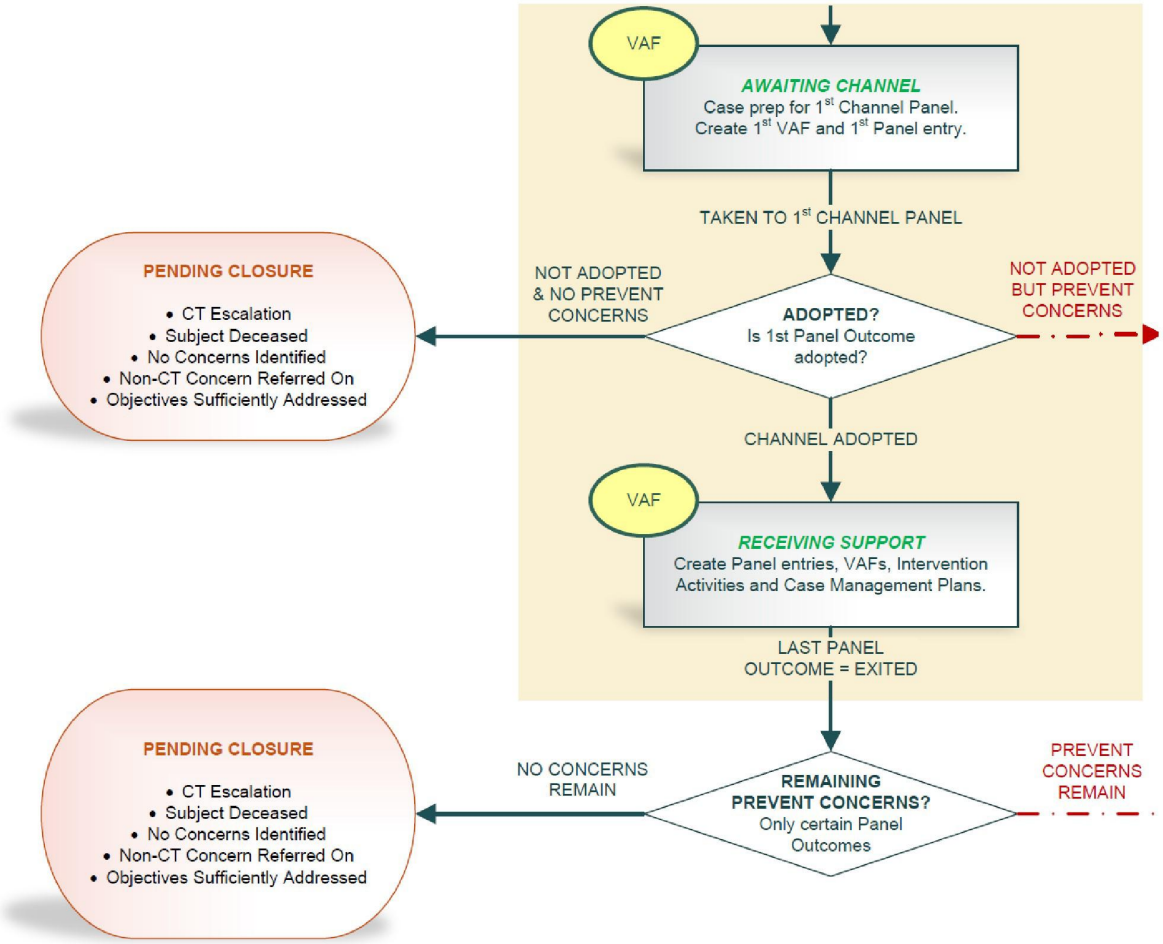
12) Closing the Case:

a) If a decision has been taken to close a Case for any of the outcomes listed in the Pending Closure bubble in the above diagram, then the CTCO **MUST** ensure that all Case Details are fully completed on the PCMT. Refer to the PCMT Guidance available on the CTnet for the closure process and Outcome Codes.

17 CHANNEL – DOVETAIL & NON-DOVETAIL

1) This section covers the progression of Cases into Channel. This section provides an overview of:
   a) The Channel Programme.
   b) Police duties in relation to Channel Panels.
   c) Using the PCMT in relation to Channel Panels.
2) Please refer to the Channel Guidance document for full details of CTCO duties.

17.0.1 Entering Channel (non-Dovetail Flowchart)



17.0.2 Channel – CTCO General Information

1) Channel is the **Local Authority** led, multi-agency PREVENT programme, designed to support and safeguard those who are at risk of being drawn into terrorism offences within the UK.
2) It is THE primary mechanism for managing and supporting Individuals entering into PREVENT, after a decision under S.36 of the Counter Terrorism and Security Act 2015.
3) CTCOs are responsible for:

a) In **non-Dovetail** sites, identifying Individuals that there are reasonable grounds to **believe** are *"vulnerable to being drawn into terrorism."*[13] This is the culmination of the Information Gathering phase and the S.36 Decision. Referring these Individuals to the Channel Panel *"for an assessment"*[14] on behalf of *"the Chief Officer of Police"*[15] in the CTCO's Force area.

b) In **Dovetail** sites, identifying Individuals that there are reasonable grounds to **suspect** are *"vulnerable to being drawn into terrorism"* during the PGA phase, then pass these cases straight to the Dovetail-site LACC, who will make the S.36 Decision

c) Representing the CTP PREVENT at every Channel Panel[16] and for updating the Panel on the Subject's risk of terrorism offending (which remains with the Police) and any other relevant intelligence / policing issue affecting the Subject that can be shared with Partners.

4) Irrespective of whether the Panel is in a Dovetail area, CTCOs should:

a) Advise and encourage the Channel Chair to include at the Panel of any Partners that the CTCO / CTCO Supervisor believes beneficial to the Case. CTCOs / CTCO Supervisors may want them to consider the value of having local / frontline policing "PREVENT champions" as standing members to add local context and provide local support and tactical options. Except for permanent members (like CTP PREVENT), the final decision about who sits around the Channel Panel rests with the Channel Chair.

b) Ensure VAFs have been completed competently and regularly, ensuring vulnerabilities and risks towards terrorism offending are being regularly assessed and managed sufficiently.

c) Ensure relevant "watch-lists" have been considered where applicable.

d) Ensure any Police disruptions agreed in Channel case management plans are completed.

e) Ensure that relevant information regarding the Individual's changing vulnerability and risk is captured and turned into intelligence products to be fed back into the FIMU every 3 months as a minimum.

f) Ensure the prompt assessment and submission of all other relevant information that may arise between times.

17.0.3 Channel – CTCO Duties (Dovetail & Non-Dovetail)

1) Where a Subject resides (or is believed to reside) in one of the Local Authorities of England and Wales, a CTCO will have responsibility to carry out the following:

a) Manage the receipt of PREVENT information and referrals from the public, Statutory Partners and FIMUs, record them on the PCMT, ensuring biographical details are obtained,

b) CTCOs must ensure that referrals from Partners and the public that have **not** been de-conflicted & PURSUE Assessed are passed to a FIMU for these to be completed.

c) Update the PCMT on return of any referral to CTCOs from FIMU de-confliction.

d) Respond to the referral originators wherever possible to acknowledge receipt and gain further information.

e) If they have not been included in the handover from the FIMU, and cannot be subsequently found out from the FIMU, CTCOs should conduct background checks on the Subject using policing systems, identifying any relevant activities and incidents involving a Subject (e.g. missing person reports, crime allegations, etc.).

f) Screen and triage threat, risk and vulnerability at the PGA stage by using the **Dynamic Investigation Framework** (**DIF**), ensuring that the PCMT is updated.

g) Ensure all relevant intelligence obtained through any triage, assessment or management process within PREVENT is fed back into the FIMU.

h) Identify any potential travel risks and ensure that appropriate markers are placed on PIW, PNC and Local Intel Systems.

---

[13] CTSA S.36 (1 & 3).
[14] CTSA S.36 (2).
[15] CTSA S.36 (3).
[16] CTSA S.37 (1b)

2) As a key Statutory Partner of PREVENT, CTCOs must attend **every** Channel Panel, irrespective of whether it is a Dovetail or non-Dovetail Case.

3) Wherever appropriate, the preference and goal for CTCOs is to be able to progress all Subjects who are suitable for Channel into that programme. This can be straight after the PGA Decision and subsequent S.36 Decision, or at any point during the Police-led Partnership space where the reviewing CTCO and CTCO Supervisor believe:

   a) The risks that prompted the CTCO to direct the Subject into PLP has decreased sufficiently, **but** the Subject still requires further PREVENT support, or,

   b) A PREVENT Subject who was always suitable for Channel but previously refused to engage, now wishes to engage with that voluntary programme

4) Through the Chair, the CTCO should ensure that wider family support is considered, e.g.: the family may need support to help cope with the complex needs of the Individual within PCM, and where the family is assessed as being protective and supportive of the Individual, CTCOs must ensure that updates and outcomes are given wherever appropriate and whilst maintaining confidentiality (i.e.: between the Subject and IPs).

17.0.4 Channel – CTCO Duties (Non-Dovetail)

1) **In non-Dovetail sites CTCOs will:**

   a) Carry out Information Gathering, record those activities on the PCMT, and also record any other relevant matters on the PCMT.

   b) Determine if there is **Reason to Believe** that the Subject is vulnerable to radicalisation (i.e.: as per the **CTSA, S.36 (3),** the Individual is *"vulnerable to being drawn into terrorism"*), and if so, refer the Case to a Channel Panel.

   c) For Cases accepted onto Channel, CTCOs will manage these day-to-day on CMIS.

   d) Visit Individuals in Channel (alongside relevant Partners and IPs) and risk assess them using professional judgement and the **VAF**.

   e) Manage the Case through the Channel Programme:

      i) Creating agendas, in conjunction with the Channel Chair, for Channel Panel meetings.

      ii) Organise Intervention Providers and the Intervention Sessions.

      iii) Attend **all** Channel Panel meetings as a **mandatory** Partner. Officers must be truly alive to intelligence and actively (and usefully) involved in Panel discussions.

      iv) Reassessing VAFs, updating CMIS and the PCMT, ensuring all case information is accurately recorded and retained on the Home Office approved case management system.

      v) Disseminating pertinent intelligence to relevant Partners.

      vi) Compiling all other documentation required to take a Case to each Channel meeting.

      vii) CTCOs are the only Partners able to refer cases to Vulnerability Support Hubs, so they must act as a conduit for any findings or recommendations between the Vulnerability Support Hubs and the Panel.

      viii) Capture any significant shifts in terrorism related vulnerabilities and risks uncovered during Channel Panel meetings and submit for FIMU assessment, wherever relevant.

      ix) Determine the most suitable route for a Case should it no longer be suitable for Channel, but the CTCO holds a reasonable belief that the vulnerabilities or risks towards terrorism offending have escalated e.g.:

         (1) Submit such Cases to the FIMU for reassessment.

17.0.5 Channel – CTCO Duties (Dovetail)

1) The following applies where a Subject is a potential candidate for being in the Channel Programme in a **Dovetail** site:

a) CTCOs refer Cases involving individuals to a **Local Authority Channel Coordinator** (**LACC**) no more than **5 working days** from de-confliction, or as close to this as is practicable within the circumstances of the Case.

b) Such cases are referred straight after the PGA decision for Cases where the CTCO has a **reasonable suspicion** that there is a PREVENT-relevant issue that may need addressing.

c) These submissions to the LACC must be endorsed by a CTCO Supervisor on the PCMT.

d) Submissions must be on the standard LACC referral form, and CTCOs should offer support the LACC by providing information and intelligence around the terrorism related vulnerabilities and risks that an Individual poses.

e) CTCOs must pass all relevant information from their Gateway Assessments to a LACC.

f) The LACC is responsible for entering the referral onto CMIS and subsequent management of the case Information Gathering for VAFs. Compiling all necessary documentation for each Channel meeting.

g) CTCOs must still attend Dovetail Channel Panels as a statutory Partner, supporting them with policing queries, CT related risks and potential mitigation suggestions as well as updating them with any relevant intelligence relating to the Subject. Officers must be fully engaged in this process and employ the same professional curiosity as they do in non-Dovetail sites and the PLP process.

h) CTCOs still capture relevant intelligence and submit to the FIMU for assessment.

i) CTCOs may still determine the most suitable route for a Case should it no longer be suitable for Channel in Dovetail sites. If risk escalates to such a degree that the CTCO and CTCO Supervisor agree that the case must be escalated out of Channel, this must be raised with the Channel Chair as a priority. Where there are risks of imminent terrorism offending, Police take lead in crime prevention and public protection decisions, but they must be fully justified on the PCMT.

j) CTCOs must still submit Cases to the FIMU for reassessment from Dovetail sites.

k) Where risks are policing / CT issues, these must continue to be managed by Police until an effective coordinated plan is drawn up. All risks should be fully documented on PCM in the Notes as well as any communication with the LACC.

l) **I&S**

17.0.1 Channel – Exiting & Outcomes for the Programme

1) If the Channel Chair decides that a Case can be closed, the Channel Outcome **MUST** be set on the PCMT. Refer to the CMIS & PCMT Guidance for Closure Codes and their rationales.

2) In non-Dovetail sites CTP PREVENT is responsible for selecting the MAP closure outcome on CMIS which follows the same process as above.

3) Channel Cases can only be moved to **Pending Closure** on PCMT if one of the above Channel Outcomes have been set.

4) Police are also expected to set up the review dates for the 6 and 12 month reviews.

17.0.2 Channel – Police Withdrawing Subjects from the Programme

1) Police have the power to remove Individuals from the Channel Programme if it is deemed necessary and proportionate in terms of the terrorism risk posed by the Individual.

2) Situations where this might arise could include where Police have reasonable grounds to believe that that the risk of terrorism related activity is escalating to the point where it may satisfy the requirements of an IHM lead or Priority Investigation. Should intelligence arising from a Channel meeting (or any other reasonable source) suggest that the risk posed by an Individual means that he/she is no longer suitable for Channel then, following discussions with CTCO Supervisors and the FIMU, a decision should be taken to remove the Individual from the Channel Programme, but this should be discussed with the Channel Chair **prior** to any action being taken.

3) Except where the terrorism risk has escalated, the Police cannot remove a case from Channel without the agreement of the Panel. Where there is a dispute between CT Police and other agencies on this issue it should be recorded on the PCMT. If the dispute cannot be resolved between CTCO Supervisors or 2nd line managers, then it should be referred to the Regional PREVENT Co-ordinator or their deputy.
4) Where a Channel Panel rejects a case as unsuitable, the CTCO must consider whether the issue that brought case into PREVENT still remains. If so, then it must be dealt with as a PLP case. Where there is no CT risk but a safeguarding risk remains, the case must be exited to the appropriate safeguarding service (e.g. local MASH).
5) Where a Channel Panel has accepted a case and subsequently closed it, should the CTCO believe that a CT risk or a serious enough PREVENT issue remains, consideration should be given to whether the case should be dealt with as a PLP case or exited to a safeguarding function such as a MASH.

17.0.3 Channel – Completing the VAF

1) In non-Dovetail sites, CTCOs complete initial VAFs for Individuals accepted into the Channel Programme. Officers should refer to the VAF Guidance on the CTNet for help on how to complete VAFs. VAFs should only be completed by a CTCOs with a good understanding of the vulnerability assessment.
2) Officers should note that the DIF contains all the considerations of the VAF (with additions), so the findings of the DIF(s) completed at the PGA and Information Gathering stages should translate well into an initial VAF. This vulnerability assessment should initially be completed by the relevant CTCO (Channel Case Officer) and then be circulated in full to Panel members in advance of meetings so that all relevant Panel members can contribute their knowledge experience and expertise to the case. Although mandatory, and just as with the DIF, the VAF complements rather than replaces other vulnerability and/or risk assessments that officers or Local Authorities are required to make around Individuals brought to their attention, as per national or local policies.
3) Completing the assessment for all 22 factors requires a thorough knowledge of the Individual that may not be available on first referral. Additional information should be sought as part of the Channel multi-agency process.
4) If the Individual is referred to an intervention more information will come to light from the intervention provider once they have built a relationship with the Individual. If the intervention is by mainstream services or is diversionary then knowledge of the Individual will build more slowly than if the Individual is to receive, for example, one on one faith counselling or mentoring.

17.0.4 Channel – Sharing the DIF with Partners (Dovetail & Non-Dovetail)

1) The DIF is a policing tool, one of our tactics. It is not automatically relevant for Local Authorities to see them in their totality, and nor is it a requirement in the Channel Guidance. However, it is the form itself (and the extended questions behind it) that is the tactic. The information put into a DIF by CTCOs is relevant for LACCs and Channel Panels, with the following caveats.
2) **Dovetail & Non-Dovetail:** When referring cases to a Channel Panel, whether this happens in a Dovetail or Non-Dovetail site, it is vital that all relevant information from DIF assessments are shared), **but there are some issues and caveats** around sharing DIFs in their totality:
   a) Will it be open to FOI requests or is there an Data sharing agreement, preventing this?
   b) Is there confidential information within the DIF that cannot be shared with Local Authorities, even with Data sharing agreements in place?
3) In any handover package provided to Local Authorities for the purposes of Channel, it is vital that CTCOs remove information that is irrelevant to PREVENT safeguarding and which might harm legitimate Policing purposes should it become more widely known. For example this could include:
   a) Specific policing **tactics** I&S,
   b) Secret or highly sensitive **sources** of information, (from intelligence partners perhaps),

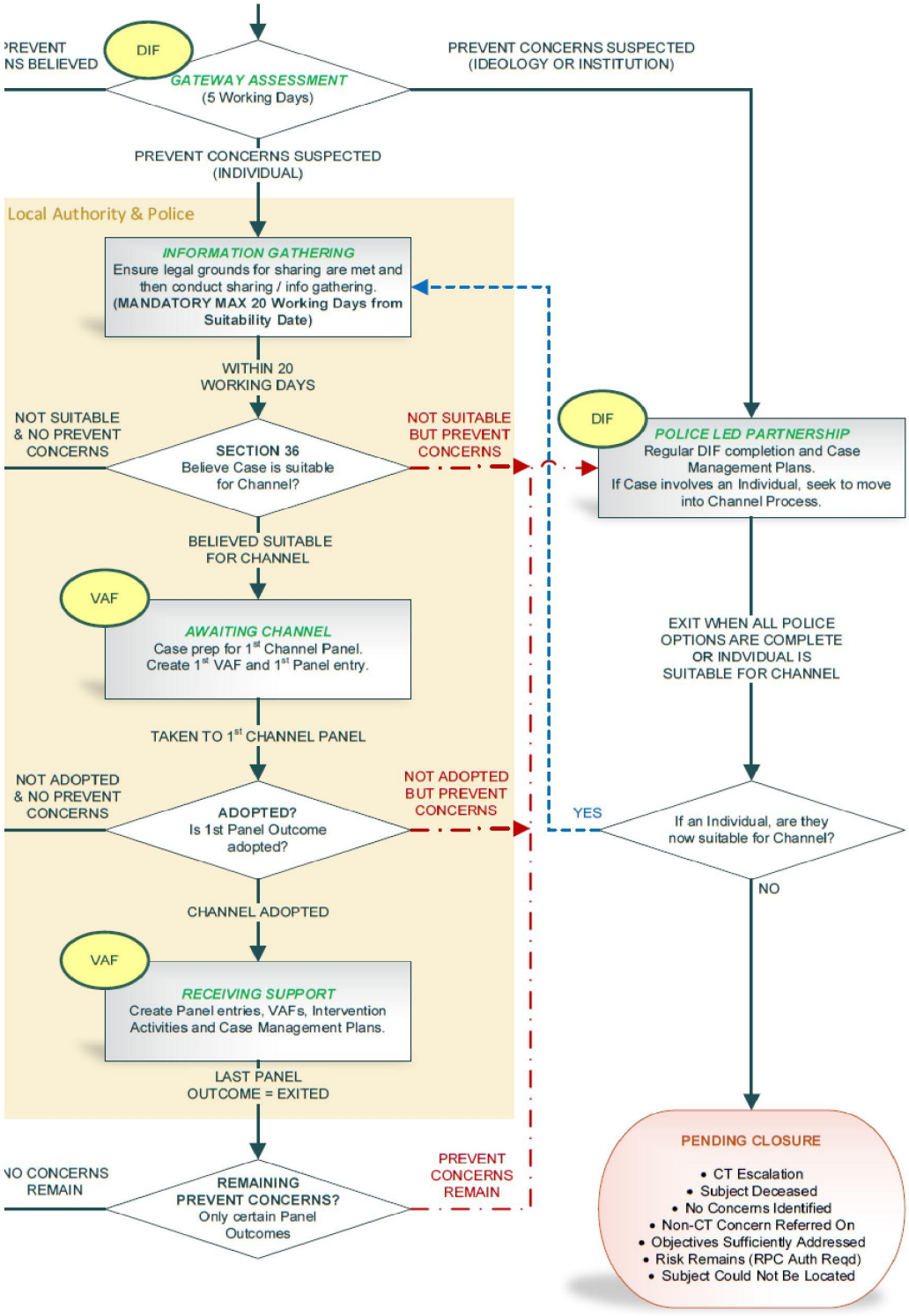
c) Personal or confidential information that has no bearing on the PREVENT case but has found its way into the DIF for whatever legitimate reason. This might include private information about the Individual's friends or family that has absolutely no bearing on the PREVENT issue at hand, nor any possible avenues of support or safeguarding. It could also include information around an active, covert Pursue case connected to the PREVENT case somehow.

4) **Non-Dovetail:** In non-Dovetail sites, CTCOs should be sharing initial VAFs, not DIFs. These VAFs should contain everything relevant found through the first use of the DIF during the Gateway Assessment and during the information gathering process. So in other words, everything relevant recorded in the DIFs, **BUT put into the initial VAF**.

18 PLP - POLICE-LED PARTNERSHIP & PANELS

1) The Police-led Partnership (PLP) process concerns the management of individuals, groups or institutions that are not suitable for Channel, but which have identified Prevent-relevant issues requiring support or mitigation, led by Police but working in partnership with other agencies. Refer to the PLP Panel Terms of Reference (ToR) first and use these notes for further clarification.

18.0.1 PLP – Basic Flowchart



18.0.2 PLP - General Information

1) **Channel vs. Police-led Partnership:**

   a) The PLP space has many similarities with Channel, except CTP PREVENT lead on the former and the Local Authority on the latter.

   b) Channel is the preferred route for all **Individuals** within PREVENT. For all viable PREVENT Cases, where an Individual resides (or is believed to reside) in one of the Local Authorities of England and Wales, the basic question should be **why this Case is not suitable for Channel**?

   c) Channel is a **voluntary** programme, PLP **does not require Subject agreement** to be accepted onto it. Channel is an **overt** programme, meaning that (within data protection, GDPR and human rights law) the 'bias' is to be open around information in relation to the Subject. PLP may have stricter and situational confidentiality requirements around cases and Subjects that are incompatible with Channel's overt nature.

   d) If an Individual is deemed to have PREVENT-relevant concerns that needs addressing, but is otherwise unsuitable for Channel, they are therefore likely to be suitable for PLP space.

2) **Who is Suitable for PLP Panels?**

   a) The following are all suitable for entry into the PLP process, with the stated caveats:

      i) An **Institution** – including recreational premises, religious or educational establishments, businesses, charitable bodies, public or private organisations where there are PREVENT relevant concerns.

      ii) An **Ideology** – this is only really an option where an Individual or Institution cannot be identified, so consider extremist or terrorism-related leafleting or stickering campaigns, signs, or other material appearing in an area that cannot be linked to an Individual or Institution in the first instance.

      iii) An **Individual,** with the following caveats:

         (1) **Individuals who are suitable for Channel:** but refuse consent to the support package and refuse to engage with the IPs of that programme.

            (a) Channel is a voluntary programme in the sense that the support it offers can be refused. As such, Individuals may withhold their consent or refuse to engage.

            (b) If a CTCO / PREVENT CTCO Supervisor has made a Section 36 (CTSA) decision to refer an Individual to a Channel Panel, and that Individual is accepted by the Panel but refuses Channel support, Police must regard the PREVENT concerns that merited the S.36 decision as risks that **still need managing**.

            (c) If an Individual is already **within** the Channel programme, but subsequently withdraws consent or refuses to engage with IPs, the CTCO and CTCO Supervisor must review all the Case information and assess whether any PREVENT-relevant concerns remain in play. All concerns should be discussed at the Channel Panel with the Channel Chair, with the intention of moving the Case into the PLP space if required.

            (d) **Primary objective:** develop a PLP case management plan (CMP) for the Individual, providing support, intervention providers and if necessary disruption of high risk or unlawful behaviours. All of this will be managed by means of PLP Panel.

            (e) **Secondary objective:** CTCOs and CTCO Supervisors must work in conjunction with the Channel Chair to reassure and support the Individual towards consenting / engaging with the Channel programme.

         (2) **Individuals who are willing to engage with Channel but who prove to be unsuitable:** if information indicates they pose too high a risk in terms of escalation towards any terrorism related activities. This is decided by the CTCO and CTCO Supervisor. It does not relate to non-CT or extremism related crime, violence or risks, which can and should be managed within Channel as normal, with Police support.

(a) Consider whether there is an operational need for CTP PREVENT to take direct control of case-management of the Individual, but where the Individual does not yet meet the threshold for an IHM lead to escalate out of PREVENT into the PURSUE space.

(b) Referring to Channel would create an unacceptable risk to the safety of any individuals involved with that Pursue case, or the potential Channel case.

(c) Examples might include Individuals who need control measures in place, or people who might be entrenched groomers, coercers or deliberate radicalisers of others towards terrorism offences, and who will not respond to Channel support.

(d) We should not be moving cases into PLP space because of an increase in **general** threat. An example might be a dramatic increase domestic violence by a Subject. Even though the threat posed by the Subject to family has escalated to an extent that "harder" Police control methods and prosecution might need to be employed, Subjects should remain in Channel for as long as they engage with that programme. There has to be an increase in the threat around **terrorism related activity**, i.e.: the PREVENT-relevant concerns.

(3) Individuals at RADO 4, where there is no PURSUE investigation.

(a) Individuals whom the FIMU assess as RADO 4 *may* be referred to PREVENT if the FIMU deems it appropriate, providing there are no active PURSUE investigations around that Individual, and providing it is CTP PREVENT that now "owns" that case. If the result of the CTCO's gateway assessment (which still must be completed) is that the case does not need to be re-escalated back to PURSUE, and the CTCO and Supervisor believe that the Subject's risk can be managed adequately by PREVENT, the RADO 4 Subject may be forwarded straight into the PLP process.

(4) Individuals who are connected to an overt PURSUE investigation or covert PURSUE lead.

(a) Family members of charged or convicted terrorism-offenders may well be suitable for PREVENT support, providing they are not Subjects of an ongoing Pursue investigation themselves.

(b) Although Individuals connected to an overt CT investigation are not automatically precluded from PREVENT if there are vulnerabilities that PREVENT could best address, their inclusion would need to be approved with the FIMU and/or the "owning" PURSUE case officer before any move into or out of the PCM process. Individuals who have a direct and concerning connection with an ongoing Pursue investigation[17] may not be suitable for management in PCM, and particularly the Channel programme. Channel is an **overt** supportive programme and it is contingent upon securing the **consent** of the Individual for involvement in a tailored intervention.

(c) Individuals already under covert investigation by PURSUE must not be accidentally "tipped-off" that CT Police are aware of them because PREVENT approaches one of their family members, for example.

(i) Former SOIs (RSOIs) and/or their family members that need support **may** enter PREVENT (potentially ether Channel or PLP) depending on the unique circumstances of the case. This must be agreed between CTCOs and CTCO Supervisors, and also the relevant FIMU / case-owners within the PURSUE space.

(ii) PREVENT interventions around these individuals **may** have to be more circumspect and indirect, as dictated by the complexities of the Case.

18.0.3 PLP – Entering Police-led Partnership

1) Entering PLP

[17] For instance, the individual may be a family member of an SOI currently under covert investigation, and referral to Channel may "tip off" the SOI, potentially placing the SOI's family members, or even the investigators themselves, at an increased risk of harm.

a) Some cases **can** be referred straight into the PLP space as a gateway decision, **without having to go through the information gathering phase or a S.36 Decision**.

b) These are cases where the Subjects are:

i) Ideologies,

ii) Institutions, or;

iii) Individuals where they meet the caveats described in the previous section.

c) Most other Cases referred into the PLP will be so **after** information gathering and a S.36 Decision. Some other cases may come from Channel, having either refused to engage with Channel support plans or having been escalated out of Channel due to dramatically increasing PREVENT-relevant risk, or terrorism related threat. An auditable record of decision-making must be kept within the case's notes on the PCMT to enable quality assurance. Accurate minutes provide an important account of this process. Minutes should be copied into the case notes on the PCMT and clearly identified as Panel minutes. Minutes should not be stored on other databases. In all circumstances, handling and retention of Panel minutes must be MOPI compliant.

3) Who Decides?

a) A decision to adopt the Case into PLP will be made because the CTCO & CTCO Supervisor, in some contexts this may be in consultation with an RPC or Channel Chair.

b) Channel Chairs should always be free to give their honest (even critical) advice and opinions to CTCOs, CTCO Supervisors and PLP Panel Chairs. Channel Chairs cannot dictate when a case should move into the PLP space, nor can they dictate when a case moves out of PREVENT into the PURSUE space.

c) CTP-PREVENT have a statutory duty to identify Individuals vulnerable to being drawn into terrorism related activity and make CTSA 2015, S.36 Decisions to refer them to the Channel programme wherever they deem appropriate. CTP-PREVENT cannot simply **dictate** to a Channel Panel that an Individual **must** be accepted for Channel management, although officers are expected to argue their cases professionally and with due care and attention.

d) Channel Chairs do not have to accept into Channel any Individuals referred to them by Police, although they should justify their decisions. Channel Chairs **may** also choose to offer Channel support to Individuals whom the Police decided, in their S.36 decision, to NFA from PREVENT. Although this is less likely as a Channel Chair may not be aware of cases closed by Police prior to a Channel referral.

e) Channel Chairs cannot "pull" Individuals out of the PLP space unilaterally, although they are free to make recommendations or raise concerns they have in a structured and auditable fashion.

18.0.4 PLP Case Management – Prioritising Cases

1) Every case entering PLP needs to have a priority level assigned to it. These are:

a) **High Priority (Red) –** This rating is assigned to any Case that suggests potentially higher, urgent or imminent threat, risk or vulnerability factors, e.g.:

i) **Any** unmitigated **Escalation** or **Mobilisation** factors (noted in the DIF).

ii) **Harm –** there is an apparent, imminent or escalating risk of harm to self or another.

iii) **Mental Health –** the Vulnerability Support Hub or other MH professionals have identified urgent concerns.

iv) **Time-Lock –** there is a deadline (like upcoming foreign travel) before which any assessments need to be completed.

v) **PURSUE Relevance –** This reflects the possibility that an individual involved in planning low-level, non-violent, terrorism offences (such as a groomed young person planning to travel to a conflict zone) may be recommended for inclusion in Prevent. However, anything that a CTCO or CTCO Supervisor suspect to be PURSUE-relevant. Bear in mind

that if you suspect a case might be PURSUE relevant, your first goal is to escalate it through the FIMU as a potential lead, so the case is very unlikely to stay within Prevent.

vi) **Professional Judgement –** anything that CTCOs & CTCO Supervisors believe to be particularly concerning within the unique context of the Case. Includes anything that officers believe might develop into, or encourage, critical or major incidents, or anything posing a significant risk to the reputation of PREVENT or the operation of Policing processes more generally.

(1) High Priority Cases should ideally be looked at every week until the specific high priority factors are mitigated. At the minimum, a new DIF assessment **MUST** be completed (along with any updates to the CMP, CTCO Supervisory review and sign-off):

(a) At least once every 4 weeks, or,

(b) Before any PLP Panel meetings, or,

(c) After any concerning changes in the Individual's complex needs, or,

(d) After any other **significant** changes in the Individual's life more generally.

b) **Standard Priority (Amber) -** This rating is assigned to any Case that suggests, within the professional judgement of the CTCO & CTCO Supervisor, moderate, developing or inferred risk / vulnerability factors, e.g.:

i) At least one PREVENT-relevant factor/indicator identified through the DIF that the CTCO suspects requires further work.

ii) Anything else that the CTCO and CTCO Supervisor agree requires work and/or corroboration, within the particular context of the Case.

(1) Standard priority Cases should generally be worked on every week or so until the specific standard priority factors are mitigated. However, at the barest minimum, a new DIF assessment **MUST** be completed (along with any updates to the CMP, CTCO Supervisory review and sign-off):

(a) At least once every 8 weeks, or,

(b) Before any PLP Panel meetings, or,

(c) After any noted change in the Individual's complex needs, or,

(d) After any other **significant** changes in the Individual's life more generally.

c) **Monitored (Green) –** No Cases enter into the PLP space assigned as "Monitored". It is the review period for all cases before they can be exited from the PLP space. This rating is assigned only to Cases that are already being managed within PLP, and where either the risk, vulnerabilities and priorities seem to have de-escalated demonstrably and consistently, or if it is deemed necessary to observe the Subject for a longer period of time before judging the impact of management and interventions upon the PREVENT issues / CT risk then such cases must not be closed. Instead the case must be shown as monitored.

d) Monitoring may also be used for circumstances where an Individual is not in the community for a short period (e.g.: is going abroad for three months), or has been sentenced to a short custodial period (e.g.: 12 weeks), but it is not appropriate to close the case.

e) There are no fixed timelines around Monitored Cases. It could be quite a short period. Timelines need to be decided and justified between the CTCO Supervisor and CTCO within the unique context of each Case. That said, Monitored Cases do need to be wrapped up and Subjects in this space either exited from PREVENT altogether (if the Case priorities associated with them have resolved), exited into Channel (if appropriate and the Individual is willing), or exited from PREVENT and escalated into Pursue if their CT risk has increased enough. Generally speaking, Monitored Cases should be reassessed:

i) At least once every 3 months, or;

ii) Before any PLP Panel meetings, or;

iii) After any noted change in the Individual's vulnerability, or;

iv) After any other **significant** changes in the Individual's life more generally.

18.0.5 PLP Panels – Terms of Reference (Expanded)

1) **PLP Panel Chairs:**
   a) Wherever possible, PLP Chairs must be CTP PREVENT Sergeants / CTCO Supervisors or above, and;
   b) The PLP Chair should not be the CTCO managing the cases discussed at the Panel, although it is recognised that this may not be possible across the entirety of the CTP PREVENT network due to operational and/or staffing pressures.
2) **PREVENT Coordinators:**
   a) Although the attendance of PREVENT Coordinators may be beneficial for PLP Panel meetings, it is recognised that this may not be possible in every region or for every Panel meeting.
3) **Channel Chairs:**
   a) It is good practice to involve Channel Chairs, where appropriate, at PLP Panels (in non-chairing capacity) to offer advice and/or assist in the management of PLP cases where:
      i) the individual concerned is suitable for Channel but rejects the programme, refusing to engage with Channel support plans, or;
      ii) the CTCO & CTCO Supervisor have assessed that an Individual being managed in the PLP Panel has decreased in risk / sensitivity to the extent that Channel is becoming the more appropriate case management pathway.
   b) It is recognised that some Channel Chairs may wish to remain "independent" of the PLP Panel process, perhaps because they feel that doing so will better allow any future referral from the PLP process to Channel to be assessed entirely "neutrally" or at "face value" on the merits presented. This is the prerogative of the Channel Chair.
4) **Channel Panel Members:**
   a) It is good practice for PLP Panels to comprise of the same Members as Channel Panels. However, Each PLP Panel must be constituted to meet the needs of the case, so there may be occasions where it is inappropriate for some Channel Panel Members to be present at a PLP Panel, depending on the vetting levels of these Members in relation to the sensitivities of the cases in review. The PLP Chair will decide and explain, on a case-by-case basis, who should be present at a PLP Panel and in what circumstances.
5) **PLP Panel Arrangements:**
   a) PLP Panels must operate separately from Channel Panels and PLP cases must not be heard as Any Other Business (AOB) at the end of Channel Panels.
   b) It is recommended that PLP Panels are held directly after Channel Panels wherever possible, whilst relevant Partners are gathered together. It is recognised that this may not be possible across the entirety of the UK PREVENT network and that alternative local arrangements might be required. These must be recorded on the PCMT within the notes of each case.
   c) Where a PLP Panel cannot follow directly after a Channel Panel, the PLP Chair will decide where and when a PLP Panel will take place. Necessity may dictate that some PLP Panels need to sit at short notice.
   d) Where PLP Panels follow directly after Channel Panels, there must be no accidental "overlap" between Channel and PLP cases. The Channel Chair will state clearly when the Channel Panel has finished, and the PLP Chair will state clearly when the PLP Panel has commenced. This should be clearly recorded in both sets of meeting minutes / actions.
6) **PLP Panel Chair during meetings:**
   a) Identify anyone who should not be at the Panel.
   b) Pass on the apologies of invited Members who cannot be present.
   c) The PLP Chair will ensure that independent PLP Panel agendas, minutes and actions are generated.

d) The PLP Chair will ensure that all relevant activities arising from previous PLP Panel meetings concerning open cases are reported back to the Panel for discussion.

e) The PLP Chair will ensure that Police retain all records on the PCMT, within the relevant cases. External partners to the Police must not keep separate records of PLP Panel cases.

f) The PLP Chair will ensure that all actions and minutes arising from the PLP Panel are provided in a timely manner to the responsible CTCOs for the cases discussed.

g) The Chair, through the CTCO, should ensure that wider family support is considered, e.g.: the family may need support to help cope with the complex needs of the Individual within PCM, and where the family is assessed as being protective and supportive of the Individual, CTCOs must ensure that updates and outcomes are given wherever appropriate and whilst maintaining confidentiality (i.e.: between the Subject and IPs).[18]

7) CTCOs after meetings:

a) The responsible CTCOs will update the relevant case on the PCMT with the minutes and actions resulting from PLP Panels, along with all other relevant details and outcomes.

8) Information Sharing Arrangements:

a) Information sharing between PREVENT Partners is permitted, and in some cases required, through existing legislation.

b) Data sharing agreements (DSA) should be considered best practice within the PLP process. DSAs streamline the information sharing process, laying out mutually agreed parameters to the uses, storage and deletion of the information shared. It is the responsibility of each region or force area to establish whether a PLP-specific DSA with partners is required, in addition to DSAs that may already be in place for Channel Panels. There is an editable DSA template available on the Ctnet.

18.0.6 PLP – PLP Panel Detailed Guidance

1) Overview: Each PLP Panel must be constituted to meet the needs of its subject.

a) Multi-agency working is the foundation of Prevent. PLP Panels, even though they are led by Police, are likely to involve appropriate non-Police partners, with the caveats noted in the **PLP Attendees & Chairs** section above.

b) Prior to Entering PLP it is imperative that **CTCO Supervisors** ensure that there is a **completed DIF with a full and clear rationale uploaded onto the PCMT detailing why the S.36 Decision (CTSA 2015) was to not refer the individual to a Channel Panel**.

2) Consent vs. No Consent Needed:

a) In Channel, Individuals within the programme have agreed to engage with the support plan and intervention providers.

b) In the PLP space, the Individual might not have agreed to engage, so the supportive interventions may have to focus on key people **around** the Individual (family, schools, etc.), whilst disruptive interventions could still focus on the Individual but also or people around them, where proportionate and necessary.

3) Frequency of PLP Panel Meetings:

a) It is best practice to hold PLP Panels monthly where there is a live case, though there may be occasions where meetings need to be held more frequently.

b) As a minimum, where a live case is held, there should be a minuted discussion between the Chair, relevant partners and the CTCO relevant to the Cases at hand to review progress and actions.

c) It is good practice to schedule meetings as far in advance as possible, preferably 12 months in advance, in order to support partner planning.

[18] http://www.ctnet.apps.Police.uk/wp-content/uploads/2019/05/CTP-Only-Toolkit-Safeguarding-Child-Returnees-from-Conflict-Zones.pdf (last accessed: 25/06/2020)

d) In the absence of live cases, PLP Panels should endeavour to meet at least quarterly. These meetings can be used to review practice, conduct audits, develop or monitor improvement plans or to plan and deliver Panel training.

4) Composition & Nature of PLP Panel Meetings:

a) The composition of the Panel is a decision that should be made based upon the nature and specifics of individual cases and time-bound actions that may be required. Panels could involve multiple people, or even just the CTCO and Supervisor for some "simple" Police disruption cases. The Chair should ensure the relevant CTCO is consulted and kept informed of any changes to Panel membership, and brief explanations of specific Panel membership should be included in the notes of each case.

b) Where partner input is required but cannot be secured in person, the Chair has discretion to facilitate the virtual input from partners, through systems such as video or tele-conferencing provision, though this should not be a consistent feature of Panel meetings.

c) The Chair will need to be satisfied that the confidentiality and integrity of the meeting is maintained (e.g.: whether a STRAP environment is necessary or not) and that the minutes reflect this. Confidentiality must also be secured for and from any partners inputting virtually.

d) The relevant CTCO will present the referral to the PLP Panel based on the information gathered:

i) During the multi-agency information gathering stage, and;

ii) From Channel Panel Partners if the case started at Channel before being drawn into the PLP space, and;

iii) Any DIFs completed by the CTCO.

e) It is best practice for there to be Panel consensus around PLP Panel decisions, particularly if the Case is a safeguarding one that is not in Channel only because of issues around consent. However, where this cannot be achieved, the PLP Chair has the casting vote.

f) CTP PREVENT will have executive power to make unilateral decisions around matters pertaining to their areas of responsibility and expertise – in this case the prevention of crime and judgement of terrorism related risk and threat for disruption or escalation out of PREVENT.

5) Deputy Chairs for PLP Panels:

a) If the Chair for an area cannot be the PREVENT CTCO Supervisor for reasons of resources or operational necessity, then the CTCO Supervisor must be satisfied that the designated Chair is a person with the required skills, experience and vetting, and ensure they have sufficient capacity and resource to fulfil these functions.

b) Wherever possible, and to ensure resilience, a Deputy Chair role should also be designated to an officer of similar standing and/or experience as the Chair. It is the responsibility of the unit to keep details of named officers designated by PLP Chairs to fulfil these roles and to confirm suitable arrangements are in place to meet the requirements set out in this guidance.

c) To enable the Chair / Deputy Chair to take full ownership of the PLP Panels process and apply appropriate rigour and challenge (where necessary), the following core competencies should be applied wherever possible to the appointment of the Chair / Deputy Chair, to ensure PLP Panels and the Chair responsibilities are fulfilled to a consistently high standard:

i) Have operational experience and a sound understanding in CTP PREVENT, Channel and the CONTEST strategy more generally.

ii) Hold sufficient authority to direct CTP PREVENT activities in the area and ensure multi-agency delivery.

iii) Have previous experience in chairing multi-agency meetings (such as Channel, MAPPA, Pathfinders, MARAC, Problem Solving Panels, etc.).

iv) Preferably have an understanding of child and/or vulnerable adult safeguarding.

v) Be committed to completing all training as required.

d) Chairs / Deputy Chairs of PLP Panels must be STRAP cleared and must acquire UK National Vetting clearance at 'Security Check' (SC) level (or higher where possible) to enable the sharing and handling of more sensitive information between the PREVENT and PURSUE spaces, wherever necessary.

6) Wider Responsibilities for PLP Panel Chairs:

a) In addition to the duties mentioned above, PLP Panel Chairs should:

i) Have oversight of all PLP Cases in their area.

ii) Ensure good communication and effective working with the Channel Chairs in their areas.

iii) Establish effective relationships across partners of the Panel to ensure effective cooperation over information sharing, attendance at Panel meetings and delivery of support.

iv) Ensure the various partners **on** the Panel carry out their elements of the support plan, holding these partners to account where necessary through proactive management of actions, enquiries and interventions.

v) Ensure appropriate information exchange occurs where Individuals transfer between services / agencies, or between PLP and Channel.

vi) Provide oversight that escalating threats of Individuals subject to PLP Panels are referred in a timely manner to the FIMU / PURSUE.

vii) Apply professional judgement and providing the casting vote on the adoption of cases where there is any uncertainty from CTCOs.

viii) Ensure compliance (within the specified exemptions for CTP PREVENT), around MOPI, GDPR and DPA 2018, in partnership with relevant information governance and legal teams.

7) Wider Responsibilities of CTCOs in PLP Panel Cases:

a) Attend all meetings where the CTCO's cases are being discussed.

b) Identify and engage approved Intervention Providers.

c) Create agendas for Panel meetings, as per directions from PLP Chairs / CTCO Supervisors.

d) Advise PLP Chairs as to which Partners may be relevant and useful to the Case are present at the PLP Panel.

e) Take any findings or recommendations from the **Vulnerability Support Hubs** to the Panel meeting and refer any new concerning behaviours or circumstances back to the Hubs, as relevant.

f) For every Individual they bring to PLP Panel, CTCOs must develop CMPs, in conjunction with Partners where relevant, that are proportionate and justifiable within the context of the Case.

g) Identify any potential travel risks and ensure that appropriate markers are placed on PIW, PNC and Local Intel Systems, if appropriate to the Case.

h) Use the DIF, the approved CTP Intervention Guides, and the NDM for risk assessments and in the development of CMPs, to be presented as relevant at PLP Panels.

i) Compile all other documentation required to take a Case to each PLP Panel meeting.

j) Disseminate any other pertinent information to relevant Partners.

k) Capture relevant information from PLP activities regarding the Individual's escalating or de-escalating risk of terrorism offending, and feed this information back into the FIMU for re-assessment and/or closure from PREVENT.

l) Determine, along the CTCO Supervisors, the most suitable route for a Case should it no longer be suitable for the PLP.

8) CTCO Responsibilities Between PLP Panels:

a) Work through the plan with any relevant Intervention Providers, ensure DIFs have been completed competently and regularly to ensure vulnerability and risk are being regularly assessed.

b) Wherever appropriate, CTCOs will manage interventions, supportive or disruptive, within PLP cases, paying particular attention to who is best suited to enact each intervention in each context.

c) Use the DIF and feedback from the Panel (and VS Hubs) to re-assess vulnerabilities and risks posed by (and to) Subjects at regular intervals, or whenever there is a significant event in the Individual's life.

d) Update relevant warnings or "watch-lists" that have been activated where applicable.

e) Update PLP Panel Partners of anything pertinent to the Panel's management of the Case, and bring all relevant information to each Panel.

18.0.7 PLP Panels – Case Management Plans (CMPs)

1) What is a CMP?

a) All cases are managed on the PCMT system. Please refer to the PCMT Guide (attached and on CT-Net) for details.

b) All Cases in the PLP route and currently the subject of a PLP Panel require a **Case Management Plan** (**CMP**).

c) Each case is handled separately. People deemed appropriate to receive support will have a tailored package developed for them, according to their identified PREVENT-relevant vulnerabilities, risks and/or threats.

d) CMPs are a combination of risk / vulnerability assessments and multi-agency support and interventions plans for Individuals within the PLP space.

e) The CMP must include each identified risk and vulnerability (i.e.: the **Case Priorities)** and their underlying causes, along with an associated action plan for each of these, with the intended outcomes of each intervention and a suggested means of measuring when a Case Priority has been suitably mitigated.

f) Support offered for some Individuals could span the competencies of several different Police units, and agencies outside of the Police.

2) Sources for CMPs?

a) CMP uses:

i) DIFs completed by CTCOs, and any other risk or vulnerability assessments completed around the Case (VAFs, etc.).

ii) The input of Partners around PLP Panel, or minutes from Channel Panels if the Case has been at the Channel Panel previously.

iii) The **National Decision Model** (**NDM**) is the method by which we decide on actions, interventions and outcomes at PLP Panels.

3) Developing a CMP:

a) Consideration should be given to:

i) Risks posed to the Individual of being radicalised, groomed and exploited in a PREVENT-relevant sense,

ii) Risks posed by the Individual of radicalisation, grooming and exploitation in a PREVENT-relevant sense,

iii) Wider vulnerabilities and complex needs of the Individual that feed into the PREVENT-relevant concerns.

b) All analyses and assessments so far should be brought together to plan the next steps for this Case. As a minimum, and wherever possible, consider:

i) Any advice from the Vulnerability Support Hubs and any other Partners involved in a PLP Panel.

ii) Your Individual's apparent strengths in relation to their apparent needs.

iii) Which vulnerabilities & risk factors you think need to be prioritised, why & in which order.

iv) What still needs to be found out, corroborated or explored further.

v) The supportive & disruptive needs, & provide a timetable for your proposed interventions.

vi) Who might be best placed to lead / enact proposed interventions.

vii) Anything that might worsen any of any risk or vulnerability factors.

(1) What are they?

(2) Which specific factors might they aggravate?

(3) How might they do so?

viii) Anything that might help improve any risk or vulnerability factors.

(1) What are they?

(2) Which specific factors might they help?

(3) How might they do so?

ix) How you will 'layer' your interventions to maximise positive intended outcomes, & minimise negative unintended outcomes.

x) How & when you will assess the success or failure of any interventions.

4) To help establish the above, draw upon the breadth of the intervention manuals and guides available to CT Policing. Currently, these are primarily the:

a) I&S

iii) College of Policing: Menu of Tactics,

5) I&S

a) All supportive and/or disruptive interventions you plan to attempt **MUST** be documented within your CMP and uploaded to the PCMT.

6) **YOU DO NOT HAVE TO COMPLETE A WHOLE NEW DIF EVERY SINGLE TIME YOU WISH TO ATTEMPT A NEW TACTIC. However, use professional judgement in relation to the effect of the tactic in terms of its potential significance to the Subject.**

a) Simply add the new tactic you will be attempting, along with timelines and rationales (etc.), to the rolling log of your CMP in the notes section of the PCMT. Make sure you record everything you intend to do.

b) Each CMP must be reviewed at a minimum every three months. Where a case priority is deemed to be **High** then the CMP should be reviewed on a more frequent basis. During the management of a Case the CMP should also be reviewed whenever a significant event occurs. A significant event can be anything that has the potential to change the risk assessment (Travel, arrest, changes of circumstances, additional intelligence etc.). Each piece of intelligence received should be assessed to determine if there is an impact on the Case and the CMP reviewed accordingly.

c) All interactions and activities involving the Individual or those connected with the Individual should be documented on the PCMT.

18.0.8 PLP Panels – Case Resolutions

1) Before considering case closure, a final CMP **MUST** be completed to ensure that all risks have been identified and mitigated to the fullest extent.

2) If a decision has been taken to close a Case then the CTCO **MUST** ensure that all Case Details are fully completed. This should include:

a) Subject Bio Data (First & Last Name, Date of Birth, Addresses, Telephone Numbers, Additional Info and Social Media Information).

b) Case Information (Summary, Primary Influence, Primary Activity, ERT Theme, De-confliction Information, Actions Closed and All Relevant Activities Are Selected).

c) All Referrals must be captured.

Go to Contents

CTPHQ000034_0065

19 DIF - THE DYNAMIC INVESTIGATION FRAMEWORK

1) This section looks at the DIF itself:
   a) What it is.
   b) What it does.
   c) When we use it.
   d) How we use it.
2) **IMPORTANT:**
   a) **If It Isn't Recorded, It Didn't Happen:**
      i) If you have not recorded something relevant that you have found out, considered, suspected or done within the DIF, or at least within the Notes section of the PCMT, then if there is a review of the Case there may be no evidence that you did any of the above. If something has not been explained and recorded, it is possible that it will be treated as though it never happened for the purposes of internal disciplinary purposes, Serious Case Reviews or the Courts.

19.0.1 DIF – Background

1) **Dynamic Investigation Framework (DIF):**
   a) The DIF is built upon the VAF,
   b) It is a CTP tool designed to help CTCOs screen, triage and risk manage PREVENT Cases.
2) **DIF Uses:**
   a) The DIF is used at the gateway assessment stage and at the CMP stage, and indeed for any and all assessments completed by CTCOs outside of the Local Authority led space. So it only applies **prior** to Channel and for Cases within PLP processes. The DIF helps CTCOs establish specific facts about a Subject and the Subject's context. These facts can then be assessed in their contexts to identify vulnerabilities and risks around radicalisation, extremism and potential terrorism offending (or the escalation towards these).
3) **What "DIF" means:**
   a) **Dynamic –** like other dynamic risk assessments, the DIF is "dynamic" in the sense that it is a "rolling" assessment. It is supposed to be reactive to new information. It is not 'static'. As new research or knowledge comes about, the DIF form and the guidance around it will be updated. Also, whilst actually using the tool to make our assessments, assessors must be open to new information and shifting priorities.
   b) **Investigation –** Police are investigators. CTCOs are no exception to this. To do our job we need to ask questions, and think critically and creatively. The DIF helps us do that.
   c) **Framework –** the DIF is a **guide**, a foundation, to help us investigate and assign priorities better. It does not, however, do all the work for us. It does not replace the need for our professional judgement.
4) **Designed for UK CTP PREVENT:**
   a) The DIF is designed to be used within its unique context, with three tiers of triage, supervision and assessment:
      i) Used by trained CTCOs,
      ii) Checked by trained & experienced CTCO Supervisors,
      iii) In tandem with **Vulnerability Support Hubs**: these provide greater nuance (and, where necessary, detailed formulations) around Subjects.
   b) These integrated tiers of triage, supervision & assessment are designed to complement each other, filtering out those who do not need support through the CT safeguarding programmes of PREVENT. This minimises false-positives and improves accuracy for support, safeguarding, disruption and other interventions.
   c) They also help reviewers to:

i) assign resources more appropriately,

ii) narrow the focus of their investigations,

iii) develop detailed management and intervention plans,

iv) direct Cases to the most appropriate forms of management and interventions,

v) identify Case priorities (specific terrorism / extremism / radicalisation / grooming related risks and offences),

vi) identify complex needs, vulnerabilities 'intrinsic' to the Subject or around the Subject's wider circumstances,

vii) record and justify decisions and actions clearly and with a greater degree of accuracy and rigor.

5) **Structured Professional Judgement**:

a) The DIF takes a Structured Professional Judgement approach.

b) This means it helps identify specific facts around vulnerability and risk factors and indicators, which can then be assessed using professional judgement to establish Case relevance, priorities and to develop Case Management Plans (CMPs) within PLP Case Management (PCM).

6) **Simple to Use:**

a) It is designed for use by **CTP PREVENT Practitioners** without specific or in-depth training in mental health issues or the behavioural sciences.

b) It is designed to flag up known push & pull indicators, and risk factors that frequently have relevance in the escalation towards almost any sort of terrorism related activity (including non-violent offences).

c) These various factors and indicators can then be assessed in their contexts in order to manage the Individuals concerned within the PREVENT space.

7) **Vulnerabilities, Risks & Threats:**

a) The DIF identifies behaviours, contexts, conditions and relationships that, depending upon their unique circumstances, may well be indicative of requiring support and/or mitigation in order to PREVENT escalation towards harm and/or offending.

8) **Engagement, Intent & Capability:**

a) These three areas are the core of the VAF and therefore the core of the DIF.

b) They are considered separately. Experience has shown (for instance) that it is possible to be **engaged** without **intending** to cause harm, and that it is possible to **intend** to cause a massacre without being particularly **engaged** with a terrorist group or ideology.

c) Experience has also shown that it is possible to **desist** (stop a dangerous PREVENT-relevant behaviour) without fully **disengaging** (losing all sympathy or interest to the "cause"), though losing sympathy with the cause (disengaging) generally results in desistance (loss of intent), unless a replacement and equally dangerous cause is adopted to replace the previous one.

d) **Capability** includes both people are **physically capable** of doing (such as training, experience or useful networks), and also what they **think they are capable of.** For example, if I decide very firmly that I am both a warrior and stone cold killer, even if I have no particular physical capabilities in these directions and no history of relevant offending, I still have access to a car or kitchen knives and so may be able to cause harm to myself and others if my circumstances do not change.

9) **Context**

a) The DIF encourages reviewers to regard the **context** of apparent **engagement**, **intent** and **capability** as closely as these three themselves.

b) A social or familial context that is permissive towards (or actively promotes or causes) violence, acute anger or other kinds of serious offending can be as relevant as the specific behaviours of the Individual being assessed, and this can apply even if that context of violence, anger, and/or offending is not specifically extremist in nature.

10) **Not a Predictive Tool:**

a) The DIF is not able to definitively predict terrorism activity in all circumstances. However, more efficient support and intervention procedures of vulnerable people do not necessarily require definitive prediction-of-terrorism, as indeed with any other vulnerability or risk assessment in the public sphere.

19.0.2 DIF – Overview

1) CTCO Expertise:

a) To our Statutory Partners and to the public / news-media, CTCOs are regarded as the criminological / CT PREVENT "expert" in the PREVENT process. What CTCOs say (or do not say) carries weight for good or for ill.

b) Completed DIFs are the professional (and expert) opinions of dedicated Counter-Terrorism Case Officers, based upon all the information to hand.

2) Professionalism & Rigour:

a) CTCOs must complete each DIF with a level of care and rigour that would be reasonably defensible to:

i) Internal scrutiny and Case reviews,

ii) A judicial review or Coroners' Court Case (etc.),

iii) External scrutiny such as a serious Case reviews by an independent body,

iv) The news-media (under Freedom of Information) or even a governmental select committee.

3) Who, When & How:

a) Who:

i) DIFs should only be completed by CTCOs, or a CTCO Supervisor if operationally necessary.

b) When:

i) Gateway assessments on FIMU de-conflicted referrals.

ii) During information gathering, prior to Channel / PLP.

iii) Within the PLP space in order to develop CMPs, inform PLP Panels and to close cases.

c) How:

i) The CTCO must have a good understanding of the DIF.

ii) For Gateway Assessments it should first be carried out following the initial background checks and call to the Initial Referrer and/or the last person or organisation that handled the referral prior to in arriving with CTP PREVENT, using any information gleaned. This is a triage not an in-depth assessment.

iii) For case management plans in PLP, the DIF needs to be more comprehensive and requires the CTCO to have much clearer knowledge of the Subject, after further information gathering, probably involving other agencies.

iv) It should then be shared by the CTCO at any PLP Panels formed around the Case, so that all practitioners can contribute their experience.

v) The DIF should complement (and where relevant, be informed by) any other local or national mandatory safeguarding or risk assessments, depending on the unique circumstances of the Case and the people involved.

vi) Whatever the Case, if the Individual has concerning connections to extremism or terrorism offending, or if the Individual is showing signs of interest in extremism or terrorism connected offences of any kind, then these are PREVENT relevant concerns and a DIF is appropriate to determine the specific vulnerabilities around the Individual being drawn towards terrorism offences.

4) Learning by Doing:

a) The best way to learn how to use the DIF is to work through each section methodically, read each box, follow the instructions and endeavour to ask and answer **all** the questions provided wherever possible within the unique context of each Case.

b) Each box has a heading and an associated, generic question for the CTCO reviewer to consider in relation to the Case at hand.

c) Every underlined word or heading in the form is a link to further guidance and more specific considerations.

d) When completing a section:

i) Read the title of the box,

ii) Read the basic question of that section,

iii) Follow the link to the more detailed questions of each section and consider them carefully within the context of the Case,

iv) Consider any wider issues that may be associated with the Case but which do not appear in the questions and considerations provided.

5) Professional Duty of Care:

a) Every question box requires an answer that shows you have considered the matter at hand within the specific context of the Case.

b) This means answers of "N/A" or "None Present" are inadequate in most circumstances. Explain briefly why the section is not relevant or why there are no risk or vulnerability factors or indicators present. This is particularly important at the gateway assessment stage, although it remains relevant for every use of the DIF.

c) At the end of the assessment section there is an Outcome section where CTCOs record their decisions, prioritisations and plans around the Case, and where the CTCO Supervisors provide their approval and any further advice or comments.

19.0.3 DIF – Making Assessments

1. **The 4 Rs:** At their most basic, every assessment in PREVENT policing involves**:**
    a. **Risk –** Identify PREVENT-relevant risks, threats and safeguarding concerns from information or intelligence received.
    b. **Rationale –** Consider strategies, tactics, actions to address or mitigate the identified these concerns.
    c. **Record –** Ensure all decisions are recorded and explained on the PCMT.
    d. **Review –** Timely review of new information or intelligence, and all decision-making, throughout lifecycle of a Case, including at point of closure.
2. **The RADO Model:** To unpack the above a bit more, the basic principles for making an assessment of vulnerability, risk and/or threat are explored very well in the RADO process, reproduced here with a PREVENT case management slant:
    a. **Receive –** information and intelligence from the FIMU, the public or any other source or mandatory check, etc..
    b. **Assess –** The following are the **sorts** of considerations you must bear in mind (this is not an exhaustive list and the following sections break down specific PREVENT considerations):
        i. *Risk*
        ii. *Threat*
        iii. *Credibility*
        iv. *Actionability*
        v. *Safeguarding*
        vi. *Proportionality*
        vii. *Evidential Opportunities*
        viii. *Intelligence Opportunities*
    c. **Decide –** Using the **National Decision Model** (and referring to the DIF and the guidance in this document) you must decide on the most appropriate outcome and forward pathway of the Case after every assessment. You must always provide rationales.
    d. **Outcome –** This refers to the actual outcome of your decision; where the case actually ends up**.**

3) **Types of Information & "Evidence":**

a) CTCOs, like any other Police officer, must often investigate and assess information and evidence.

b) CTCOs must bear in mind that looking for evidence around PREVENT concerns does not automatically equate with a criminal investigation for evidence, and as such should be treated with even greater sensitivity. A PREVENT relevant concern may involve allegations of criminality, but this is by no means certain, and PREVENT referrals do not require a criminal element for there to be concerns around someone being drawn towards terrorism offences. Similarly, if there are allegations of crime involved in a referral, crimes committed by PREVENT relevant Subjects do not have to involve terrorism connected offences. Such offences would generally propel the Case out of the PREVENT space into the Pursue space.

c) The DIF is a means to **collate** and **assess** data and information around a Subject's potential vulnerability, risk and threat in relation to being drawn towards terrorism connected offences. The DIF does not necessarily have to operate at the "beyond reasonable doubt" standard. It often operates upon the "balance of probabilities", or even lower at the level of "reasonable suspicion". As such, whilst identifying recording information within a DIF, CTCOs should include any information that they may reasonably suspect to be relevant. This can include direct, hearsay, and circumstantial information:

i) **Direct Information:** like direct evidence, is any information that directly proves or disproves a proposed "fact":

(1) For a comparison, the most well-known type of direct **evidence** is testimony, given under oath, from a corroborated eye witness, where the witness states exactly what they experienced, saw, or heard.

(2) For our purposes in the DIF, direct **information** could include clear CCTV showing the matter at hand, or the direct experience of the CTCO of the concerning behaviour by the Subject, or any direct evidence given as part of other lawful proceedings.

(3) Direct information may also be found in the form of documents. Legal documents or statements by a certified expert on a matter pertaining to their direct area of expertise (such as a formal medical diagnosis from a qualified physician), may be considered direct information.

ii) **Hearsay Information:** is any "an out-of-court" statement offered as a statement of truth about a matter that has been asserted. For our purposes completing DIFs, this means:

(1) Anything the Subject says about a Second or Third party, outside of court and outside of a formal, signed witness statement, and therefore without corroboration (direct evidence) to confirm it.

(2) Anything a Second party (perhaps a teacher or family member) says about the Subject or a Third party (perhaps an associate of the Subject), outside of court or a formal, signed witness statement, and therefore without corroboration (direct evidence) to confirm it.

i) **Circumstantial Information**: is information that does not point directly to a fact and requires an **inference** in order to prove that fact:

a. For example, a person who comes into a building. It *may* be raining outside (although you cannot see because you have no windows), and the person is carrying a wet umbrella and wearing a wet rain coat.

b. You could **infer** that it is raining outside from the circumstantial evidence of the wet umbrella and coat.

c. For our purposes within PREVENT, you might infer that a Subject has white supremacist sympathies if he/she is a member of a dedicated white supremacy online chatroom, frequently logs into that chatroom, or has white supremacist friends online, even if he/she has not written anything to support or critique the ideology.

d. Circumstantial evidence, like hearsay evidence, needs corroboration wherever possible. In the example given above, without corroboration, the Subject may have no toxic sympathies at all and may just visit the white supremacy chatrooms to study those attitudes for research purposes.

e. **Corroborated or Single Source Information**: irrespective of the type of information you receive, you need to ascertain whether it is from a single source (reliable or otherwise), or whether it has come from multiple sources, and is something you can corroborate. Detail all corroborating sources.

19.0.4 DIF – Breaking It Down: What to Write

1) Gateway Assessments vs. Case Management Plans (CMPs)

a) How the DIF is used will vary depending on whether you are using it to:

i) Arrive at a PGA Decision, or,

ii) To develop and update a PLP Case Management Plan.

b) Gateway Assessment:

i) Speak to Initial Referrer and/or the last person or organisation that handled the referral prior to in arriving with CTP PREVENT.

ii) If you have not received a FIMU handover with confirmation of the following checks, or if you do receive a handover but with no details of whether any PREVENT-relevant issues (and other relevant vulnerabilities) were identified, complete the following mandatory background checks (at least) looking for any issues potentially relevant to PREVENT:

(1) PNC.

(2) PND.

(3) NCIA.

(4) Local Crime & Intel Systems.

(5) CT Holmes (where available).

iii) Other Research: may be deemed necessary if it is considered as appropriate by CTCOs and CTCO Supervisors in relation to the information around the case. It is not mandatory for every case. These might include:

(1) Dedicated Tracing Unit (DTU),

(2) National Domestic Extremism Disorder Intelligence Unit (NDEDIU).

iv) Try to ascertain:

(1) Is the Subject aware of the current PREVENT referral?

(2) Has the Subject been visited by Police for this or any previous PREVENT / CT matter?

(3) Include dates, reasons & outcomes (if known).

(4) Previous contact may influence intervention tactics & their success.

v) PGA Decision:

(1) THE PGA PHASE IS NOT COMPLETE UNTIL THE DECISION IS APPROVED BY A CTCO SUPERVISOR.

(2) Once you can demonstrate a **Reasonable Suspicion** of any PREVENT relevant concern, your PGA Decision will be to keep the Case within PREVENT for now. You do not have to decide yet whether it is a Local Authority Led Channel case or a PLP case, because the next step will be to put the case into the Information Gathering Phase.

(a) Once you have reached a reasonable suspicion of a PREVENT relevant concern, providing you have explored, clearly articulated and justified that concern, **you no longer need to answer every question** if you do not wish to**.** This is because your Gateway Assessment is complete in the sense that you have decided to keep the Case within PREVENT and to forward it to the information gathering phase, during which all other unanswered questions must be answered. Once a PGA Decision has been made and Supervised, you can upload you're your DIF with rationale to the PCMT.

(b) **CAUTION:** if it is likely that you will not be able to address the case for several days after forwarding it into the information gathering phase, and you have not investigated every section of the DIF, there is a danger that some risks may be present, imminent and unaddressed in the meantime.

(3) Once you can demonstrate a **Reasonable Belief** that there are no PREVENT relevant concerns associated with the case, or that there is a PURSUE relevant concern that needs escalating out of PREVENT, your decision can be to close the case. You may also stop investigating every element of the DIF questions for cases that have clearly been entered in error, or which are obviously and demonstrably misguided, malicious or misinformed. However this **must be demonstrated** very **carefully** and **thoroughly** in your closing rationale and approved by your CTCO Supervisor.

(a) Once you have reached a reasonable belief of **no** PREVENT relevant concern, providing you have **investigated**, clearly **articulated** and clearly **justified** or **evidenced** that absence of relevant concerns, you can stop filling out the DIF form. Your Gateway Assessment is complete and you can upload your PGA Decision and your rationale to exist the Case from PREVENT.

(b) **CAUTION:** this is an even higher risk area than mentioned above. If you have not explored all avenues of vulnerability and risk because you believe that the referral you have assessed it is likely that you will not be able to address the case for several days after forwarding it into the information gathering phase, and you have not investigated **every** section of the DIF, there is a danger that some risks may be present, imminent and unaddressed in the meantime.

c) **DIFs During PLP Panels:**

i) As with the VAF, completing a detailed DIF assessment requires a thorough knowledge of the Individual that will not be generally be available during the PGA Additional information should be sought as part of the multi-agency information gathering process.

ii) If the Case is not closed after Information Gathering and the S.36 Decision is to refer the Individual into the PLP space, more information will come to light from any intervention providers once they have built a relationship with the Individual.

iii) If any interventions are by mainstream services or is diversionary, then knowledge of the Individual will build more slowly than if the Individual is to receive, for example, one on one faith counselling or mentoring.

iv) Speak with any Partners relevant to the Individual and the circumstances of the Case (Local Authority, FCO, other governmental or State agencies), and complete any recommended background checks for current or historical issues (at least within the last 3 years), which have not already been completed. These may include:

(1) CTP-NOC.

(2) PCMT.

(3) Open Source.

(4) Voters Register.

(5) Missing Persons.

(6) Briefing Systems.

(7) FCO – International PREVENT Desk.

(8) KINs (**Key Information Networks** where they are relevant and proportionate).

iii) Where necessary and proportionate, ascertain whether the following are at all relevant to, or impactive upon, the Case at hand:

(1) Is the Subject 'On License'?

(2) Immigration / Asylum Status?

(3) Current & Previous Workplace?

(4) Disabilities, Disorders or MH Issues?

(5) Family Makeup / Who Lives with Subject?

(6) Ideology, religion or politics of the Subject?

(7) Do they have a National Insurance Number?

(8) Nationality / Country of Origin / UK Citizenship?

(9) Current & Previous Educational Establishment(s)?

(10) Where they are currently staying / residing (if different from their registered address)?

2) Say What You See, What You're Told, When, Where & by Whom:

a) Be sure to state clearly where you got the information, who told it to you and in what context.

b) You need to know the difference between Direct, Hearsay and Circumstantial information, although you do not need to describe the different kinds of evidence in these terms.

c) Never present hearsay or circumstantial information as "fact". Always described the **context** of the information. Any information that could be described as hearsay must be ascribed to the person you uttered or provided it. Never present hearsay as a "fact". For example:

(1) If a Subject's mother says the Subject is autistic, but there is no diagnosis, this should be recorded in a similar way to the following - "the mother has stated that she believes her son to be autistic, although she has confirmed to me that she has not taken her concerns to her son's GP and there has been no formal diagnosis to this effect yet".

(2) If there is only hearsay evidence that the Subject punched someone and you think it's true, then do not write "the Subject punched this person", instead write "this person says that the Subject punched him and I believe this to be credible for XYZ reasons."

3) "N/A", "NONE", "NOT KNOWN":

a) It is generally inappropriate for CTCOs to record "N/A", "NONE", "NOT KNOWN" in any section of a DIF where the Subject of the Case is an **Individual**.

b) It **is** acceptable to do this for some sections if the Subject is an **Institution** or **Ideology** – an ideology is not going to have Complex Needs, for instance.

c) If a CTCO writes: "None Present" in the **Intent** box, for example, when what they really mean is: *"with the limited information available at this time, I have not found any specific intent factors",* then our Partners, the Courts and to any other person or agency that may end up reviewing your work, may interpret this to mean that the CTP experts have formally designated that there are no Intent factors present **at all**.

d) CTCOs should endeavour to give a brief explanation of **what** they have looked for, or **where/how** they have looked, even if they can otherwise only write something like: *"nothing apparent at time of assessment"*.

4) "COMMENTS & FURTHER ENQUIRIES":

a) These boxes are there to help with recording thought processes in a structured way. You do not always have to write something in them.

b) They are for CTCO notes around the information in the section above them - if there are any doubts around the information being recorded, or any other issues or comments the CTCO thinks relevant.

c) So for instance in the COMPLEX NEEDS box you might put:

i) "Jonny's mother says that he is: *'a bit autistic'*, but his father (who lives separately) says Jonny isn't autistic at all. There's apparently no formal diagnosis either way."

d) If the CTCO finds it helpful, the COMMENTS section could include something like:

i) *"I contacted the child's school and GP (with mother's permission), but the school is on a holiday and the clinic was closed. I'm unlikely to get a response before the 5 working days of the Gateway Assessment have passed. However, as Jonny lives with his mother, her observation may be worth considering. If it is deemed relevant to Jonny's risk & vulnerability to being drawn into terrorism in his particular circumstances, the suggestion of autism would need to be corroborated."*

e) This could apply to anything else, particularly where there is one word against another, or strong allegations or suggestions from people who SHOULD know something, but where there is little or no corroborating evidence in the first instance.

20 CMPS – CASE MANAGEMENT PLANS & INTERVENTIONS

1) In this section we will explore how Case Management Plans (CMPs) are developed.

20.0.1 CMPs - Overview

1) Every PLP Case must have a current **Case Management Plan** (**CMP**).
2) This is where you pull together your analysis & plan the next steps for this Case, using all tools available to you, including the DIF, any Partners around a PLP Panel, and of course the NDM. For safeguarding and supportive measures, it is imperative that CTCOs draw upon the expertise of Partners and formulate plans in conjunction with them.
3) It is recognised that the three themes that make up what we refer to as the "Subject" - **Individuals**, **Institutions** and **Ideologies** - can overlap and so CTCOs must decide upon the most relevant sub-division when developing a CMP, bearing in mind that the order of preference **must** be, wherever possible:
   a) **Individuals.**
   b) **Institutions.**
   c) **Ideologies.**
4) It is important that CTCOs are aware of how their tactical delivery of PREVENT supports the broader strategic vision for the policing role in this specialist area.
5) A comprehensive CMP should not only aim to weaken and reduce risk factors but also to enhance protective and "promotive" factors.
6) **Subject's Biography:** CTCOs need to be aware of how a Subject's past and present affects their current situation:
   a) Understanding the context and recent past of a Subject is crucial.
   b) Trauma awareness is vital, as is understanding potential 'triggers', when planning interventions.
   c) Documenting and understanding the Subject's complex needs, grievance narratives and engagement factors (at the very least) are vital to 'pitching' any approaches or interventions towards them.
7) **Previous Assessments:** Build on every previous use of the DIF, or VAFs, or Vulnerability Support Hub appraisal / trigger plan, or any other assessment completed around your Subject.
8) **Baseline Beliefs and Behaviours**: try to establish, as far as possible, what they Subject's baseline beliefs and behaviours are, so that escalations and de-escalations in worrying behaviour & activities can be identified more easily.
9) **Specific Considerations:**
   a) Consider your Subject's apparent strengths against their apparent needs. How certain are you around these?
   b) Consider what still needs to be found out, corroborated or explored further. Detail these in a way that is easy for you, or someone else, to refer back to and check.
   c) Describe which vulnerabilities & risk factors you think need to be prioritised, why & in which order.
   d) Every Case priority, every risk and vulnerability, must have an associated action on the CMP, for this consider interventions, support & disruption needs.
   e) Consider the timetable for your proposed interventions – when they will be enacted and when they will be assessed.
   f) Consider who will lead / enact your proposed interventions.
   g) Consider anything that might worsen any risk or vulnerability factors. What are they? Which specific factors might they aggravate & how might they do so?
   h) Consider anything that might help improve any risk or vulnerability factors. What are they? Which specific factors might they help alleviate & how might they do so?
   i) Consider how you will layer your interventions to maximise positive intended outcomes, & minimise negative unintended outcomes. Describe how you will achieve this.

j) Consider how & when you will assess the success or failure of any interventions.

20.0.2 CMPs – Protective Factors (Potential Issues)

1) **Protective Factors:** For a more detailed unpacking of Protective Factors, please refer to the glossary at the end of this document. For our purposes here, a word of caution -
   a) You need to be able to **evidence** and **evaluate** the utility, success or failure of any protective factors (and any disruptive tactics for that matter), in order for them to be useful. If you cannot assess whether an intervention is succeeding or failing in helping to mitigate one of your Case priorities, you should not assume that it is making a difference, or worth the continued time, effort and money put into it.
   b) It is often the Case that the mere existence of something (like supportive parents who are pro-Police & pro-PREVENT) is a protective factor. This is not necessarily the Case. Supportive parents were supportive **before** and **during** the referral of a Subject into PREVENT, so their presence is not necessarily enough to be considered a protective factor by itself. In that circumstance, parents could be described as a **potential** protective factor, if given appropriate advice / support. CTCOs need to be able to unpack how otherwise supportive parents (or anything else) can be empowered to become a measurable protective factor.
   c) Following the implementation of an intervention, different risks and vulnerabilities may escalate, de-escalate, or stay the same. In the Case where one escalates, CTCOs should consider whether other, currently unaddressed, factors may be causing the escalation. Also, a Subject may be responding well to some supportive interventions and may be succeeding at various "healthy" activities, but if there are still **any** escalating or mobilisation factors present, or, depending on their context, potentially any other complex needs, risks or vulnerabilities identified (or not) through the DIF that have not been mitigated through interventions, then these protective factors cannot be regarded as automatically sufficient protection, by themselves, without further evidence of their effectiveness.

20.0.3 CMPs – Introducing Interventions

1) **Interventions:** these are planned approaches by CTCOs and Partners into the lives, circumstances and/or contexts of Subjects within the PLP space of PREVENT
2) In developing the intervention element of any CMP, consideration should be given to:
   a) **Strategic Oversight:** CTCOs needs to co-ordinate and time the use of the tactics, and keep oversight of the complete suite of tactics to ensure they are complimentary.
   b) **Tactical Leads:** whereas the "strategic" lead and owner of the CMP is the CTCO in the Case, it may not be the Case that the "tactical" lead for each intervention or group of interventions will be the CTCO. The most appropriate agency should be selected to lead on the related interventions, providing they feed back to the CTCO.
   c) **Holism:** Using an "holistic" combination of tactics to disrupt a single or multiple elements of the Subject's problematic / extremist / criminal activities or lifestyle. Unless there is an immediate criminal offence to counter, or a public protection / threat to life and limb consideration, do not only consider interventions to stop the immediate concern. Consider whether a specific intervention will detrimentally affect or exacerbate other (potentially more serious) risks, vulnerabilities or needs.
   d) **Partnership:** Engagement with the full range of agencies and Partners who are supporting the intervention plan.
   e) **Information Gathering:** Using each intervention as an opportunity for further information gathering and refreshing the plan.

20.0.4 CMPs – Types of Interventions

1) CTCOs should endeavour to focus their interventions upon **Individuals**, **Institutions** or **Ideologies**, in that order (see the following sections for details). Generally speaking, Interventions can manifest in numerous ways. Here follow some examples of the types of interventions available (though not specific tactics):
   - **a)** **Direct:** involving the direct engagement with the Subject, willingly or otherwise (i.e.: support or disruption).
   - **b)** **Indirect:** involving engagement with a Subject's co-dependents, family, school, Local Authority, medical practitioners, workplaces, or venues used by the Subject, with the intention of influencing the Subject 'by proxy'.
   - **c)** **Voluntary Engagement:** where the Subject provides consent and chooses to engage with the intervention directly.
   - **d)** **Involuntary Engagement:** where there is no consent, or no voluntary engagement, by the Subject, but where the intervention is imposed – such as Criminal Behaviour Orders, which can require engagement with supportive or disruptive interventions.
   - **e)** **Supportive:** these interventions are designed to help Subjects manage, or even mitigate, complex needs and vulnerabilities. They are generally voluntary, but in the Case of some acute issues (e.g. serious mental illness), supportive interventions may sometimes also be imposed and involuntary –such as detentions under the Mental Health Act.
   - **f)** **Disruptive**: Involving actions by Police and Partners designed to **Divert**, **Deter** or **Desist** problematic behaviours in Subjects who are either not suitable for supportive interventions, or who refuse to engage with them, whilst still escalating in risk and/or committing offences whilst in the PREVENT space.
   - **g)** **Deficit-Based Interventions:** aim to reduce certain risk factors by offering protection against behaviour that might compromise Individual well-being. In the PREVENT context, the image of a shield serves to illustrate the point. For example:
     - **i)** Working with family or even court orders to restrict access to extremist webpages or forums could help safeguard some Individuals from grooming, coercion or self-radicalisation towards extremism & terrorism offences.
   - **h)** **Strength-Based Interventions:** aim to promote attitudes and behaviours that empower your Subjects in their environment. In the PREVENT context, this might include:
     - **i)** **Media literacy:** how to identify, assess or even avoid groomers and online exploiters of all kinds, as well as conspiracy theories, propaganda & misinformation.
     - **ii)** **Learning to engage with their concerns confidently:** cultivating 'personal agency', responsibility and constructive expression. So healthy, appropriately critical engagement with political and other social processes within the democratic framework, or within a religious organisation.

20.0.5 CMPs - Interventions: General Goals

1) **Building Resilience:** One of the most fundamental goals in supportive CMP Interventions is the development of individual and communal resilience against radicalisation and extremism. Enhancing positive factors is often even more important minimising negative ones.
   - **a)** Resilience is the ability to 'bounce back' from adversity. Some key points on resilience within PREVENT:
     - **i)** Resilience does not exist by itself necessarily, it needs to be cultivated at different levels of interaction, and an awareness of situational contexts and (family) histories are key,
     - **ii)** It is as much a collective as it is individual endeavour. This is demonstrated by the reactions to terror in cities around the world.
     - **iii)** A Subject may be resilient to some risks but not necessarily to others,
     - **iv)** Resilience is formed at both an individual and a social level,
     - **v)** "Functional", communicative, supportive, law abiding families are one of the strongest buffers against PREVENT issues,
     - **vi)** In diaspora / immigrant communities, resilience tends to be shaped by a combination of home country experiences and the mainstream values of the country of residence.

b) Consider whether your PREVENT Subject has:

i) Individual social support,

ii) A positive "emotional climate",

iii) Stable religious / ideological values,

iv) Existing strategies for coping with adversity,

v) Personal resources for coping with problems effectively,

vi) Educational circumstances that allow for (and promote) autonomy, open-mindedness and the value of success,

c) If your Subject is missing these, what can be done to promote / enable them?

2) **Protect against political alienation**: focus on democratic citizenship.

a) The mechanisms of radicalisation (e.g. propaganda, grooming) are relevant here.

b) How can you help/enable a PREVENT Subjects with grievances to actively engage with and express themselves in a democratic experience through the development of non-violent skills and conflict resolution skills?

3) **Protect against apocalyptic ideology:** offer stable, rounded religious knowledge or other ideological guidance.

a) Identify **Intervention Providers** or other means that can provide benign counter-narratives, internet safeguarding measures, balanced and more nuanced political guidance.

4) **Protect against identity crises:** stimulate personal participation.

a) The ability of an Individual to negotiate or "get their heads around" multiple identities works as a protective factor against cultural / identity crises.

b) Consider how to enable Subjects to truly relate to others, perhaps to "walk a mile in another's shoes", to provide perspective on Subject's identity in relation to others, and to experience and better understand what unites people even through cultural and "cosmetic" physiological differences.

c) Helping the Subject develop coping mechanisms, like anger management or even trauma therapy, both of which help Individuals manage general life adversities.

5) **Protect against the pull of the "extremist milieu":** promote / enable a warm and/or supported family environment.

a) A parenting style that provides warmth whilst also observing rules and provides definitive boundaries is considered the most protective.

b) Family members can be supported with strategies (like awareness-raising or family therapy) which are appropriate for different life stages.

6) **To help develop "character":** cultivate means in your Subject to resist negative influences from negative friendship or kinship, by developing autonomy and self-esteem.

a) A strong sense of self-esteem and self-control / personal agency can render Individuals less susceptible to group dynamics, groomers and extremist religious interpretations.

b) Character development of this kind will also enhance students' grades, social-emotional well-being and life skills.

7) **Protect from feelings of exclusion**: enhance social coping skills.

a) Hate crimes, for example, must obviously be treated as the crimes they are, but the underlying dissatisfaction leading to, or stemming from, hateful identity politics must be addressed and taken seriously.

b) Identify and look for means to mitigate feelings of "social pain" in an increasingly polarised society, and work proactively around the social needs, talents and ideals of your Subjects.

20.0.6 CMPs – Interventions: Individuals

1) PREVENT activities around Individuals include, but are not limited to:

a) Risk & vulnerability assessment of Individuals referred to PREVENT by Partners or the public.

b) Use of the Local Authority led **Channel** programme to support vulnerable Individuals and provide interventions through multi-agency Panels.

c) Use of the PLP process to support vulnerable Individuals who refuse to engage with Channel and provide interventions through multi-agency Panels, and also to disrupt higher risk Individuals who are no suitable for Channel, in order to deter, divert or desist problematic behaviours.

d) Use of **Multi-Agency Extremist Screening Meetings** (**MAESM**) and **Multi-Agency Public Protection Arrangements** (**MAPPA**) processes in conjunction with **NOMS** to identify opportunities for Channel activity with prison releases of Individuals.

e) Consideration regarding the deployment of a CTCO within a PURSUE investigation to identify vulnerabilities and co-ordinate support to the family of Subjects of Interest (SOIs) post-arrest.

f) Identify potential holistic family interventions for Individuals vulnerable to extremist messages.

g) Consider whether interventions with some Individuals the context of anti-firearm, anti-gang or other organised crime reduction initiatives in the CTCOs geographic area.

h) Examination of Individual lifestyles to establish whether there is any criminal activity outside of CT arena.

i) Consider the use of 'Troubled Families' or similar initiatives to support wider family and address potential vulnerabilities.

j) Visits to "Returnees" from conflict areas, potentially in conjunction with the DDP programme.

k) Banning of an Individual from certain premises that are under the control of Statutory Partners, e.g. Local Authority meeting rooms, university halls, etc.

l) Use of non-TACT legislation to prosecute Individuals of justifiable concern to PREVENT and the use of stringent bail conditions to limit association and movement.

m) Briefing of local Police resources to target concerning Individuals using routine Police powers.

n) Safeguarding visits to people who may be intending to travel to areas of conflict, e.g. Syria.

2) Example "Individuals":

a)

b)

I&S

iii) Where Individuals are identified as vulnerable to being drawn into TACT offences, CTCOs can refer them through PREVENT processes and on to Channel, where appropriate.

20.0.7 CMPs – Interventions: Institutions

1) PREVENT activities around Institutions include, but are not limited to:

a) Risk & vulnerability assessment of Individuals referred to PREVENT by Partners or the public.

b) Supporting institutions through providing messaging on specific issues, e.g. facilitation, fund raising.

c) Disruptive intelligence led overt messaging into specific venues.

d) Engagement with key personnel at venues in order to encourage due diligence and to deny access to extremist speakers or to ensure meetings are not closed groups.

e) Consider Local Authority options for disruption if a municipal centre is being used. Work jointly with Local Authority including using planning regulations and licensing conditions.

f) Use of enforcement agencies to undertake visits and disrupt activity, e.g. Environmental Health, HMRC, OFSTED.

g) Maintaining relationships with venues for wider PREVENT opportunities for the future.

h) Identify audience members and assess risk of vulnerable persons being radicalised.

i) Arrange for Charity Commission to support engagement opportunities with key venues to promote safer giving. Consider whether some charities are committing criminal offences in relation to fraud and explore opportunities for criminal investigation.

j) Refer Cases where charitable assets and property are at risk of loss or abuse, or where there are concerns relating to extremist speakers and/or publications, for Charity Commission monitoring inspection visits or other regulatory intervention.

k) Deployment of overt resourcing at institutions of interest at key times to disrupt activity, i.e. timetabling activity to coincide with visits of Individuals at institutions.

2) Example "Institutions":

a)

b)

I&S

20.0.8 CMPs – Interventions: Ideologies

1) PREVENT activities around Ideologies include, but are not limited to:

a) Supporting the dissemination of effective counter-narratives through PREVENT leafleting/messaging bespoke to local context / operation, and within a specific geographical area, e.g.: Syria passport, PKK fundraising, etc..

b) Disrupting the activities of extremist groups through the use of non-TACT legislation such as the Public Order Act 1986 where offences are identified.

c) Disruption of events where extremist narratives are promulgated through supporting local Partners to exercise due diligence in their booking procedures.

d) Supporting initiatives that empower local communities / institutions to directly confront ideologues who espouse extremist narratives.

e) Supporting initiatives that make use of open source material to lawfully undermine an Individual's status within communities in order to erode their extremist credibility.

f) Example "Ideologies":

i)

I&S

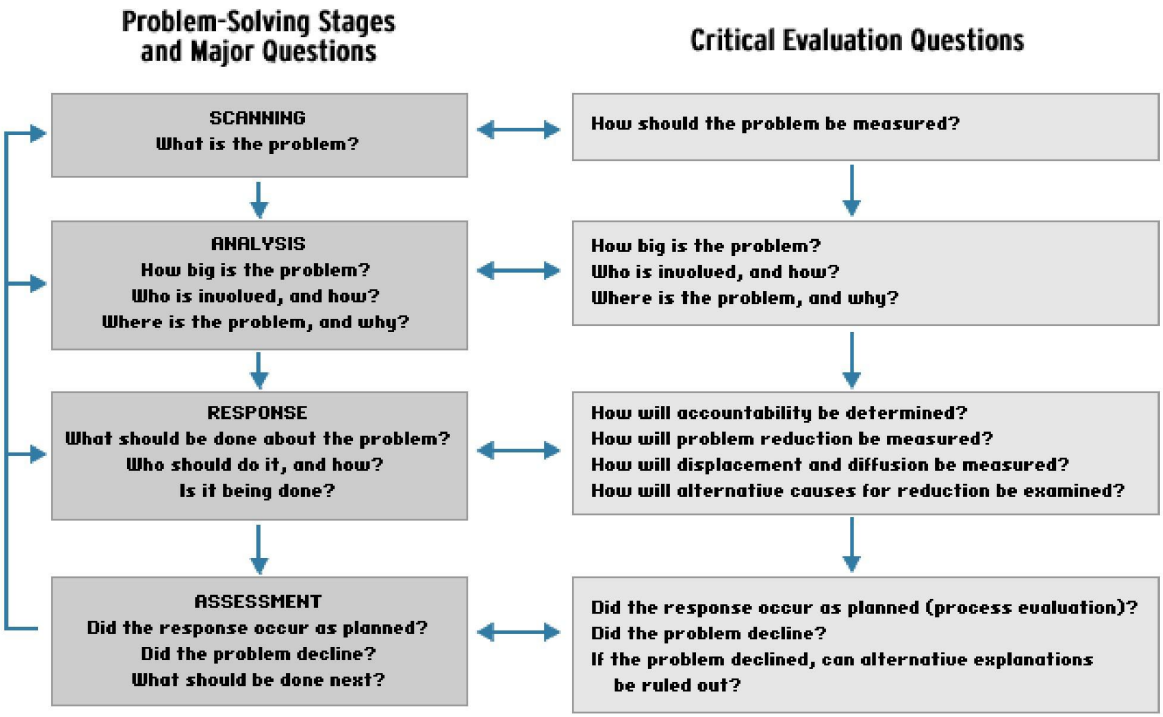
Go to Contents

ii)

iii)

I&S

20.0.9 CMPs – The Problem Solving Approach



20.0.10 CMPs – Tactical Options for Interventions

1) I&S

c) College of Policing: Menu of Tactics.

I&S

i) Despite calling itself a "Disruption Guide", this document contains gamut of possible interventions, disruptive and supportive (including the Channel programme itself), and should be regarded by CTCOs as a supportive and safeguarding guide as well as a disruptive guide.

ii) This is currently our **primary tool** for planning interventions within PREVENT, providing a step-by-step approach to building intervention plans. It should be used as the gateway for CTCOs seeking to formulate interventions within a CMP.

iii) It is shared in common with our PURSUE colleagues, so it provides a high degree of inter-operability and a common parlance for us.

iv) These guides are either available through the CTnet website or are held by your RPC and are available to you upon request.

21 CASE OUTCOMES, CLOSURES, TRANSFERS & REVIEWS

1) Using reduction of risk as the main closure criteria is in line with other developed risk management processes. It ensures that cases are not prematurely closed and focuses on risk reduction and the impact of activity rather than closure after the activity itself (e.g. closing following arrest).
2) Cases within PCM (PLP, Channel and prior to these) can only be closed where:
   a) The Subject is deceased;
   b) There was no actual CT concern;
   c) The Subject could not be located;
   d) The case was escalated to the Pursue space;
   e) There was no actual CT concern however there was a non-CT issue referred onwards.
3) **PLP Cases** can also be closed where:
   a) The risk in the case has decreased to a level where management is no longer necessary to prevent the Subject being drawn into terrorism related activity or the public from harm, i.e.:
      i) It can be demonstrated that the previously-relevant PREVENT issues have been successfully **diverted**, **deterred** or **desisted**, and the Individual is consistently disengaging from involvement with concerning Individuals, Institutions, Ideologies or other extremist or CT-related issues.
   b) With the permission of the Regional PREVENT Co-ordinator, **some** Cases may be closed with PREVENT issues remaining, or some low level CT risk remaining. Such cases must show a clear and detailed justification on PCMT as to why management should not continue and why escalation cannot be undertaken despite Prevent-relevant concerns / CT risk remaining.
4) **Channel Cases** can also be closed where:
   a) The Channel Panel has adequately addressed all CT and Safeguarding concerns.
   b) The Channel Panel (including the CTCO member) has determined that the Subject already has sufficient support in place to address all CT and Safeguarding concerns.
5) **Monitoring:** If it is necessary to observe the Subject for a longer period of time before judging the impact of management on risk then such cases must not be closed. Instead the case must be shown as monitored by changing the priority banding to 'monitored'. The case notes must be updated, a new DIF and CMP completed to show the frequency with which the case will be reviewed.
6) **Reasonable Belief:** Cases closed at the end of the PGA phase as the PGA Decision **must** have a completed and supervised DIF demonstrating a reasonable belief that there are no PREVENT relevant concerns. All relevant activities which have taken place during case management must be selected within the PCMT Actions page and described in detail on the notes page.
7) **Closing DIF:** All cases under Police-led Partnership Management must have a closing DIF completed and supervised at the point of closure.
8) **Closing VAF:** All cases under Channel Management must have a closing VAF completed and supervised at the point of closure.
9) **Closure When Issues Remain:** CTCO Supervisors can authorise case closure for all PLP cases except where a case is closed with an unaddressed CT risk (RPC authority is required for such cases).
10) **Transferring Cases:** In the event of a case transfer between areas, the outgoing force must contact the new force at the point at which the move or potential move first becomes known. The general principle is that cases should be managed where the risk is and the NSIM multi-equity principles should be applied. In cases where a Subject is detained under mental health or immigration legislation in an area outside of their normal place of residence, the relevant areas should discuss the case and decide upon the area must suited to continue management of the case on the basis of risk. Where such cases are under Channel, transfers are not a Police decision and instead sit with the Channel Panel. In such cases Home Office Channel Guidance must be followed. Any case transferring between areas must have an up-to-date DIF/VAF completed at the point of transfer by the outgoing force (with the exception of Dovetail cases in which the LACC will complete an outgoing VAF if appropriate). The receiving force must complete

a new DIF/VAF upon receipt of the case (with the exception of Channel cases in Dovetail area cases) and if it is a PLP case a new Panel should be organised and a new CMP must be completed and supervised reflecting the change in circumstances arising from the move between areas.

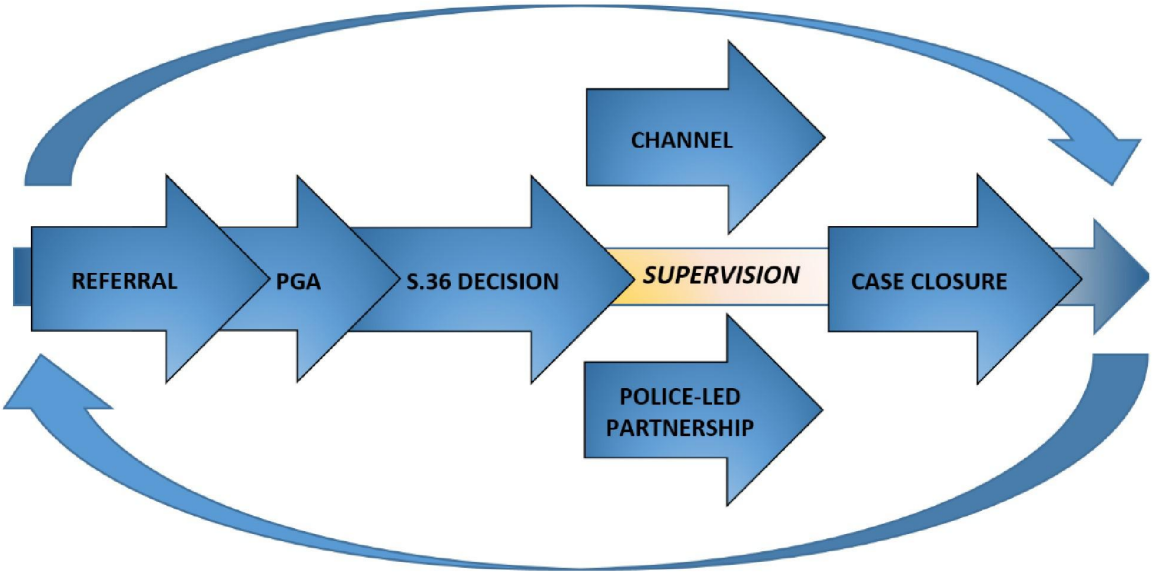
11) **Reviewing Closed Cases:** All cases that have been adopted into the PLP process must be reviewed by the CTCO (and the PLP Panel if one was convened for the Case), and approved by the CTCO Supervisor, at 6 months and 12 months from the point of closure. At the point of closure, it is the responsibility of the CTCO to accurately record the closure on the PCMT to ensure review triggers are flagged at the appropriate time. This review process must be undertaken for all PCM Cases adopted by PLP. This includes those PLP cases that are adopted but are subsequently referred elsewhere. The review process should be informed by relevant information from PLP Partners to Police intelligence systems. Reviews should be completed within five working days of the request being made and should include Police checks, change of circumstances, current social care involvement, any concerns since case closure and contact with the Initial Referrer and/or the last person or organisation that handled the referral prior to in arriving with CTP PREVENT. The review should either be set as a flag for 6 and 12 months to the CTCO / Supervisor on the PCMT (if the functionality has been built in for this), or in a calendar notification. One way or another, details should be recorded in the relevant case on the PCMT.

12) **Exit Reviews:** Police should strive to improve their practice and effectiveness in reducing terrorism vulnerability and tailoring support plans to needs identified in the vulnerability assessment. To enable CTP PREVENT to gain greater insight into practice, consideration should be given to capturing the experience of individuals exiting PCM which could be used to highlight good practice or areas requiring improvement.

13) **Sharing Good Practice**: Police and Local Authorities may find it useful to form regional Channel chair networks to facilitate the sharing of good practice in running Channel and PLP Panels. These networks should come together to share best practice, discuss case studies and provide mutual support and advice. This can be a useful resource for those local authority areas that have few Channel or PLP cases, in order to learn from more experienced areas, or for new Channel and PLP Chairs to observe practice. PLP Panel chairs also endeavour to attend regular national forums to share good practice more widely.

22 INTELLIGENCE CYCLE

1) The basic flow of the information management process and how they fit together



2) **IMUs & FIMUs:**

a) IMUs are the only part of the CTP Network who have the potential to see the whole intelligence picture. It is essential that intelligence obtained through the PREVENT Case Management methodology is passed back to a FIMU to allow for proper assessment of any risk/threat and identification of escalation of risk. CTP PREVENT across the entirety of the UK network will be engaging predominantly with Fixed Intelligence Management Units (FIMUs) but on some occasions may also be working alongside OIMUs (Operations Intelligence Management Units).

b) FIMUs must be informed of any significant changes in risk to a case or the case Subject throughout its lifetime in PCM. This could include potential escalations in risk or threat around any CT issues, (e.g.: concerning behaviours or contexts) within the case, or it could be the discovery of hitherto unknown contacts, addresses or phone numbers associated with the PREVENT Subject that one might reasonably suspect could be relevant to wider CT picture held by a FIMU. This sort of information could arise at any point within PCM, but specific junctures to consider are: reception of the Referral, the PGA phase, the S.36 decision after further information gathering, during Channel or PLP, and at the point of Case Closure.

3) **Relevant Updates:**

a) All biographical information obtained on a Subject or associates during the PREVENT process must be submitted to the FIMU

b) Any intelligence, which either does, or has the potential to change the DIF assessment, Case Management Plan or VAF must be submitted to a FIMU, this includes intelligence obtained through attendance at a Channel Panel or other partnership interaction as well as DIF or VAF assessments. It must be made clear on the intelligence submitted whether the risk in the case is escalating, de-escalating or remaining static. This must be undertaken for both PLP and Channel cases.

4) **Intelligence in Channel:**

a) For Channel cases, all relevant intelligence necessary for the effective management of risk must be shared with the Channel Panel and Chair.

5) **Flags:**

a)

I&S

I&S

I&S All decisions must err on the side of caution, as PREVENT should not show on any background checks they may be subjected to as part of their work or daily lives. Consideration and decision must be recorded on the PCMT.

6) **Interventions & Interviews:**

   a) All encounters between the Subject under management and Police / Partners must be assessed by the CTCO and any relevant intelligence reviewed and, if appropriate, submitted to a FIMU (e.g. missing person reports, crime reports etc.).

7) **Sharing Intelligence Between Police Forces:**

   a) All PREVENT teams must have access (directly or via FIMUs or Force Intelligence Units) to the Police National Database (PND) to allow regular checks with other UK Police Forces to see if Subjects have come to notice elsewhere in the country. Where necessary, the CTCO must make further enquiries in relation to crime investigations, missing person enquiries or other non-CT policing incidents in order to ensure they have a full understanding of the relevant incident, including any intelligence products that have been generated (e.g. cell site data, phone downloads etc.). Any intelligence received or generated which is relevant or potentially relevant to another force must be transferred to them through the local force transfer process (e.g. an intelligence report marked up as suitable for dissemination to another area).

8) **Travel Risks:**

   a) For any Subjects who show a propensity to travel to areas of conflict or who are juveniles, consideration must be given to requesting CTP-POC create a Police Intelligence Watchlist (PIW) entry. Where a PIW request is made CTCOs must ensure that both CMISv2 (where appropriate) and PCMT records clearly articulate the travel risks and any other relevant information staff at ports may require in order to make a decision under schedule 7 of the Terrorism Act 2000 or other relevant legislation.

9) **Minimum Updates:**

   a) If no other submissions have been made to a FIMU then an up to date summary should be submitted to the FIMU every 3 months. Regions or Forces may decide for themselves, in conjunction with their FIMUs, how best to pass this information across. However, best practice is that it is done in writing, perhaps as an intelligence report, in a manner that can be audited if necessary.

ANNEX 1: COMPLETING THE DIF

1) In this section unpacks in greater detail at the specific considerations, questions and advice that make up the body of the DIF.

SUMMARISING THE ISSUE

1) *Extract & bullet-point the relevant details & concerns from the initial referral & any subsequent inquiries. Clearly summarise the reasons this Case was referred to PREVENT.*

- **a)** These are the general points around the Case. This section is filled in at the PGA step & not usually added to once the Gateway Assessment is completed.
- **b)** Subsequent assessments using the DIF that are uploaded onto the PCMT for Cases in the PLP space *may* include updated Summaries, at the discretion of the CTCO and/or CTCO Supervisor.
- **c)** Within the **Summarise the Issue** box, CTCOs needs to summarise, preferably in clear bullet-points:
  - **i)** What the initial-referrer's concerns were,
  - **ii)** Relevant generalities added by the FIMU in the handover to CTCOs,
  - **iii)** Relevant generalities discovered through contacting the Initial Referrer and/or the last person or organisation that handled the referral prior to in arriving with CTP PREVENT,
  - **iv)** Relevant generalities discovered through the various other mandatory & recommended checks completed.
- **d)** Note that the specific, granular detail of any issues, risks & circumstances are unpacked in the subsequent DIF boxes.

COMPLEX NEEDS & VULNERABILITIES

1) *Identify, clarify & wherever possible corroborate any needs or vulnerabilities associated with the Subject. Detail & refer any MH concerns or diagnoses to your Vulnerability Support Hub.*

- **a)** Here CTCOs need to consider whether there is there anything in the Subject's life that might be affecting their wellbeing or that might be increasing their vulnerability in any sense? Consider existing needs & vulnerabilities **as Subjects enter Prevent**, & any that **develop after** that point:
  - **i)** **Mental Health Issues:** Mental ill health and disorders can increase an Individual's vulnerability towards being targeted by groomers, or being coerced towards terrorism offences, or (in some contexts) self-radicalised towards extremism. Identifying mental health issues is crucial to planning successful support & interventions plans.
  - **ii)** Do not let a potential MH issue slip through the net. CTCOs must detail diagnoses for MH issues. Also, comments from people close to the Subject around their MH may be relevant, as might your own observations be around the Subject's MH. Clearly identify formal **diagnoses** & **evidenced facts** vs. **comments** from others & your own **observations**.
    - **(1)** **Autistic Spectrum Disorder** (**ASD**): research around radicalised people with ASD (particularly by the Radicalisation Awareness Network, **RAN)**, discovered that certain characteristics can make people with ASD more vulnerable to radicalisation & violent extremism in the "right" context. For example, they may be deliberately targeted & influenced by recruiters / groomers of extremist groups, or they may have other vulnerabilities & grievances connected to the condition in their context. However, traits of ASD can be either a **risk** or a **protective** factor depending on the Individual & their unique circumstances. Considering which traits are more prominent in the Individual will assist CTCOs in making a more accurate assessment & effective Case-management plan, hence the need for more expert input from the Vulnerability Support Hubs & MH practitioners in the Local Authority.
    - **(2)** **Psychotic Disorders:** Managing Individuals with psychotic disorders & borderline personality disorders may require medicinal treatments, the identification and prescription of which being things that Police cannot (and should not) be involved with. This emphasises the importance of seeking input from appropriately qualified & experienced MH

practitioners for Case-management planning. Although it is certainly not always the Case, "radicalisation" *can* in some Cases be a symptom (or expression) of psychosis, delusion, or pathologically narcissistic & predatory behaviours. The most important protective factor for PREVENT Individuals diagnosed with these sorts of conditions is access to appropriate healthcare services.

iii) Consider demographic or personal factors that you believe are *unlikely* to be changed through interventions **within the timeframe of most Cases** (i.e.: "static" factors). These can include:

(1) Child – 17 years old or younger.

(2) Disability – as per the 2010 Equality Act, S.6.

(3) Chronic or Potentially Terminal Illness. Consider whether the Subject suffers from an illness that in their context might suggest a vulnerability to exploitation, (bribery, blackmail, coercion or grooming), or that might aggravate an existing grievance narrative or engagement factor, or that may create a sense of having nothing at all to lose / live for.

(4) Mental Capacity – with respect to issues such as developmental impairments. This is a broad term & such impairments are not always or necessarily relevant in terms of "radicalisation". However we do not want to arbitrarily limit the scope of vulnerability assessments within their unique contexts, e.g.: consider mental capacity in the context of vulnerability to coercion, grooming & exploitation. See the Mental Capacity Act 2005, S.2 (1-4).

(5) Severe or Long-Term Mental Illness or Disorders – diagnoses involving antisocial personality disorders (e.g.: psychopaths & sociopaths), other personality disorders, schizophrenia, or paranoid or psychotic disorders, bipolar disorders, schizoaffective disorders or other severe mental illnesses. If Subjects with any of these conditions remain within Prevent, then wherever possible the **VS Hubs** (& any previously assigned MH Case workers) should play a significant role in advising upon the Subject's management.

iv) Consider matters around the Subject's emotions & personal circumstances, which *may* be changeable through interventions **within the timeframe of most Cases** (i.e.: "dynamic" factors). For example, we obviously cannot change a bereavement, or the fact that a Subject has already been a victim of crime, but it may be able to offer support around grief or other issues. Consider:

(1) Educational Issues.

(2) Effects of Child Abuse.

(3) Bereavement or Depression. Note that whether depression may be changeable within the lifetime of a Case may be dependent upon whether the depression is strictly 'situational' or part of a broader or more profound MH problem.

(4) Effected by Violence or Hate Crime.

(5) Divorce / Break-Up / Child Access Difficulties.

(6) Self-Harm, Self-Destructive or Suicidal Tendencies. Subjects who have self-harmed or who have suicidal tendencies should be considered very carefully by CTCOs, particularly around the potential of commit "suicide by Police".

(7) Financial Problems / Housing Issues / Unemployment.

(8) Substance Misuse or Dependence[19], or Problem Gambling.

(9) Stated / Diagnosed Sleep Problems, Insomnia, or Exhaustion.

(10) Deprivation of Citizenship / Asylum Seeker / Refugee / Deportation Order.

[19] Drug Misuse & Dependence: UK Guidelines on Clinical Management, 2007, London: Department of Health (England), the Scottish Government, Welsh Assembly Government & Northern Ireland Executive. Viewable at the following address: http://webarchive.nationalarchives.gov.uk/20170807160700/http://www.nta.nhs.uk/uploads/clinical_guidelines_2007.pdf (last accessed 21/05/2019).

(11) Being Bullied / Isolated / Neglected / Abused [20], both children & vulnerable adults.

(12) Mental Capacity – with respect to activities or circumstances that may lead a Subject to lose capacity for a specific period, (perhaps due to substance misuse, etc.), but which may be alterable through interventions. See the Mental Capacity Act 2005, S.2 (1-4).

(13) PTSD & Hypervigilance – particularly if the Subject is a war veteran, refugee or asylum seeker. Any contact with an active warzone should be considered in this context. **NB:** As PTSD symptoms can take months or even years to manifest, always err on the side of caution where there is any doubt.

(14) Any other indicator not mentioned above, e.g.: "mental health" is a broad area, see Mind's List of MH issues.

GRIEVANCE NARRATIVES

1) *Describe any political, racial, religious or single-issue grievance narratives articulated by, or associated with, the Subject, & their contexts.*

a) Here CTCOs should consider whether the Subject has actually articulated a **grievance narrative** of any sort to anyone.

b) Think along the lines of **race**, **religion**, **politics,** or other single-issue ideological or identity-based causes (like **LASIT**, **XRW**, "**Involuntary Celibate**" (**InCel**), "**Identitarian"**, **Animal Liberation** or "**class-war**" movements, etc.).

c) Grievance narratives can be real or perceived & could include:

i) **Personal Grievances**: victim of hate incidents or other direct bigotry around protected characteristics; acute personal anger towards authorities over an issue – perhaps they feel ignored over something they deem vitally important; family or friends directly affected by armed conflicts; seeking personal redemption or revenge; acutely personal feelings of social, political or religious alienation, marginalisation or discrimination.

ii) **Vicarious, Group & Hyperbolic Grievances:** righteous indignation or resentment over a racial, religious, political or other ideological cause; fixation upon one or more conspiracy theories; acute dissatisfaction stemming from polarised "them & us" identity politics; vicariously personalising distant social issues that otherwise have no direct affect upon the Subject; the idea that an any particular racial, religious, political or other ideological cause needs to be forcefully imposed upon a specific region or people "for their own good"; entrenched victimisation or persecution narratives involving any territory, or a racial, religious, political or other ideological cause, etc..

iii) **Threat Grievances:** these can include perceptions that Subjects or their loved-ones face imminent or direct threats to life or safety of any kind, which only drastic or violent action can resolve.

d) Do any of these seem to apply in this Case? Which? How long for? Do these feelings seem to be escalating?

e) Please describe anything else you think might be relevant in terms of grievance.

ENGAGEMENT FACTORS, INDICATORS & DRIVERS

1) *Describe any other suspected reasons, motivations or "push & pull" factors or indicators that may be having an effect on the Subject in relation to suspected CT or extremism issues.*

a) Here, CTCOs should describe any potential **engagement** factors or indicators that may be present.

b) Note that some of these, by themselves, do not automatically lead to terrorism offences & should not be considered **in isolation** as evidence of someone being drawn into terrorism. If this were the Case, practically every pubescent teenager who is in a transitional time of life, seeking excitement & adventure, who is naïve & rebelling against authority figures would be eligible for PREVENT. Obviously this is not the Case.

[20] The deliberate or negligent disruption of a person's wellbeing, as provided within the Care & Support statutory guidance, 2014 Care Act.

c) The indicators & factors presented below can be considered as "aggravating factors" upon which extremists, proscribed organisations & toxic movements designed to draw in the disenfranchised, the frightened, or the angry, tailor their approaches to groom new or potential members. So engagement factors & indicators can be considered the underlying vulnerabilities, or potential "push & pull" factors, motivations or "psychological hooks", for any interest or involvement in extremism or terrorism. Consider:

- **i)** Chaotic, transitional or critical times of life.
- **ii)** A belligerent sense of self-entitlement; acute narcissism.
- **iii)** Feeling coerced / blackmailed / controlled by extremists.
- **iv)** Desire for excitement & adventure; a chance at heroism.
- **v)** A need to dominate or control others; opportunistic gain.
- **vi)** Hateful essentialist identity politics; militant or apocalyptic ideological beliefs.
- **vii)** Youthful rebellion, impressionability, naïveté, & vulnerabilities that 'aid' grooming.
- **viii)** Disillusionment with mainstream protest as a means of producing political or social change.
- **ix)** Low self-esteem or a strong need for identity, meaning or belonging; desire for status or significance.
- **x)** Loyalty or duty; family, friends, or community involvement in extremism or support for extremist behaviour.

d) Please describe anything else you think might be relevant in terms of engagement.

IDEOLOGICAL CONCERNS

1) *Describe any extremist causes, ideas or beliefs expressed by the Subject or associated with the Case (identify which). Consider all religious, racial, political or other single-issue extremist ideologies, movements & causes.*

a) Here CTCOs should consider & describe the Subject's exposure to, interest in, or fixation upon, any extremist ideology or causes. Bear in mind that Subjects do not have to be "true" or fanatical believers of such an ideology in order to be vulnerable to it. Consider:

- **i)** Is there an ideology associated with the Case? What is it? Does its expression seem largely **benign** or **concerning** in the context? Please describe.
- **ii)** Consider extremist imagery or material at home or other regularly-attended places.
- **iii)** Consider age inappropriate or particularly sympathetic knowledge of an extremist ideology.
- **iv)** Consider vocal support for any public activities where unlawful extremist conduct or hate are involved.
- **v)** Personally espousing / actively promoting hateful ideas or an extremist ideology, particularly if presented in an uncompromising, absolutist or "scripted" manner.
- **vi)** Consuming or sharing propaganda material produced by (or for) proscribed organisations, or hate speeches or extremist or graphically violent content of any kind?
- **vii)** Has the Subject shown approval for, or defended, extreme violence, TACT offences, "jihad", "martyrdom", riots, political assassinations or unlawful militia-style operations of any kind, at home or abroad? Please describe.
- **viii)** If there is no clear **extremist** ideology around the Case, describe any ideas articulated around **Religious**, **Racial**, **Political** or **Single-Issue** causes that would fall into our working definition of extremism. **NB:** Single-issue ideologies may sometimes seem indistinguishable from grievances & conspiracy theories – **Involuntary Celibates** (**InCel**) or the "**Great Replacement**".
- **ix)** If the Subject claims an extremist ideology, does it seem generally consistent, or does it seem conflicted or changeable? Does the Subject shift between extremist ideologies, such as an interest in Nazism one month, then Militant Jihadism the next? If so, bear in mind that a conflicted or rapidly shifting interest between different extremist ideologies or movements is still relevant to PREVENT.

x) A concerning fascination in the tactics or terrorism, mass-killings or school massacres *per-se*, in the absence of a unifying ideology or narrative reason for this interest, ***may*** also be indicative of a Subject who requires support through PREVENT. The context needs to be explored around this interest, as, for example, an obsession like this combined with multiple/acute complex needs or grievances might be suggestive of a higher risk Subject. Explore & explain the circumstances.

b) Please describe anything else you think might be relevant in terms of extremist ideologies.

INDIVIDUALS, GROUPS & INSTITUTIONS OF CONCERN TO PREVENT

1) *Has the Subject been exposed to any extremist Individuals, groups or institutions, or shown a desire to associate with any of these?*

a) Consider all known contacts & relationships, particularly any identified as a concern in the referral, & which of them might pose the greatest risk of negatively influencing, grooming or coercing the Subject.

b) Pay particular attention to the type & extent of the Subject's exposure to the **Individuals**, **groups** or **institutions** in question:

i) Has the Subject been exposed to extremist Individuals, groups or institutions? Which? When? How frequently?

ii) Has the Subject leaked membership, or a desire for membership, in a proscribed organisation? How? When? Which groups? What was said? Does it seem credible?

iii) Has the Subject leaked personal support for, or a fixation upon, a proscribed organisation, extremists or terrorists, contemporary or historical? How? When? Which groups? What was said?

c) Please describe anything else you think might be relevant in terms of exposure, engagement, Mobilisation Identity or fixation concerning Individuals or institutions.

CAPABILITY TO OFFEND OR CAUSE HARM

1) *Describe anything suggesting the Subject has (or **believes** they have) relevant capabilities, physical or psychological.*

a) Here CTCOs need to consider whether there is anything to suggest that the Subject might have the **capability** to commit, or deliberately enable, terrorism offences?

b) Think about how the Subject's self-perception might influence his/her psychological capability to commit such offences (e.g.: "even though I have no training, I still see myself as a soldier in a war"). When it comes to terrorism it is not only what a Subject has directly **trained** to do or has direct experience of doing, but what Subjects **believe** themselves **capable of doing** that also matters. Consider:

i) Connections to extremist, terrorist or criminal networks, funding or equipment.

ii) A history of notably high risk or dangerous behaviour, or a persistent use of violence to solve problems.

iii) Arrests, cautions or charges for predatory violence (including domestic violence), or any other relevant offences (see below).

iv) Does the Subject seem to **believe** he/she has the relevant skills & capabilities to commit TACT offences, even if there is little tangible evidence to suggest these skills or capabilities are present in real terms?

v) Individual knowledge, skills & competencies that may be useful towards the commission of any TACT offences, (such as military training, combat experience or membership in a criminal gang/organisation), or a previously demonstrated willingness to PURSUE any such knowledge, skills & competencies.

vi) Please describe anything else you think might be relevant to a Subject's physical or psychological capabilities.

c) **RELEVANT OFFENCES:** It is important to take note of the **nature**, **dates** & **frequency** of any relevant offences (& ASB). This can help establish possible, intent, capabilities & baseline behaviour. **Convictions** for relevant offences *may* increase risk even further, reflecting a Subject's confirmed ability to commit such offences & also the possibility that a conviction might create or exacerbate a grievance narrative. Consider the following:

i) Hate offences.

ii) **Terrorism offences** & offences involving **serious** or **persistent violence**.

iii) **Predatory offending** – premeditated violent offences or targeted ASB where **malice of forethought** was associated with the *intent*, *planning* or *execution*.

iv) ASB or offences that involved "sadistic" behaviour, or deliberate hate or "othering" behaviour, e.g.:

(1) Deliberate & extreme cruelty towards any people or animals,

(2) The deliberate identification & dehumanisation of "out-groups", e.g.: referring to them as "scum", "evil", "kafir", "insects", "monsters", "slaves", "infidels", "vermin", "animals", "beasts" etc., or by any deliberately abusive racial or other hateful epithets.

v) **Gang Membership –** obviously for gangs already involved in extremism, but also:

(1) If membership resulted in violence offences, particularly any weapon offences, or acute & deliberate ASB, or other serious & organised criminality.

(2) Gang members may also have increased vulnerability in terms of their ages, abusive or coercive relationships, drugs misuse or dependence, or mental health problems (including, in severe Cases, PTSD & Hypervigilance).

vi) **Court Martials** – involving **charges** for any relevant offences mentioned in this section, or any **investigation** for offences detailed within:

(1) The Geneva Conventions Act 1957.

(2) The International Criminal Court Act 2001.

(3) The Criminal Justice Act 1988, S.134, Torture.

vii) **Paraphilia / Extreme Sexual Deviance** – depending on the Subject's **context** & **circumstances**, any of the following could be indicative of a pattern of dehumanising behaviour on the Subject's part, or may leave Subjects open to blackmail or coercion, or help feed narratives that the Subject needs to take drastic action to become "clean" again, or may indicate a predatory and dehumanising mindset. Pay close attention to Subjects with a particular interest in, or direct physical involvement in:

(1) Bestiality.

(2) Paedophilia / child sexual exploitation.

(3) Pre-meditated and/or "stranger" rape.

(4) Physically violent sexual assaults of any kind.

(5) Long-term or habitual sex-offending of any kind.

viii) Other examples of relevant offences **may** include, depending upon the details of the Case & the Subject's context:

(1) FGM; honour-based violence.

(2) Charity fraud; money laundering.

(3) Aggravated burglary; armed robbery.

(4) Domestic violence; frequent / habitual violence offences.

(5) Stalking; trespassing with intent to commit sexual offences.

(6) Genuine 'threats-to-kill'; wounding or GBH w/intent; arson w/intent to endanger life; murder & attempted murder.

(7) Offences involving the possession / use of explosives; noxious materials; firearms; or any other offensive weapons.

(8) Modern slavery, servitude & forced or compulsory labour; kidnap & attempted kidnap; immigration offences; human trafficking w/intent.

(9) CTCOs need to bring a critical eye & draw upon their experience with law-enforcement & advice from the VS Hubs to help assess such offences within the CT context of the Case at hand. As a general guideline, if the CT context /

PREVENT concern is deemed genuine (even if far 'upstream' of TACT offences), then any such offending as listed above should be viewed as potentially relevant & aggravating to the risk posed by the Subject.

INTENT TO COMMIT OFFENCES OR CAUSE HARM

1) *Describe any relevant intent factors or indicators towards an "out-group".*

- **a)** Here CTCOs need to consider whether there is anything to suggest that the Subject might have the **intent** to commit (or deliberately enable) any unlawful extremist conduct or TACT offences? For example:
  - **i)** Has the Subject identified a personally hated or enraging political, religious or racial "out-group"?
  - **ii)** Has the Subject had fantasies (or made notes) about committing murder or mass-killings?
  - **iii)** Attitudes that seek to justify or defend **anyone** committing relevant offences against any "out-group".
  - **iv)** Previous membership or desired membership in a proscribed organisation – the stated intentions of that organisation may also prove to be the unspoken intent of the Subject.
  - **v)** Has the Subject shown a particular fascination (openly or in private) with mass-killings (e.g.: school massacres) or terrorist attacks, or the tactics used in them? This could include an obsession with the attackers / terrorists themselves. Consider the wider context of this fascination in relation to the Subject's baseline behaviours.
  - **vi)** Using explicitly threatening, dehumanising or demonising language towards an "out-group". For example, using terms like "scum", "insects", kafir / kuffar, "slaves", "infidels", "vermin", "animals", or any deliberately hateful or racist epithets.
  - **vii)** Expressed harmful "ends justify means" rationales. For example:
    - **(1)** The Subject believes that direct, illegal and/or violent action must be taken against a perceived "out-group" in order to stop a threat the Subject believes this group poses.
    - **(2)** If the Subject believes that "punishing" or hurting this group will end their perceived threat, then any means employed to do so **may** become justified to their minds, potentially including violence & murder.
- **b)** Please describe anything else you think might be relevant to a Subject's intent.

OPPORTUNITY TO OFFEND OR CAUSE HARM

1) *Describe any potential opportunities that the Subject has, or appears to be seeking, in relation to planning or committing any terrorism offences.*

- **a)** Here CTCOs should consider whether there is anything to suggest that the Subject might **have** the opportunity, or might be **seeking** the opportunity, to commit (or deliberately enable) TACT offences.
- **b)** Consider:
  - **i)** Secretiveness or acute evasiveness that family, friends, teachers or close colleagues find worrying. What specifically? Who has the concerns & why? Do they involve:
    - **(1)** New & unknown "friends" or "hobbies"? Who, or doing what? Where?
    - **(2)** Suspicious travel plans? Are they sudden, unexplained or out-of-character? Why & how-so? Travelling to where? With whom?
    - **(3)** New or multiple phones or SIM cards? What are they for? Has the Subject intentionally destroyed any of these? Why? Where did the phones / SIMs come from? Do we know their numbers?
  - **ii)** Has the Subject gone "missing" or disappeared for periods of time, without corroborated & benign explanations about where they were, who they were with, & for what reasons? When? How frequently? What are the issues with finding out the details?

iii) Short of actual hostile reconnaissance, has the Subject an apparent interest in potential terrorism targets? Think about places or people towards whom the Subject seems to have an inexplicable, or hateful, or obsessive interest, particularly if the Subject has uninhibited or regular access to the object of this interest

iv) Does the Subject have a place where he/she can act completely unhindered or unobserved by authorities or by socially responsible friends, family or colleagues? Where is it? What happens there? Does anyone else frequent that place? Consider "safe-spaces" (e.g.: a lockable bedroom or shed) or another "secret" place where the Subject can PURSUE or prepare for any concerning activities, with no oversight or interference.

c) Please describe anything else you think might be relevant to a Subject's opportunity.

INTERNET & SOCIAL MEDIA "LEAKAGE"

1) *Describe anything concerning about the Subject's mobile phone, direct messaging, social media or online activities, e.g.: Viewing or posting extremist or hateful content? Any returns from Police open-source checks?*

a) Here CTCOs need to consider whether a Subject's social media or online activities seem concerning or fixated in any Prevent-relevant sense, or whether anything PREVENT-relevant has been unintentionally "leaked" online.

b) Consider:

i) The Subject viewing or downloading extreme or "real" & very graphic violent imagery.

ii) Social media / direct messaging applications with extremist people or groups. Consider any returns you may have received around open-source Police checks.

iii) Suspicious, closed or secret Facebook groups (or similar). What is their content / purpose?

iv) Blogs, chatrooms or posts (political, religious, criminal, hate or extremist). What was written?

v) Accessing the 'Dark Web' or suspicious password-protected websites? Which? How frequently? Why?

vi) Does the Subject have online friendships with concerning Individuals or groups? How many? With whom? Is it possible to establish the extent of this "friendship"?

vii) Generating his/her own online extremist material on Facebook, Twitter, YouTube, Instagram, Pinterest, Tumblr, etc..

viii) Self-generated material should be regarded as potentially even more urgent if the Subject uses **imperative** or **absolutist** language in relation taking direct, violent or illegal action around any religious, political, racial or single-issue ideological causes, i.e.: "this **must** happen / this **needs** to happen", "we **have** to do this", "there's **no other option**", rather than using softer, more general "shoulds", "coulds" & "it would be better if..." terms.

c) Please describe anything else you think might be relevant in the context of suspicious internet use & social media leakage.

SUSPICIOUS TRAVEL OR DESTINATIONS

1) *Describe any concerns in relation to actual or planned suspicious travel, or travel to suspicious destinations, by the Subject or someone close to the Subject, whether by choice or coercion.*

a) Travel to suspicious destinations has been a very prominent issue for the UK CT community. We have seen UK citizens leaving for warzones to fight, both on the as part of a proscribed organisation that they have joined, or in order to fight against such organisations, but yet still illegally by national & international law.

b) This is often aggravated further by the fact that many such travellers have either been children themselves, or taking children with them, which has raised a host of constituent safeguarding concerns for the PREVENT network.

c) As such, CTCOs need to consider any proposed, planned or suspected travel by Subjects towards:

i) Active warzones of any kind.

ii) Any region in the world where there is a **significant** likelihood of **direct** (particularly if it is also unlawful) contact between Subjects & terrorists and/or proscribed organisations.

d) Known 'gateway hubs' to either of the above (Turkey is a current example).

e) You should ascertain whether the Subject has:

i) Expressed desires to travel to a suspicious destination? Why, when & in what context?

ii) Planned / attempted to take / send any other person to one? Why, when & in what context?

iii) Planned / attempted to leave for one or arrived to the UK from one? Why, when & in what context?

iv) Actually visited one for an extended period or on multiple occasions, but without providing a reasonable explanation as to why?

f) Are / were a Subject's travel arrangements suspicious in themselves? Consider:

i) One-way tickets or tickets altered at the very last moment in suspicious circumstances. Please describe.

ii) Applications for new passports in suspicious circumstances or claims of "lost" passports. What are the contexts?

iii) Using a travel agencies "of interest" to authorities for fraud, trafficking, unlawful extremist conduct or TACT offences? Which agencies & what offences or conduct?

iv) Is the Subject acutely evasive or seemingly unable to answer simple questions whilst discussing his/her travel itinerary to (or around) suspicious destinations? Please describe.

g) Please describe anything else you think might be relevant in the context of potentially suspicious travel.

PREMISES OF INTEREST OR CONCERN

1) *Describe any connections the Subject may have to premises linked to hate crimes, extremism, terrorism, charity fraud, or that have hosted or accommodated concerning Individuals or groups.*

a) Bearing in mind that past exposure to extremism, proscribed organisations & TACT offenders can leave their marks on a Subject's psychology, where possible (and proportionate) CTCOs should consider where the Subject has lived (or has been frequently associated with) in the last 3 years.

i) Have any of these places been connected with any premises linked to extremism or TACT offences, or that have hosted, accommodated or frequently attracted terrorists, SOIs, RSOIs, PCMT Subjects, proscribed organisations, extremists (domestic or foreign), or hate speakers / preachers?

(1) When was the Subject linked to such premises? In what ways were the premises linked to these issues? Is the Subject **still** connected to any of these premises?

ii) Have any premises connected to this Case **produced**, **promoted**, **permitted** or **disseminated**:

(1) Hate speech, extremist material, or serious & graphic violent material of any kind?

(2) Propaganda material produced by or for proscribed organisations?

iii) If you have a positive answer to any of the above, please give as much detail as possible about the premises as may be relevant. Are they:

(1) Abandoned / empty / derelict?

(2) A venue for sport or personal training?

(3) Owned / controlled by a registered charity?

(4) A healthcare provider or an educational establishment?

(5) A residence or accommodation / living quarters for anyone?

(6) Premises intended for any commercial, business or retail purposes?

(7) A premises of any kind that is rented or hired out for events / conventions?

(8) Private or rented, or used for State / public / council / religious / community / social / cultural / political / governmental / military nature? Please describe.

b) Please describe anything else you think might be relevant or useful to know in relation to premises connected to this Case & the possibility / necessity for interventions.

ESCALATIONS, TRIGGERS & WARNING BEHAVIOURS

1) *Describe possible escalations in the Subject's behaviour from their baseline norm. Has their behaviour or context worsened? Consider possible "**tipping points**" & "**triggers**" specific to the Subject.*

a) **I&S**

b) They are the possible "tipping points", so any changes significant to a concerning Subject with existing PREVENT-relevant risk or vulnerability factors or indicators, which may prompt a move from general stability towards mobilisation behaviours.

c) Depending on your professional assessment of their context & the concerns around them, they could include the very rapid onset of **any factor or indicator mentioned previously**, escalating dramatically from the Subject's baseline norm.

d) More specifically, consider the following:

i) Has the Subject been started harassing or stalking a potential target?

ii) Has there been a sudden shift in vulnerability for the Subject? This should be considered for its potential to escalate other risk indicators, or even become a trigger. Consider potentially **any** detrimental or very dramatic shift in a Subject's personal or professional life.

iii) Has the Subject leaked anything about new or current attempts to become a **member** in a proscribed organisation? Which one? What was said? When was it said? In what context? To whom?

iv) Has the Subject started collecting money for a cause of unknown or suspicious provenance? For whom or what? Why is it suspicious? Can this be corroborated?

v) Has the Subject's threatening or extremist behaviour recently shown a noticeable burst of energy, or sudden, new or dramatically escalated frequency, fixation or pathology? What happened? What do you think is the cause, the wider context & the impact?

vi) Has the Subject drawn up an obvious "hit-list" or "hate-list" of perceived enemies, or at "attack plan" on a particular premises / area? This could be more of a Mobilisation behaviour if the people or area concerned are actually known to (or accessed by) the Subject, so examine the context of such a list.

vii) Has the Subject suddenly taken up intensive physical training in self-defence or martial arts, or weight training / bodybuilding where there was no interest previously? Why? With whom? Where? What's the motivation? Does this relate to a growing "warrior" / "pseudo-commando" self-identification?

viii) Has a Subject changed appearance dramatically in a short period to align more clearly with a particular ideology or extremist movement, or imposed such changes upon family or other dependants, **in conjunction with an escalation in hateful / violence-supporting views**? Consider dressing & grooming in an ostentatiously "orthodox" fashion where he/she hadn't previously, but also consider racist, extremist, gang or proscribed-organisation tattoos.

ix) Has the Subject posed in a picture or video with a firearm (real or replica), or a sword, combat knives or any other **made** offensive weapon, or in any military style gear or uniform? When? Why? In what context? Consider what this might be signalling in terms of intent, leakage, mental health, or Mobilisation Identity.

x) Has the Subject suddenly & unexpectedly changed jobs to one where heavy vehicles are used, or attempted to obtain or purchase a C1 or heavier vehicle driving license (real or fake), or a heavy vehicle itself with no obvious personal or professional reason? Please explore & describe the context.

xi) Has the Subject suddenly chosen to abandon, or has been rejected by or excluded from:

(1) A legitimate place or institution of worship or political membership? In what circumstances? What is the impact of this upon the Subject's behaviour / activities?

(2) Any known extremist group, proscribed or otherwise, that he/she wanted to affiliate with? Why? What's the impact of this upon the Subject's behaviour / activities?

xii) Has anyone close to the Subject expressed concerns about sudden or dramatically increased secretive, evasive or "worrying" behaviour, particularly in relation to:

(1) Political or religious activities or "civil disobedience"? Why? In what ways? Where? With whom?

(2) Increasingly "fanatical", threatening & hateful attitudes of any sort, or a growing sense of acute anger & aggressiveness? Please describe, include any timelines.

(3) Sudden, notable & unaccounted for income or expenditures, where money has "appeared" or "disappeared" without explanation, or with nothing to show for it? Where does it come from & go to?

xiii) Has any Subject expressed a **new** or **urgent** sense of grievance involving a perceived **imminent** or **direct** life-or-death threat towards anyone or anything of value to him/her, or has he/she started attaching a "time imperative" to a grievance narrative, suggesting that **urgent action** is required in order to address the perceived threat? When did this start? What's its nature? How can it be addressed?

e) Please describe anything else you think might be relevant in the context of any shifts in vulnerabilities, or significant changes in personal circumstances, or escalating warning behaviours.

MOBILISATION, FINISHING OR "LAST RESORT" BEHAVIOURS

1) *Describe possible "mobilisation" or "finishing" behaviours associated with the Subject. Consider any indicators that may suggest a close-proximity intention to enact violence, to die, or to "go away".*

a) **I&S**

b) These are the points where thoughts & words of a concerning Subject with existing PREVENT-relevant risk or vulnerability factors or indicators, seem to be shifting to active preparation for TACT offences or "combat-readiness".

c) They apply mostly to Subjects already within Prevent, but the CTCO should judge new Cases at PGA stage with an open mind in this respect.

d) For instance:

i) Has the Subject joined a proscribed organisation? Which one? When? In what context?

ii) Has the Subject's extremist behaviour, particularly online, suddenly stopped or dropped off dramatically? This is especially relevant if it seems self-motivated or cannot be attributed **directly** to benign interventions or control measures by Police or Partners.

(1) This could suggest that the Subject's extremist feelings are being channelled elsewhere, possibly into action.

(2) Terrorism groomers have been known to tell recruits to stop on line activity prior to an attack or during its final preparation stages

iii) Has the Subject made any concerning statements of intent about:

(1) killing or deliberately hurting **anyone**,

(2) "Holy War", "jihad" or "martyrdom",

(3) "war-fighting", or "guerrilla" / "militia" operations,

(4) any unlawful extremist conduct or other terrorism related offences?

iv) Has the Subject started to mimic in dress, or self-identify as, a soldier, warrior, jihadi, guerrilla, or "pseudo-commando" of any kind, as this can be a strong warning signal of a Subject's preparation to take violent action, **particularly** if he/she fixates on or identifies him/herself with any recent or historical:

(1) Terrorists / Political Assassins / Hostile-State Actors / Mujahidin / Crusaders / Mass murderers.

v) Has a Subject suddenly obtained, attempted to obtain, or become fixated upon:

(1) Military / paramilitary / commando / "survivalist" training?

(2) Direct training from any proscribed organisation, willingly or otherwise?

(3) Controlled firearms, swords, combat knives or any other **made** offensive weapon?

(4) Paramilitary or militia-style gear (fatigues, stab-vest, weapon harness, gasmask, etc.)?

(5) Specific weapons training, e.g.: firearms, swords, combat knives, martial arts weapons etc.?

(6) Apparent logistical planning that could reasonably be suspected as enabling terrorism offences?

(7) Material describing technical skills for terrorism offences, e.g.: bomb-making guides, or guerrilla, terrorism or insurgency manuals, etc.

(8) Potential weapon precursors: bomb making parts, noxious substances, corrosive acids, or suspiciously large quantities of fireworks, pool-sanitisers, fertilisers, paint-removers, etc.?

(9) Hostile reconnaissance, or items, training or activities useful for hostile reconnaissance, including an apparent fixation (or possible selection as a target) any person, group or institution or location, State, government, military or religious, or busy public locations, governmental or State properties, commercial areas, tourist spots, public transportations, etc..

vi) Has the Subject started to demonstrate very concerning secretive behaviour, e.g.:

(1) Obvious attempts to cover his/her tracks or disguise his/her identity in a suspicious contexts? Please describe.

(2) Using codenames or code-words for him/herself or anyone else who could reasonably be suspected as being Individuals or institutions of concern, or for any items, ideas or activities that could be reasonably suspected of being connected to TACT offences?

vii) Has the already concerning Subject demonstrated any "finishing" behaviours, doing things that could reasonably be suspected as preparations to "go away" (e.g.: abroad indefinitely or to prison), or perhaps even to die? Please describe any such activities & explain why they may be considered concerning in the context, e.g.:

(1) A sudden & dramatic change towards very high-risk or hedonistic, over-indulgent or even "sleazy" behaviour in stark contrast to the Subject's usual behaviour? It is not unknown for extremists with the most austere, unforgiving or even "prudish" beliefs to embark on sudden & intense periods of hedonistic activity prior to launching attacks where they know that they are likely to be killed or where they actively seek death as part of their attack. Describe the behaviour. When / how recently did it start? Why? What's the context?

(2) Suddenly & unexpectedly getting married, with no preparation or warning. What's the context? What do family or friends think? Is this an unexpected protective factor or an example of the Subject "wrapping things up"?

(3) Saying obvious "goodbyes" to family or friends by whatever means, without there being any obvious, innocent & lawful explanation for doing so.

(4) Very rapidly incurring (or paying off) **significant** debts – like running up huge credit-card bills or suddenly paying off a mortgage entirely. What's the context? Where did the money come from? Where did it go?

(5) Shaving all body hair where they have not done so before & without a clear reason why. This is a relatively common finishing behaviour for militant Jihadist terrorists preparing for death or "martyrdom". However, be certain that the instance in question is not a part of a mourning custom/ceremony for a deceased loved-one, or for some other benign religious or cultural reason.

viii) Please describe anything else you think might be relevant in the context of potential mobilising or finishing behaviours.

ANNEX 2: COMPLETING THE VAF

1) The DIF has been designed to work in conjunction with the VAF, containing all of its considerations.

2) The Vulnerability Assessment Framework (VAF) is the vulnerability and risk assessment tool mandated by the Home Office for use within and for Channel. This annex provides a description of the VAF to guide decisions about whether an Individual needs support to address their vulnerability to being drawn into terrorism as a consequence of radicalisation and the kind of support t that they need. It should not be assumed that the characteristics set out below necessarily indicate that a person is either committed to terrorism or may become a terrorist.

3) The assessment framework involves three dimensions: engagement, intent and capability, which are considered separately.

a) Engagement with a group, cause or ideology:

i) Engagement factors are sometimes referred to as "psychological hooks". They include needs, susceptibilities, motivations and contextual influences and together map the individual pathway into terrorism. They can include:

(1) Feelings of grievance and injustice

(2) Feeling under threat

(3) A need for identity, meaning and belonging

(4) A desire for status

(5) A desire for excitement and adventure

(6) A need to dominate and control others

(7) Susceptibility to indoctrination

(8) A desire for political or moral change

(9) Opportunistic involvement

(10) Family or friends' involvement in extremism

(11) Being at a transitional time of life

(12) Being influenced or controlled by a group

(13) Relevant mental health issues

b) Intent to cause harm:

i) Not all those who become engaged by a group, cause or ideology go on to develop an intention to cause harm, so this dimension is considered separately. Intent factors describe the mindset that is associated with a readiness to use violence and address what the individual would do and to what end. They can include:

(1) Over-identification with a group or ideology.

(2) 'Them and Us' thinking.

(3) Dehumanisation of the enemy.

(4) Attitudes that justify offending.

(5) Harmful means to an end.

(6) Harmful objectives.

c) Capability to cause harm:

i) Not all those who have a wish to cause harm on behalf of a group, cause or ideology are capable of doing so, and plots to cause widespread damage can take a high level of personal capability, resources and networking to be successful. What the individual is capable of is therefore a key consideration when assessing risk of harm to the public. Factors can include:

(1) Individual knowledge, skills and competencies.

(2) Access to networks, funding or equipment.

(3) Criminal Capability

3) The three criteria are assessed by considering 22 factors that can contribute to vulnerability (13 associated with engagement, six that relate to intent and three for capability). These factors taken together form a holistic view of the vulnerability of an Individual that will inform decisions on whether an Individual needs support and what kind of support package may be appropriate. These factors can also be added to and are not considered an exhaustive list. By undertaking regular vulnerability assessments, the progress that is being made in supporting an Individual can be tracked through changes in the assessment.

4) Completing a full assessment for all 22 factors requires thorough knowledge of the individual that may not be available at the point of the initial referral. However, there are a number of behaviours and other indicators that may indicate the presence of these factors.

5) Example indicators that an Individual is ***engaged*** with an extremist group, cause or ideology include:

   a) spending increasing time in the company of other suspected extremists;

   b) changing their style of dress or personal appearance to accord with the group;

   c) day-to-day behaviour becoming increasingly centred around an extremist ideology, group or cause;

   d) loss of interest in other friends and activities not associated with the extremist ideology, group or cause;

   e) possession of material or symbols associated with an extremist cause (e.g. the swastika for right-wing groups);

   f) attempts to recruit others to the group/cause/ ideology, or;

   g) communications with others that suggest identification with a group/cause/ideology.

6) Example indicators that an Individual has an ***intention*** to cause harm, use violence or other illegal means include:

   a) clearly identifying another group as threatening what they stand for and blaming that group for all social or political ills;

   b) using insulting or derogatory names or labels for another group;

   c) speaking about the imminence of harm from the other group and the importance of action now;

   d) expressing attitudes that justify offending on behalf of the group, cause or ideology;

   e) condoning or supporting violence or harm towards others, or;

   f) plotting or conspiring with others.

7) Example indicators that an Individual is ***capable*** of causing harm or contributing directly or indirectly to an act of terrorism include:

   a) having a history of violence;

   b) being criminally versatile and using criminal networks to support extremist goals;

   c) having occupational skills that can enable acts of terrorism (such as civil engineering, pharmacology or construction); or

   d) having technical expertise that can be deployed (e.g. IT skills, knowledge of chemicals, military training or survival skills).

8) The examples above are not exhaustive and vulnerability may manifest itself in other ways.

9) The VAF should initially be completed by the Channel Case Officer and then be circulated in full to Panel members in advance of meetings so that all relevant Panel members can contribute their knowledge experience and expertise to the case.

10) The VAF should complement and inform rather than replace professional judgement and/or other forms of safeguarding assessment when deciding on the most appropriate types of support at Panel meetings.

ANNEX 3: EXTREMISM – OVERVIEW FOR CTP PREVENT

1) For the working definition of "extremism" for CTP PREVENT, refer to the **Extremism – Operational Guidance** section in the Glossary of this document.
2) In this section we will look at the wider background and operational guidance around "extremism" for CTP PREVENT.
3) The PREVENT Duty touches upon the correlations between "extremism", terrorism offences and PREVENT:
   a) *"Terrorist groups often draw on extremist ideology, developed by extremist organisations. Some people who join terrorist groups have previously been members of extremist organisations and have been radicalised by them."*[21]
   b) *"The PREVENT strategy was explicitly changed in 2011 to deal with all forms of terrorism and with non-violent extremism, which can create an atmosphere conducive to terrorism and can popularise views which terrorists then exploit. It also made clear that preventing people becoming terrorists or supporting terrorism requires challenge to extremist ideas where they are used to legitimise terrorism and are shared by terrorist groups. And the strategy also means intervening to stop people moving from extremist (albeit legal) groups into terrorist-related activity."*[22]
4) So "extremism" is relevant to PREVENT insofar as the term is used in relation to escalation towards, or the actual commission of, terrorism connected offences, or in the popularisation of views and values that may seem to legitimise or promote terrorist activities.

Extremism – 2011 PREVENT Strategy

1) There is currently no primary legislation within the UK that defines "extremism".
2) A national consultation is underway that intends to provide a legal definition of "extremism" within the UK contexts. However, at the time of writing we only have the definition provided by the **2011 PREVENT Strategy** and **2015 Channel Guidance** as:
   a) *"[…] vocal or active opposition to fundamental British values, including democracy, the rule of law, Individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas."*
3) This definition has been Subject to much scrutiny and critique over the years, primarily around what is meant by "British values". It is relatively straightforward to Police established crimes and antisocial behaviour (ASB), but it is not explicitly clear what is meant by "British values", nor where the boundaries of "British values" may lie, i.e.:
   a) Within the UK context where there is freedom of conscience, freedom of disagreement and freedom of speech, it is not immediately clear without further guidance how the Police are expected to judge the limits of "British values" and differences between:
      i) A strong but otherwise benign cultural difference or philosophical disagreement with these "British values", and,
      ii) A physically dangerous or genuinely harmful opposition to these values, along with a desire to undermine them.
4) Even after the 2015 update to the Guidance, where the "British values" reference was changed to "our shared values", this still did not provide CTP PREVENT clear and nuanced enough guidance on the nature of PREVENT relevant concerns, offences, ASB or other behaviours.
5) As such, CTPHQ PREVENT has devised operational guidance for "extremism" for CTP PREVENT, drawing upon existing criminal legislation and established Police safeguarding and crime prevention policies, which can be lawfully and proportionately operationalised by CTCOs wherever we are asked to look into "extremism" or judge whether an Individual is at risk from "extremists".

[21] PREVENT Duty Guidance in England and Wales, 2015, Introduction, S.7.
[22] PREVENT Duty Guidance in England and Wales, 2015, Introduction, S.8.

6) This practical, working, guidance focuses on factors that Police already have powers and duties in relation to, or that it is proportionate, lawful & justifiable for us to consider for PREVENT. It is important to note that in our working definition here, extremists are not automatically criminals or TACT offenders (although they certainly *can* be), and "extremism" is not used simply as another word for "violent extremism", "terrorism" or "TACT offender". See the "extremism" entry in this document's glossary for details.

Extremism - Disrupt, Deter & Prosecute

1) Not all extremists become terrorism offenders, and it is by no means a clear progression from the former into the latter. Similarly, not all extremists intend direct violence against other people, i.e.: not all extremists are violent extremists. However, to fulfil our duty in relation to PREVENT, Police are expected to take action in order to deter, divert, disrupt, and if necessary, prosecute "extremists".
2) In complying with the duty, Police should engage with, and where appropriate disrupt, extremist activity, in partnership with other agencies wherever possible. Police are also expected to prioritise activities that disrupt terrorist and extremist material on the internet, and extremists living and/or working within the UK.
3) Officers should consider the full range of investigative and prosecution options when it comes to disrupting extremist behaviour. Wherever appropriate, draw upon the range of tactics presented in the **CTP Disruption Guidance** and the associated documents (such as the College of Policing **'Menu of Tactics'**). The sorts of relevant tactics can include:
   a) Providing high visibility Police presence at relevant events in public places,
   b) In concert with our PURSUE colleagues, enforce terrorist-proscription and public order legislation,
   c) Advising other specified authorities, for example Local Authorities or universities, to develop venue booking processes and good practice,
   d) Lawfully disrupting, or, where proportionate and lawful, attending events involving extremist speakers in both private and municipal establishments,
   e) Working with Local Authorities to consider municipal powers, including local highways and leafleting by-laws, using legislation around safeguarding of young and vulnerable people.

Extremism – Offences & Unlawful Extremist Conduct

1) As shown in the previous sections, extremists can be involved in high level aggravated activism, or commit terrorism offences, serious criminal offences and hate offences of various kinds. However, by our working definition, not all extremists need to actually **plan** or **commit** terrorism offences, or other serious offences mentioned above, in order to be people of relevant concern to PREVENT. They could "advocate" or "threaten" them.
2) Within PREVENT we must look to manage any of the criminal activities of extremists, falling short of the planning or execution of terrorism offences, which fall within the purview of PURSUE. Whereas terrorism offences are described within primary legislation and official CPS guidelines, the term "unlawful extremist conduct" is used within this document only as **guidance**. "Unlawful conduct" refers here to behaviour occurring in any part of the UK that is unlawful under UK criminal laws. However, this also includes conduct by UK citizens and residents that occurs **outside** of the UK, providing that the conduct in question would be unlawful under UK legislation if it occurred within any part of the UK.
3) Unlawful extremist conduct is intended to encompass any ASB and criminal offences that are outside of UK terrorism legislation, but which are initiated by Subjects as **deliberate** expressions of their extremist mindset (as defined above), or to further an extremist racial, political, religious or single-issue ideological goal or cause. This broad definition is not so much concerned with the specific **nature** of offences as it is their **intentions,** or their extremist **contexts**.

4) Unlawful extremist conduct is established here in order to help CTCOs identify persistent or escalating **courses of conduct** by Subjects within their contexts, and in order to better identify, deter, divert or disrupt possible escalation towards TACT offences.

7) Possible examples of relevant conduct can be found right across the UK's criminal legislation, including, but not limited to:

a) **Criminal Damage Act 1971:** deliberate vandalism or sabotage.

b) **Criminal Justice and Public Order Act 1994**: around aggravated trespass.

c) **Control of Pollution Act 1974**: unlawful use of a loudspeakers on the street.

d) **Poisons Act 1972:** particularly the offences around the precursors to explosives.

e) **Antisocial Behaviour, Crime & Policing Act 2014:** Orders, Injunctions & Dispersals.

f) **Malicious Communications Act 1988:** indecent or grossly offensive messages or threats.

g) **Hate Offences:** including any relevant antisocial behaviour or criminal offences as found within the:

i) **Public Order Act 1986,**

ii) **Crime & Disorder Act 1998,**

iii) **Football Offences Act 1991,**

iv) **Racial and Religious Hatred Act 2006,**

v) **Offences Against the Person Act 1861,**

vi) **Criminal Justice & Immigration Act 2008.**

h) **Protection from Harassment Act 1997:** particularly harassment, stalking & putting people in fear of violence.

i) **Highways Act 1980:** Obstructing Highways; Depositing Things on Highways; Unauthorised Signs / Posters / Banners / Marks.

j) **Theft Act 1978**, the **Forgery & Counterfeiting Act 1981**, the **Fraud Act 2006:** any offences enacted with an extremist intention.

k) **Public Order Act 1986:** Riot; Violent Disorder; Affray; Fear or Provocation of Violence; Intentional Harassment, Alarm, or Distress.

l) Cyber-Crimes, under the **Computer Misuse Act 1990**, the **Data Protection Act 1998**, the **Regulation of Investigatory Powers Act 2000**, & perhaps even the **Official Secrets Act** (and amendments), depending on contexts (particularly with respect to the **Public Interest Disclosure Act 1998**).

ANNEX 4: LEGISLATION RELEVANT TO PREVENT

1) In this section we look at the most prominent Acts of Legislation that are relevant to PREVENT.
2) It is important to note that in order to be **convicted** of a terrorism offence, a person does not actually have to **commit** what could be considered a terrorist attack. There are numerous non-violent terrorism offences. Hence PREVENT has to take this reality into consideration – our mandate is to PREVENT people being drawn into any and all terrorism offending, not "only" the high-visibility massacres and/or murders that comprise the worst-Case terrorism offences.

TACT 2000 - Terrorism Act

1) Between them, the 2000 - 2006 Terrorism Acts (TACT) define in primary legislation exactly what is meant by "terrorism", from mass murder through to the equally PREVENT-relevant offence of "glorifying" or "encouraging" terrorism.
2) In summary:
   - **a)** Terrorism is the **use** or **threat** of action, both within and outside of the UK, designed to influence any governmental organisation (national or international), or to intimidate the public or any section of the public.
   - **b)** It must also be for the purpose of advancing a **political**, **religious**, **racial** or other **ideological** cause.
   - **c)** Examples of the relevant "action" could include:
     - **i)** Serious violence against a person or serious damage to property,
     - **ii)** Endangering a person's life (other than that of the person committing the action),
     - **iii)** Creating a serious risk to the health or safety of the public or a section of the public,
     - **iv)** Action designed to seriously interfere with or seriously to disrupt an electronic system.
3) **Notes:**
   - **a)** TACT does not define or limit what is meant by "**political, religious, racial or ideological cause**", nor does it restrict "**ideological cause**" to being **only** political, religious or racial, or to being solely those ideologies held or promoted by already Proscribed Organisations.
   - **b)** TACT also does not stipulate that a terrorist has to have a long-standing or deep-seated or "fanatical" belief in the ideology or cause that he or she is ostensibly supporting by committing a TACT offence.
   - **c)** Some Individuals seek to support or enact TACT offences without a clear understanding of the ideology or cause they are ostensibly supporting.
   - **d)** Individuals whose ideological motivations are unclear, mixed or unstable, but who still demonstrate a connection to, or personal interest in, extremism, terrorism or mass-murder, should be given the same consideration for support and intervention as those whose concerning ideological motivations are more consistent and obvious.
   - **e)** Also, the "**threat**" of "relevant action" is technically enough to complete a TACT offence, so the action does not need to be physically enacted for a terrorism offence to be complete, if a credible threat to enact it has been made.
   - **f)** Also note, where this "action" involves the "use or threat" of firearms or explosives, there need be no specific intention on the perpetrator's part to "influence" (or intimidate) the government or public. The offence is complete without them where firearms or explosives are concerned.
4) **Offences Beyond Murder & Attempts**:
   - **a)** PREVENT seeks to stop people being drawn into **any** terrorism-related offences.
   - **b)** Planning, assisting and even collecting information on how to commit terrorist acts are all crimes under British terrorism legislation, and are therefore all offences that PREVENT needs to consider.
   - **c)** For instance, TACT makes it an offence for both attempts and successes around:
     - **i)** Encouraging terrorism.
     - **ii)** Restricted-weapons training.

iii) Preparing of acts of terrorism.

iv) Directing a terrorist organisation.

v) Supporting a proscribed organisation.

vi) Dissemination of terrorist publications.

vii) Attendance at a place for terrorist training.

viii) Possession of an article for terrorist purposes.

ix) Become a member of a Proscribed Organisation.

x) Assisting others in preparation of acts of terrorism.

xi) Providing or receiving instruction or training for terrorism.

xii) Finance and money laundering in relation to terrorism acts.

xiii) Wearing a uniform associated with a proscribed organisation.

xiv) Distribute a terrorist publication with the intention of encouraging acts of terrorism.

xv) Collecting or making a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism, or to possess a document or record containing information of that kind.

xvi) Making and possession of devices or materials: Prohibits the making or possession of any radioactive device (i.e.: a "dirty bomb").

xvii) Misuse of devices or material, and misuse and damage of facilities: Prohibits using radioactive materials or a radioactive device in a terrorist attack, and the sabotage of nuclear facilities which causes a radioactive leak.

xviii) Terrorist threats relating to devices, materials or facilities: Prohibits anyone from making threats to demand that they be given radioactive materials.

xix) Trespassing (etc.) on nuclear sites (Section 12): Extends a previous ban on trespassing, imposed by the Serious Organised Crime and Police Act 2005, to cover any nuclear site.

CTSA 2015 – Counter Terrorism & Security Act

1) The 2015 **Counter Terrorism and Security Act** explores the role of Police in relation to the PREVENT Duty. It highlights how, alongside other agencies and Statutory Partners, the Police play an essential role in most aspects of PREVENT work.

2) Police hold information that can help assess risks and vulnerabilities around radicalisation, and disrupt people engaged in grooming or coercing others towards any TACT offences.

3) We work alongside other sectors, playing a galvanising role in developing local PREVENT Partnerships and bring together a wide range of other organisations to support local delivery of PREVENT.

4) Police are uniquely placed to tackle terrorism, and whilst it is acknowledged that the Police Service will designate dedicated PREVENT roles within Policing, a key objective for the Police is to ensure that PREVENT is embedded into **all** aspects of policing, including patrol, neighbourhood and safeguarding functions.

5) In fulfilment of our duties, consideration must be given to the use of all suitable Police resources, not just those specifically designated as PREVENT.

6) **The Police specified authorities** listed in Schedule 6 to the CTSA are as follows:

- **a)** Police Forces in England & Wales.
- **b)** The Civil Nuclear Police Authority.
- **c)** Police & Crime Commissioners.
- **d)** The British Transport Police.
- **e)** Port Police Forces.

7) **Supporting People Vulnerable to Radicalisation.**

a) PREVENT requires a multi-agency approach to protect people at risk from radicalisation. When people who are vulnerable in this sense are identified, Police will undertake the following:

i) In Partnership with other agencies including the Local Authority (particularly the Channel programme), to develop Case management plans that include consider appropriate interventions, to support and safeguard these vulnerable Individuals.

ii) Work in Partnership with (and support) Channel Panels, chaired by Local Authorities, to co-ordinate Channel Partners and execute Channel actions.

iii) Support existing Intervention Providers, and identify potential new Intervention Providers.

8) Screening PREVENT Referrals.

a) CTCOs are responsible for identifying people who may be vulnerable to being drawn into terrorism. This requires making some sort of assessment of the referred Individuals.

b) Although this process is not explored in detail within the Act, CTCOs must receive and triage PREVENT Referrals from FIMUs, after the FIMU de-confliction and PURSUE / RADO Assessment.

c) CTCOs must then use the **Dynamic Investigation Framework** (**DIF**) to conduct the initial PREVENT assessment, more commonly referred to as the PREVENT Gateway Assessment (PGA), which helps them determine whether the referral should be:

i) Closed from PREVENT.

ii) Enter the Local Authority led, multi-agency strand of PREVENT (Channel).

iii) Enter into the PLP, multi-agency strand of PREVENT (PLP Case Management).

9) Supporting Statutory Partners.

a) CTCOs are tasked with logging such referrals on the digital PREVENT Case Management Tracker (PCM TRACKER) and subsequently passing on the Case to the Local Authority where appropriate.

b) To achieve this, CTCOs are expected to:

i) Screen & triage all de-conflicted PREVENT referrals as part of the CTP PREVENT's Gateway Assessment, within 5 working days of receiving a de-conflicted referral from a FIMU (or as close to 5 working days as is reasonably practicable).

ii) Engage fully with the Local Authority and other relevant agencies and Statutory Partners, to assess the risk of referred Subjects to being drawn towards terrorism related activities, providing details to Local Authorities / Channel Panels of the Police Counter-Terrorism Local Profiles (CTLP) wherever relevant.

iii) Support the work of:

(1) Local Authority Channel Co-ordinators,

(2) Local Authority PREVENT coordinators,

(3) Regional Further & Higher Education PREVENT coordinators,

(4) Regional Health PREVENT Leads,

(5) Regional NOMS PREVENT coordinators.

iv) Co-ordinate the delivery of the Channel program by accepting and assessing for PREVENT relevance any information or concerns received from:

(1) FIMUs,

(2) PREVENT Partners,

(3) Members of the public,

(4) including acting as a conduit for Channel referrals to Partners.

v) Support the development and implementation of a PREVENT action plans, or 'Case management plans', by this multi-agency group, to address that risk and the vulnerabilities around it.

vi) Ensure PREVENT considerations are fully embedded into PURSUE-led counter-terrorism investigations.

10) **Partners of Local Panels**: included in Schedule 7 of the CTSA, and they can include:

a) **Ministers of the Crown & Government Departments:**

i) A Minister of the Crown.

ii) A government department other than an intelligence service.

b) **Local Government:**

i) A local authority (other than a local authority that is a member of the Panel in question).

ii) A person carrying out a function of a local authority by virtue of a direction made under section 15 of the Local Government Act 1999.

c) **Criminal Justice:**

i) The governor of a prison in England and Wales (or, in the case of a contracted out prison, its director).

ii) The governor of a young offender institution or secure training centre (or, in the case of a contracted out young offender institution or secure training centre, its director).

iii) The principal of a secure college.

iv) A youth offending team established under section 39 of the Crime and Disorder Act 1998.

v) A provider of probation services within the meaning given by section 3(6) of the Offender Management Act 2007.

d) **Education, Child Care, etc.:**

i) A sixth form college corporation within the meaning given by section 90(1) of the Further and Higher Education Act 1992.

ii) The governing body of an institution within the further education sector within the meaning given by section 91(3) of that Act.

iii) A person who is authorised by virtue of an order made under section 70 of the Deregulation and Contracting Out Act 1994 to exercise a function specified in Schedule 36A to the Education Act 1996.

iv) A person with whom arrangements have been made for the provision of education under section 19 of the Education Act 1996 or section 100 of the Education and Inspections Act 2006 (cases of illness, exclusion etc).

v) The proprietor of—

(1) a school that has been approved under section 342 of the Education Act 1996,

(2) a maintained school within the meaning given by section 20(7) of the School Standards and Framework Act 1998,

(3) a maintained nursery school within the meaning given by section 22(9) of that Act,

(4) an independent school registered under section 158 of the Education Act 2002,

(5) an independent educational institution registered under section 95(1) of the Education and Skills Act 2008,

(6) a 16 to 19 Academy within the meaning given by section 1B of the Academies Act 2010,

(7) an alternative provision Academy within the meaning given by section 1C of that Act, or

(8) a special post-16 institution within the meaning given by section 83(2) of the Children and Families Act 2014.

vi) A person who is specified or nominated in a direction made in relation to the exercise of a local authority's functions given by the Secretary of State under section 497A of the Education Act 1996 (including that section as applied by section 50 of the Children Act 2004 or section 15 of the Childcare Act 2006).

vii) A person registered under Part 2 of the Care Standards Act 2000 in respect of—

(1) a children's home as defined in section 1 of that Act,

(2) a residential family centre as defined in section 4 of that Act,

(3) a fostering agency as defined in that section, or

(4) a holiday scheme for disabled children, within the meaning of the Registered Holiday Schemes for Disabled Children (England) Regulations 2013 (S.I. 2013/1394).

viii) The governing body of a qualifying institution within the meaning given by section 11 of the Higher Education Act 2004.

ix) A person registered under Chapter 2, 2A, 3 or 3A of Part 3 of the Childcare Act 2006 or under section 20 of the Children and Families (Wales) Measure 2010 (nawm 1).

x) A body corporate with which a local authority has entered into arrangements under Part 1 of the Children and Young Persons Act 2008.

xi) A person who is specified in a direction made in relation to the exercise of a local authority's functions given by the Welsh Ministers under section 25 of the School Standards and Organisation (Wales) Act 2013 (anaw 1) (including that section as applied by section 50A of the Children Act 2004 or section 29 of the Childcare Act 2006).

xii) The governing body of an educational establishment maintained by a local authority in Wales.

xiii) The governing body or proprietor of an institution (not otherwise listed) at which more than 250 students, excluding students undertaking distance learning courses, are undertaking—

(1) courses in preparation for examinations related to qualifications regulated by the Office of Qualifications and Examinations Regulation or the Welsh Government;

(2) courses of a description mentioned in Schedule 6 to the Education Reform Act 1988 (higher education courses).

e) Health and Social Care:

i) A clinical commissioning group established under section 14D of the National Health Service Act 2006.

ii) An NHS Trust established under section 25 of the National Health Service Act 2006.

iii) An NHS foundation trust within the meaning given by section 30 of the National Health Service Act 2006.

iv) A Local Health Board established under section 11 of the National Health Service (Wales) Act 2006.

v) An NHS trust established under section 18 of the National Health Service (Wales) Act 2006.

f) Police:

i) A chief officer of Police for a Police area in England and Wales (other than a chief officer who is a member of the Panel in question).

CTBS 2019 – Counter Terrorism & Border Security Act

1) The **Counter-Terrorism & Border Security Act 2019** received Royal Assent in 2019.

2) Who Can Refer to Channel?

a) This is the most relevant addition to PREVENT brought into effect by this law.

b) Local Authorities can make **S.36 CTSA** decisions to refer "identified Individuals" to a Channel Panel, where before this was a Police-only task. [23] This was introduced in order to help facilitate the '**Dovetail**' process.

c) All potential Cases still need to be de-conflicted by a FIMU and they still require CTCOs to complete the PGA step, as these are checks required within the Police-only competency of a risk of terrorism offending assessment.

d) This makes a distinction between the Local Authority and the Channel Panel itself, which a Panel that also comprises of Police representative

3) Some of the other provisions relevant to PREVENT:

a) **S.1** extends the offence of inviting support for a proscribed organisation in TACT to also cover expressions of support that are **reckless** as to whether they will encourage others to support the organisation.

[23] CTBA, S.20 (1 – 7b).

b) **S.2** clarifies that the existing TACT offence of displaying in a public place an image which arouses reasonable suspicion that the person is a member or supporter of a proscribed organisation, covers the display of images online (including of a photograph taken in a private place).

c) **S.3** updates the TACT offence of obtaining information likely to be useful to a terrorist to cover terrorist material that is just viewed or streamed over the internet, rather than downloaded to form a permanent record.

d) **S.4** provides for a new offence of entering or remaining in an area outside the United Kingdom that has been designated in regulations by the Secretary of State in order to protect the public from a risk of terrorism.

e) **S.6** confers extra-territorial jurisdiction on a number of further offences to ensure that Individuals abroad can be prosecuted for having encouraged or carried out acts of terror overseas.

TPIM 2011 – Terrorism Prevention & Investigation Measures Act

1) The **Terrorism Prevention and Investigation Measures Act** is concerned primarily with criminal investigations into terrorism-related activity, and the imposition and enforcement of terrorism prevention and investigation measures (TPIMs).

2) S.4 of the Act also clarifies offences around **involvement in terrorism-related activity** the breadth of which is **very** relevant to the concerns of PREVENT, bearing in mind PREVENT exists to stop people from being drawn into any terrorism offences as per UK law, not simply the more highly visible mass murder element of terrorism.

a) Involvement in terrorism-related activity is any one or more of the following:

i) The commission, preparation or instigation of acts of terrorism.

ii) Conduct which facilitates the commission, preparation or instigation of such acts, or which is intended to do so.

iii) Conduct which gives encouragement to the commission, preparation or instigation of such acts, or which is intended to do so.

iv) Conduct which gives support or assistance to Individuals who are known or believed by the Individual concerned to be involved in conduct falling within.

v) For the purposes of this Act it is immaterial whether the acts of terrorism in question are specific acts of terrorism or acts of terrorism in general.

vi) It is immaterial whether an Individual's involvement in terrorism-related activity occurs before or after the coming into force of this Act.

EQUALITY ACT 2010

1) CTCOs are required to consider, and have duties in relation to, a broad cross-section of human rights laws. The Equality Act is referenced in particular within the **2015 PREVENT Duty Guidance,** hence its inclusion here. This Act specifically forbids various forms of discrimination upon the basis of the "protected characteristics" detailed within it, and also stipulates the duties of Public Authorities (of which the Police are one) in relation to the Act. The relevant section of the Act is summarised below.

1) **Public Sector Equality Duty:**

a) A public authority must, in the exercise of its functions, have due regard to the need to:

i) Eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act,

ii) Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it,

iii) Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

b) A person who is not a public authority but who exercises public functions must, in the exercise of those functions, have due regard to the matters mentioned in subsection 1.

c) Having due regard to the need to advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it involves having due regard, in particular, to the need to:

- **i)** Remove or minimise disadvantages suffered by persons who share a relevant protected characteristic that are connected to that characteristic,
- **ii)** Take steps to meet the needs of persons who share a relevant protected characteristic that are different from the needs of persons who do not share it,
- **iii)** Encourage persons who share a relevant protected characteristic to participate in public life or in any other activity in which participation by such persons is disproportionately low.

d) The steps involved in meeting the needs of disabled persons that are different from the needs of persons who are not disabled include, in particular, steps to take account of disabled persons' disabilities.

e) Having due regard to the need to foster good relations between persons who share a relevant protected characteristic and persons who do not share it involves having due regard, in particular, to the need to—

- **i)** Tackle prejudice, and,
- **ii)** Promote understanding.

f) Compliance with the duties in this section may involve treating some persons more favourably than others; but that is not to be taken as permitting conduct that would otherwise be prohibited by or under this Act.

g) The relevant protected characteristics are:

- **i)** Sex,
- **ii)** Age,
- **iii)** Race,
- **iv)** Disability,
- **v)** Religion or belief,
- **vi)** Sexual orientation,
- **vii)** Gender reassignment,
- **viii)** Pregnancy and maternity.

h) A reference to conduct that is prohibited by or under this Act includes a reference to:

- **i)** A breach of an equality clause or rule,
- **ii)** A breach of a non-discrimination rule.

i) Schedule 18 of the Act (detailing exceptions) has effect.

ANNEX 5: INFORMATION SHARING WITH PARTNERS

1) PREVENT frequently requires the sharing of personal information about vulnerable Individuals, and the sharing of other information and intelligence between Partners on local threats.
2) This section provides guidance on the procedures and legislation relevant to information sharing.

Information Sharing - PREVENT Purposes

1) **Key principle:** Partners may consider sharing personal information with each other for PREVENT purposes, for instance for any referral to the Information Gathering Phase or with members of a safeguarding Panel.
2) The CTSA includes a general right of Police to share Subject information with Local Authorities / LACCs under S.36 of its provisions, for the purposes of ascertaining whether a Subject is suitable for support. Effective information sharing is vital to the delivery of PREVENT, enabling Partners to take informed action to support identified vulnerabilities and manage identified risks. This will sometimes require the sharing of personal information, particularly in connection with objectives 2 and 3 of the PREVENT strategy.
3) However, there is an expectation that the sharing of personal information must be on a Case by Case assessment, which considers:
   a) Whether the informed consent of the Individual can be obtained,
   b) Whether the proposed sharing being necessary, proportionate and lawful.
4) The lawful bases for sharing and processing information are replicated here :
   a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
   b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
   c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
   d) **Vital interests:** the processing is necessary to protect someone's life.
   e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
   f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)
5) Any sharing of personal or sensitive personal data should be considered carefully, particularly where the consent of the Individual is not to be obtained. The legal framework within which public sector data sharing takes place is often complex, although there is a significant amount of guidance already available.

Information Sharing - Necessary & Proportionate

1) The overriding principles are *necessity* and *proportionality*.
2) The sharing of information must be necessary to conduct the work in question. Only the information required to have the desired outcome should be shared, and only to those Partners necessary.
3) Key to determining the necessity and proportionality of sharing information will be the professional judgement of the risks to an Individual or the public.

Information Sharing - Case Merits

1) Each Case should be judged on its own merits and the following questions should be considered when sharing information:
   a) What information you are intending to pass?
   b) To whom you are intending to pass the information?

c) Why you are intending to pass the information, with what expected outcome?

d) The legal basis upon which the information is to be passed?

Information Sharing – Consent

1) The default should be to consider seeking the consent of the Individual to share information.

2) There will, of course, be circumstances in which seeking the consent of the Individual will be neither desirable nor possible, because it will prejudice delivery of the intended, legitimate, outcome, and there may be gateways or exemptions which permit sharing to take place without consent.

3) If you cannot seek or obtain consent, or consent is refused, you cannot share personal information without satisfying one of the gateway or exemption conditions.

4) Compliance with the **Data Protection Act** and **Human Rights Act** are significantly simplified by having the Subject's consent. The Information Commissioner has indicated that consent should be informed and unambiguous, particularly in the Case of sensitive personal information.

5) If consent is sought, the Individual should understand how their information will be used and for what purpose.

Information Sharing – Types of Personal Information

1) Personal Information requested from, or shared with, Statutory Partners may include, but is not limited to:

a) Personal information (name, DoB, ethnicity, address, telephone, email, NHS number, proof of identity, unique pupil number);

b) Parents/carers personal information;

c) Personal information about other members of household;

d) Personal information about close relatives;

e) Details of family relationships in and outside of the household;

f) Data subject and family's legal status;

g) Accommodation;

h) Employment status;

i) Details about physical and emotional well-being and parenting;

j) Details of any risk issues;

k) Youth offending information: offences (including alleged offences), criminal proceedings, convictions and sentences;

l) Medical history;

m) Mental health history;

n) Health, social care or other services provided;

o) Information about situation given to us by family/carers and/or other organisations (e.g. GP, school nurse, Police);

p) Reports relating to situation (e.g. safeguarding and other assessments, Child Protection Plans and Looked After Children reviews);

q) Educational progress and attainment information;

r) School attendance, exclusions and behavioural information, and;

s) Information such as court orders and professional involvement;

t) The data subject and immediate families' immigration history if relevant to the case (e.g. intelligence suggesting radicalisation / affiliation with foreign or transnational extremist or terrorist organisations);

u) Any documents sent to us relating to the data subject (e.g. referrals received from other agencies and professionals);

v) Police audio and video recording.

2) It may be necessary to share Special Category Data for the following reasons:

   a) Racial or ethnic origin: a subject's race or ethnic origin may provide context to a referral, for example where the views espoused are of White Supremacy.

   b) Political opinions: a subject's political views may provide context to a referral, for example holding extreme right- or left-wing views, or opposition to democratic rights.

   c) Religious or philosophical beliefs: religious beliefs may provide context to a referral, for example in identifying a change in behaviour following conversion to a religion.

   d) Data concerning a natural person's physical or mental health or condition, sex life or sexual orientation: mental or physical health may indicate a particular vulnerability to being exploited, or indicate capability to carry out terrorist acts. Sex life or sexual orientation may provide context to the person's emotional wellbeing.

   e) Where the decision is made that a referral does not reach the threshold under s.36 CTSA, information may be shared with the Local Authority PREVENT Co-ordinator alone, in order to assist them in identifying learning opportunities for statutory partners for safeguarding purposes.

Information Sharing – What is "Power to Share?"

1) The sharing of data by public sector bodies requires the existence of a power to do so, in addition to satisfying the requirements of the Data Protection Act, the Human Rights Act and the common law duty of confidentiality.

6) S.36 of the CTSA concerns the right and responsibility of the Police to share Subject information with Local Authorities / LACCs where there are reasonable grounds to believe that a Subject is suitable for Panel support.

2) It is possible to imply a power to share information because it is necessary for the fulfilment of an organisation's statutory functions.

3) The power to share information arises only as a consequence of an organisation having the power to carry out an action which is dependent on the sharing of information.

4) Having established a power to share information, it should be confirmed that there are no bars to sharing information, either because of a duty of confidentiality or because of the right to privacy enshrined in Article 8 of the European Convention on Human Rights.

5) Finally, it will also be necessary to ensure compliance with the Data Protection Act, either by meeting the processing conditions in Schedules 2 and 3, or by relying on one of the exemptions (such as section 29 for the prevention of crime). There are further details of the overarching legislation and some potentially relevant gateways in the section on legislation and guidance below.

6) Where non-public bodies (such as community organisations) are involved in delivery of PREVENT work, you may need to pass personal and sensitive information to them and your approach to information sharing should be the same – i.e. that it is necessary, proportionate and lawful. In engaging with non-public bodies to the extent of providing personal information, it is good practice to ensure that they are aware of their own responsibilities under the Data Protection Act.

Information Sharing - Legislation & Guidance

1) Although not an exhaustive list, the following acts and statutory instruments may be relevant. The original legislation can be found at the Statute Law Database **http://www.statutelaw.gov.uk/**

2) **Data Protection Act 1998**

   a) The DPA is the principal legislation governing the process (including collection, storage and disclosure) of data relating to Individuals. The Act defines personal data (that information by which an Individual can be identified) and sensitive personal data (including information about an Individual's health, criminal record and political or religious views), and the circumstances in and extent to which they can be processed. The Act also details the rights of data Subjects.

b) The first data principle states that personal data shall be processed fairly and lawfully, meaning that other statutory and common law obligations must be complied with, and that the DPA cannot render lawful any processing which would otherwise be unlawful. Schedules 2 and 3 of the Act provide the conditions necessary to fulfil the requirements of the first principle.

3) Data Protection (Processing of Sensitive Personal Data) Order 2000

a) This statutory instrument (SI 2000/417) specifies further conditions under which sensitive personal information can be processed, including conditions where the processing must necessarily be carried out without the explicit consent of the data Subject. Of particular relevance to *PREVENT* are paragraph 1 (for the purposes of prevention or detection of crime) and paragraph 4 (for the discharge of any function which is designed for the provision of confidential counselling, advice, support or any other service).

4) Human Rights Act 1998

a) Article 8 of the European Convention on Human Rights (which is given effect by the HRA) provides that "everyone has the right to respect for his private and family life, his home and his correspondence", and that public authorities shall not interfere with "the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

5) Common Law Duty of Confidentiality

a) The key principle built up from Case law is that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission. Judgements have established that exceptions can exist "in the public interest"; confidentiality can also be overridden or set aside by legislation.

b) The Department of Health has produced a code of conduct concerning confidentiality, which is required practice for those working within or under contract to NHS organisations.

Information Sharing - Gateways, Exemptions & Explicit Powers for Police

1) Review these powers and exemptions to decide which apply to a case in hand.

2) Counter Terrorism & Security Act 2015

a) **S.36(3)** of the CTSA states:

i) *"A chief officer of Police may refer an Individual to a Panel only if there are reasonable grounds to believe that the Individual is vulnerable to being drawn into terrorism."*

ii) We can infer four things from this:

(1) That Police are expected to identify and refer Individuals whom they believe are vulnerable to being drawn into terrorism – the Police cannot simply ignore a potential issue in this area.

(2) When we CAN refer – i.e.: Police have developed a **reasonable belief** that the Individual concerned is vulnerable in the relevant sense.

(3) When we CANNOT refer – i.e.: when a reasonable belief of relevant vulnerability cannot be made out.

(4) That a reasonable belief requires a relatively high level of rigour (and therefore shared information for assessment), as per the use of the term in other policing contexts and law.

b) **S.38(1-5)** of the CTSA is concerned with co-operation and information sharing:

i) The partners of a Panel must, so far as appropriate and reasonably practicable, act in co-operation with the Panel and Police in the carrying out of their functions;

ii) The Panel Partners duty to act in co-operation with the Panel **includes the giving of information**

iii) BUT this co-operation extends only insofar as it is compatible with the exercise of the partner's functions under **any other** enactment or rule of law.

iv) Nothing in S.38 requires or authorises the making of a disclosure that would contravene the Data Protection Act 1998; a disclosure of any sensitive information.

3) **Data Protection Act 2018**

a) Police processes around handling data for the law enforcement purposes as set out in s.31 DPA, these being:

i) '…the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

b) Part of the data processed will be subject to the **sensitive processing** requirements as set out in S.35(3) DPA:

i) Sensitive processing relates to "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (Art 10 LED). The processing of such data will be carried out in accordance with s.35(4) or s.35(5) DPA.

c) Where processing is carried out pursuant to s.35(5) DPA, one or more of the following Schedule 8 conditions are met:

i) **Paragraph 1: Statutory (etc.) purposes.** This condition is met if the processing:

(1) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and

(2) is necessary for reasons of substantial public interest.

(3) This condition is met by virtue of the Police exercising their PREVENT Duty pursuant to s.29 CTSA and/or their common law duties of, inter alia, preserving order and PREVENT threats to public security, preventing crime and upholding national security. The processing is plainly carried out for reasons of substantial public interest, these being to safeguard Individuals and PREVENT radicalisation, with the corresponding criminality and risks to national security.

ii) **Paragraph 3: Protecting Individual's vital interests.** This condition is met if the processing:

(1) is necessary to protect the vital interests of the data subject or of another Individual.

(2) Radicalisation can lead to loss of life and limb of the subject and/or members of the public, and so it can be inferred that preventing this is a "vital interest", as described above.

iii) **Paragraph 4: Safeguarding of children and of Individuals at risk.** This condition is met if the processing is necessary for the purposes of:

(1) protecting an Individual from neglect or physical, mental or emotional harm, or

(2) protecting the physical, mental or emotional well-being of an Individual,

(3) the Individual is—

(a) aged under 18, or

(b) aged 18 or over and at risk - an Individual aged 18 or over is "at risk" if the data controller has reasonable cause to suspect that the Individual:

(i) has needs for care and support

(ii) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(iii) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) The condition is also met if the processing is **necessary for reasons of substantial public interest**,

(5) The condition is met where the processing is carried out without the consent of the data subject for one of the following reasons:

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

d) "The protection of an Individual" or "the protection of the well-being of an Individual" includes:

i) Protection relating to a **particular Individual**,

ii) Protection relating to a **type of Individual**.

e) So this condition is met where radicalisation puts children and vulnerable adults are at risk of harm (whether physical or mental), and the Police are unable to obtain consent for any of the reasons listed.

4) Crime and Disorder Act 1998

a) Section 115 confers a power to disclose information to a "relevant authority" on any person who would not otherwise have such a power, where the disclosure is necessary or expedient for the purposes of any provision of the Act.

b) The "relevant authority" means a chief officer of Police in England, Wales or Scotland, a Police authority, a Local Authority, a health authority or a probation committee in England and Wales, and includes an Individual acting on behalf of the relevant authority.

c) The purposes of the Crime and Disorder Act include, under section 17, a duty for the relevant authorities to do all that they reasonably can to PREVENT crime and disorder.

d) It is within the Police duty to advise non-Police Partners on crime prevention, and what may constitute criminological (and therefore in this case, **counter terrorism**) risk.

5) Common Law Powers

a) Because the range of Partners with whom the Police deal has grown - including the public, private and voluntary sectors, there may not be either an implied or explicit power to share information in every circumstance.

b) This does not necessarily mean that Police cannot share the information, because it is often possible to use the Common Law.

c) The decision to share using Common Law will be based on establishing a **policing purpose** for the activity that the information sharing will support, as well as an assessment of any risk.

d) The Police may rely on common law powers to process information in relation to their powers, which are to:

i) protect life and property;

ii) preserve order and PREVENT threats to public security;

iii) PREVENT and detect crime;

iv) bring offenders to justice; and

v) uphold national security.

e) These are supported, inter alia, by:

i) Rice v Connolly [1966] 2 QB 414 at [419B – C]: '[I]t is part of the obligations and duties of a Police constable to take all steps which appear to him necessary for keeping the peace, for preventing crime or for protecting property from criminal damage. There is no exhaustive definition of the powers and obligations of the Police, but they are at least those, and they would further include the duty to detect crime and to bring an offender to justice.'

ii) Regina (Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland and another (Equality and Human Rights Commission and others intervening), Regina (T) v Commissioner of Police of the Metropolis (Secretary of State for the Home Department intervening) [2015] A.C. 1065 at [1078]: 'At common law the Police have the power to obtain and store information for policing purposes, ie broadly speaking for the maintenance of public order and the prevention and detection of crime.'

iii) Regina v Chief Constable of the North Wales Police and Others, Ex parte Thorpe and Another [1999] Q.B. 396 at [409-410]: '...When, in the course of performing its public duties, a public body (such as a Police force) comes into possession of information relating to a member of the public, being information not *410 generally available and potentially damaging to that member of the public if disclosed, the body ought not to disclose such information save for the purpose of and to the extent necessary for performance of its public duty or enabling some other public body to perform its public duty...'

f) The Code of Practice on the **Management of Police Information** (**MoPI**) defines policing purposes as:

i) protecting life and property,

ii) preserving order,

iii) preventing the commission of offences,

iv) bringing offenders to justice,

v) any duty or responsibility of the Police arising from common or statute law.

g) In general terms, if the sharing of the information is for a purpose related to policing (as above) and the conditions of the Data Protection Act are satisfied, then it will be lawful.

6) **Local Government Act 1972**

a) Section 111 provides for Local Authorities to have "power to do anything [...] which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their functions".

b) One of the functions of the Local Authority under the "PREVENT Duty" / CTSA is to support and facilitate multi-agency Panels where the Police are a statutory Partner, and where the Police are recognised by merit of their statutory and Common Law duties, as holding the CT and crime-prevention risk.

7) **Local Government Act 2000**

a) Section 2(1) provides that every Local Authority shall have the power to do anything that they consider is likely to achieve the promotion or improvement of the economic, **social**, or environmental wellbeing of the area (emphasis added).

b) This can be extrapolated outwards to infer matters pertaining to include public protection, law and order and counter-terrorism.

8) **National Health Service Act 2006 and Health and Social Care Act 2001**

a) Section 251 of the NHSA 2006 and Section 60 of the HSCA 2001 provide a power for the Secretary of State to make regulations governing the processing of patient information. This takes precedence over more local regulations around patient information.

9) **Offender Management Act 2007**

a) Section 14 of the OMA 2007 enables disclosure of information to or from providers of probation services, by or to Government departments, Local Authorities, Youth Justice Boards, Parole Boards, Chief Officers of Police and relevant contractors, where the disclosure is for the probation purposes (as defined in section 1 of the Act) or other purposes connected with the management of offenders.

ANNEX 6: TRANSFERRING PREVENT CASES

1) There are circumstances where a Case may have to be moved between regions, perhaps because the Subject of the Case has also moved.

2) The PREVENT Policy (p23) provides guidance on the transferring of Cases between force-areas:

   a) In the event of a Case transfer between areas, the outgoing force must contact the new force at the point at which the move or potential move first becomes known

   b) The general principle is that Cases should be managed where the risk is and the NSIM multi-equity principles should be applied. In Cases where a Subject is detained under mental health or immigration legislation in an area outside of their normal place of residence, the relevant areas should discuss the Case and decide upon the area must suited to continue management of the Case on the basis of risk.

   c) Where such Cases are under Channel, transfers are not a Police decision and instead sit with the Channel Panel. In such Cases Home Office Channel Guidance must be followed.

   d) Any Case transferring between areas must have a DIF/VAF completed at the point of transfer by the outgoing force (with the exception of Dovetail Cases in which the LACC will complete an outgoing VAF if appropriate).

   e) The receiving force must complete a new DIF/VAF upon receipt of the Case (with the exception of Dovetail area Cases) and if it is a PLP Case a new CMP must also be completed and supervised reflecting the change in circumstances arising from the move between areas.

   f) As a general rule, although it is not yet defined in policy, where a transfer between forces happens, although the Subject should be put through the FIMU in the target force area, it is not necessary for CTCOs in the new Force-area to wait for de-confliction on an already open PREVENT Case with an existing CMP that has already been de-conflicted in a previous Force-area before they can work on the Case.

   g) Updates to this will be disseminated when the next PREVENT Practitioners Policy Document is completed and rolled out.

ANNEX 7: DECISION MAKING

1) The section explored how decisions are reached by CTCOs and CTCO Supervisors within the lifetime of a Case. This is applicable for practically every step of the CTCO & CTCO Supervisors' jobs, but particularly around the completing of the PGA and for PLCMPs.

Decision Making – National Processes & Guidance Manuals

1) There are a number of useful processes and manuals to assist and guide decision making within PCM. These are:
   - **a)** The CTCO Guide (this document).
   - **b)** The National Decision Model (NDM).
   - **c)** The Dynamic Investigation Framework (DIF).
   - **d)** Emerging & Residual Threat (ERT) definitions.
   - **e)** I&S

     iii) College of Policing: Menu of Tactics.

I&S

Decision Making – Authorised Professional Practice (Risk)

1) Making rational, effective and defensible decisions can be difficult, especially in the complex environment of policing, which is characterised by uncertainty, multiple views of a particular problem and numerous possible intervention points and solutions.
2) Characteristics such as these turn most policing decisions into risks. Police decision makers can, therefore, be more accurately described as professional risk takers, with risk taking being at the core of Police professionalism.
3) Although the majority of risk decisions that Police personnel make are successful, terms such as 'risk' and 'risk taking' have negative connotations. The media and public tend to focus on decisions that result in poor outcomes, and this can cause CTCOs to become risk averse, with some officers and staff afraid to make decisions in Case things go wrong.
4) The College of Policing (CoP) **Risk Authorised Professional Practice** (**R-APP**) provide direction in relation to decision-making within 10 main principles, available at the **CoP website.** The most pertinent of which are summarised below.
   - **a)** **Principles 1 & 2** recognise that the willingness to make decisions in conditions of uncertainty is a core professional requirement of all members of the Police Service and that the Police have a primary duty to do so in order to maintain the safety, security and wellbeing of Individuals and communities.
   - **b)** **Principle 4** acknowledges that harm can never be totally prevented and therefore risk decisions should be judged by the quality of the decision-making and not the outcome and that this applies even in the Case of serious harm.
   - **c)** **Principle 5** also notes that being "helpful" may create other risks for Police, in that assisting other agencies in meeting their responsibilities can set up other risks for the Police. An example of this within PREVENT would be where an Individual solely displaying mental health issues, in the absence of a PREVENT or wider CT concern, is adopted by a PREVENT Panel for supervision when that Individual should be supervised and triaged within an NHS environment.
   - **d)** **Principle 9** identifies that risk taking (decision making) relies on quality information and therefore the Police must work with Partner agencies and others to share relevant information about those who pose risk or those who are at the risk of harm. This sharing of information is essential to keeping people safe and the anticipated benefits can be summarised as:
     - **i)** Better informed decision making.
     - **ii)** Improved protection of Individuals at risk.

iii) Reduction in crisis through taking earlier effective action.

iv) Improved inter-agency working.

v) Better profiling of Individual need or risk.

vi) More effective intervention, support and targeting of resources.

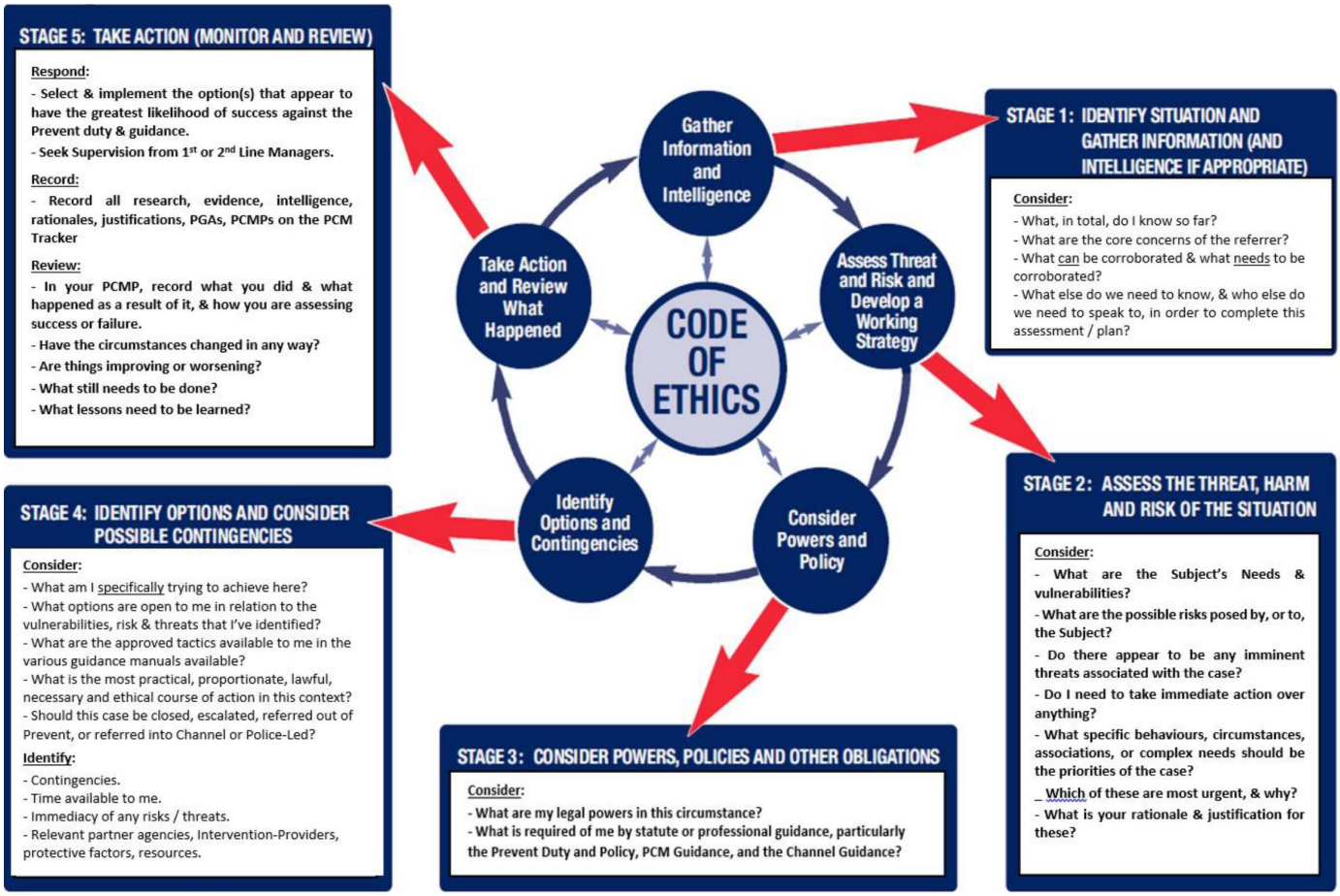
Decision Making – National Decision Model (PREVENT)

1) The **College of Policing** has approved the adoption of a single **National Decision Model** (**NDM**) for the Police Services in the UK.

2) This guidance document does not change the NDM. However it presents the NDM alongside the sorts of considerations CTCOs are required to make within the lifetime of a Case. See the PREVENT NDM flowchart (below).

3) The NDM recognises that CTCO decision making is a complex matter, executed in difficult circumstances, often within tight timeframes, and is open to subsequent challenge.

4) Many assessments and decisions are required throughout the lifetime of Cases, and the NDM should be used in conjunction with the DIF and the other, above-mentioned, national processes and guidance manuals. The decisions made must take into account the specific circumstances and have due regard for threat, risk and vulnerability.



Decision Making – CTCO Supervisors

1) CTCO Supervisors must be of at least the rank of Sergeant or Police Staff CTCO Supervisor (acting ranks are allowed providing the force has formally approved the acting rank). Constables and lowest Police Staff grades must never supervise cases.

2) Supervision is mandatory for all DIFs, Police created VAFs, Closure Reports, Case Management Plans and Police generated CMIS and PCMT entries.

3) Cases must be supervised with a frequency of no less than four weeks for High Priority Cases or eight weeks for Standard Priority Cases unless the case is monitored.

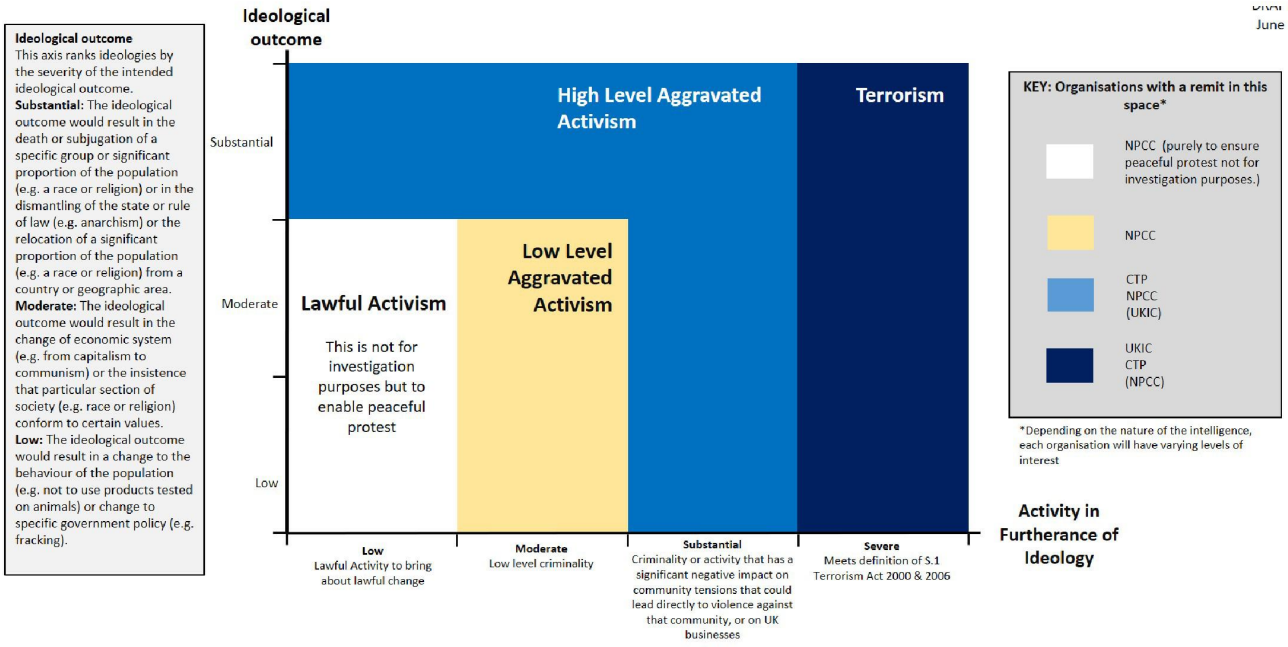
4) Monitored cases must be supervised at least every three months.

5) CTCO Supervisors should ensure that firstly the correct process is being followed under policy and then secondly that the process is completed to the required standard. This includes reviewing all CTCO uses of the DIF and VAF to ensure they have been completed to the required standard and that associated CMPs address all of the identified risks and that the proposed actions are specific, measurable, achievable, proportional and timely.

6) 2nd line managers must ensure that they establish a process to review a proportional number of cases within their area to ensure a consistent standard of decision making, case management and supervision.

I&S

ANNEX 9: PREVENT & PUBLIC ORDER (ACTIVISM – TERRORISM THRESHOLDS)



1) **Activity Definitions:**

   a) The matrix works by first measuring the level of Ideological Outcome of a group or individual, followed by the level of activity.

   b) The activity scale measures the level of activity a group or individual is associated with, in furtherance of their ideology. There are four levels of activity: Low, Moderate, Substantial, and High.

   c) Violence of any severity can be present in each level of activity, except Low. But it is only violence associated with, and in the furtherance of a group or individual's ideology, that is measured on the matrix.

   d) Travel to overseas conflict zones for unknown purposes or to engaged in combat not sanctioned by the UK government would be included in Substantial Activity.

   e) Community tensions will be affected increasingly as the level of activity increases. Local/regional community tensions are affected in Moderate activity, cross-regional/national community tensions are affected in Substantial activity, and national/international community tensions are affected in Severe activity.

2) **PREVENT Relevance:**

   a) Potentially any activity falling within the High Level Aggravated Activism designation, where it is not of Interest to PURSUE.

   b) Potentially any Low Level Aggravated Activism, where the basis of activism itself was in support of an issue that would be considered 'hateful' within UK legislation

3) **CPS Guidance for Offences During Protest, Demonstrations or Campaigns, & Subsequent Prosecution:**

   a) Headlines

      i) The rights of freedom of speech and to protest peacefully are protected by the law. However this right is not absolute, and it is unlikely to provide any defence when aggressive and threatening behaviour prevents people going about their daily lives.

      ii) Prosecutors must apply the principles of the European Convention on Human Rights (the Convention), in accordance with the Human Rights Act 1998, at each stage of a case. It is a defence to prove the conduct was reasonable and in accordance with the freedom of expression and other freedoms. If these freedoms are engaged, a justification for

interference with them (by prosecuting) must be established. A prosecution may only proceed if it is necessary and proportionate.

iii) Criminal law in respect of public order offences is intended to penalise the use of violence and/or intimidation by individuals or groups. In addition, behaviour which is repeated and unwanted by the victim and which causes the victim alarm or distress may constitute harassment. Such behaviour may also motivated by hostility to race or religion or other protected characteristics.

iv) A person may not however rely on a Convention right such as freedom of expression where they engage in any activity or perform any act aimed at the destruction or limitation of any of the rights and freedoms of others protected by the Convention. In these cases, the Convention right is not engaged and a suspect may not rely upon it.

b) Public Protests

i) Protests may take many different forms, ranging from action by one person acting alone to a demonstration attended by thousands of people. Freedom of speech and the right to protest peacefully are protected by the law (both the common law and the Human Rights Act 1998). Under the European Convention on Human Rights (ECHR), which is given effect by the Human Rights Act, Articles 10 (Freedom of Expression) and 11 (Freedom of assembly and association) are most relevant. However, freedom of speech and the right to peaceful protest are not absolute and the exercise of those rights can be restricted so long as any restriction is prescribed by law is necessary and proportionate.

ii) Examples of case law that considered these issues can be found within the full legal guidance, here. A non-exhaustive list of offences that may be committed arising out of a public protest can be found within the full guidance, at Annex A.

iii) The evidential stage should consider factors such as how an offender is identified in potentially large crowds, whether there was an element of planning before the commission of the offence can be proved, and if any electronic evidence to demonstrate an involvement in the commission of an offence is available. Some points to consider at the evidential stage can be found here.

iv) At the public interest stage, prosecutors must apply the public interest factors set out in the Code, as well has having regard to some of the factors set out here.

v) For further details see the full guidance on Public Protests here.

c) Public Order Offences

i) Related public order legislation ensures individuals rights to freedom of expression and assembly are balanced against the rights of others to go about their daily business unhindered. Relevant offences contrary to the Public Order Act 1986 may include threatening, abusive or insulting words or behaviour, or display of visible representations, which:

ii) Are likely to cause fear of, or to provoke, immediate violence: section 4

iii) Intentionally cause harassment, alarm or distress: section 4A

iv) Are likely to cause harassment, alarm or distress (threatening or abusive only words or behaviour only – not insulting): section 5.

v) It is a defence to section 4A and section 5 for the accused to demonstrate that their conduct was reasonable, which must be interpreted in accordance with the freedom of expression and other freedoms. If these freedoms are engaged, a justification for interference (by prosecution) with them must be convincingly established. A prosecution may only proceed if necessary and proportionate. Reference should be made to the charging standard purpose and the charging standard practice.

vi) The full guidance on Public Order Act offences can be found here.

d) Harassment and Stalking Offences

i) The offence of harassment contrary to the Protection from Harassment Act 1997 is committed where a person engages in a course of conduct which amounts to the harassment of another person, and they know it amounts to harassment

or they ought to know. Course of conduct is a fact-specific assessment. It requires behaviour on more than one occasion but this need not be the same behaviour on each occasion. Behaviour which begins as a legitimate complaint or inquiry may turn into harassment if unreasonably prolonged or persistent. Further information on elements of the offence of harassment can be found here.

ii) It is a defence to prove the conduct was reasonable which must also be interpreted in accordance with the freedom of expression and other freedoms. If these freedoms are engaged, a justification for interference with them (by prosecuting) must be convincingly established. A prosecution may only proceed if necessary and proportionate.

iii) The offence of stalking is committed when the harassment amounts to stalking; a non-exhaustive list of examples can be found here.

iv) Related charging guidance helps set out the difference between someone who is stalked and someone who is harassed, and if both could be applied.

v) The full guidance can be found here.

e) Hate Crime

i) Sections 28 to 32 of the Crime and Disorder Act 1998 provides that, where a series of existing offences including assault, criminal damage, stalking, harassment and public order offences are committed, and such an offence (i) was motivated by hostility to race or religion, or (ii) was accompanied by hostility to race or religion proximate to the commission of the offence, that a separate racially or religious aggravated offence is committed attracting a greater penalty.

ii) Any potential offence of incitement to racial or religious hatred or hatred because of sexual orientation should be referred to the Special Crime and Counter Terrorism Division for review.

iii) For those offences not covered but where hostility or hostile motivation towards race or religion is present, or hostility or hostile motivation towards disability, sexual orientation or transgender is present, this must be treated as an aggravating factor at sentence and stated as such in open court: sections 145/146 Criminal Justice Act 2003.

iv) Prosecutors must adopt a proactive approach to seeking evidence from the Police to help them to decide if a case can be prosecuted as a racially or religiously aggravated hate crime and that there is evidence that should be presented to the court at sentence.

v) If the case passes the evidential stage and it is a case of racial or religious hate crime, or it is motivated by discrimination against the victim's ethnic or national origin, or religion or belief, it is more likely that a prosecution is required in the public interest.

vi) For further details, see the full guidance here

f) Communications Offences and Social Media

i) Communications sent via social media may involve the commission of a range of existing offences against the person, public justice, sexual or public order offences. They may also involve the commission of communications offences (the communications offences) contrary to section 1 Malicious Communications Act 1988 (section 1) and / or section 127 Communications Act 2003 (section 127).

ii) Section 1 of the Malicious Communications Act 1988 and section 127 of the Communications Act 2003 criminalise the sending of certain communications including those alleged to be indecent, grossly offensive or menacing.

iii) Menacing means creating a sense of apprehension or fear in the likely recipient. There is a high threshold to meet the objective test of whether or not the communication is grossly offensive. A prosecution is only viable where the communication in question crosses the high threshold necessary to protect freedom of expression, even unwelcome freedom of expression, particularly in the course of robust political debate. Communication which is merely any one of the following, is likely to be protected as freedom of expression:

(1) Offensive, shocking or disturbing; or

(2) Satirical, iconoclastic or rude comment; or

iv) The expression of unpopular or unfashionable opinion about serious or trivial matters, or banter or humour, even if distasteful to some or painful to those subjected to it; or

v) An uninhibited and ill thought-out contribution to a casual conversation where participants expect a certain amount of repartee or give and take.

vi) A prosecution is only likely to be viable where a communication goes beyond the above. This is with reference to contemporary standards... the standards of an open and just multi-racial society assessing whether the particular message in its particular context is beyond the pale of what is tolerable in society.

vii) Prosecutors must be satisfied that a prosecution is required in the public interest and, where Article 10 of the ECHR is engaged, this means on the facts and merits of the particular case that it has convincingly been established that a prosecution is necessary and proportionate. Particular care must be taken where a criminal sanction is contemplated for the way in which a person has expressed themselves on social media. The full guidance sets out some relevant public interest factors to consider.

viii) Cases involving communications sent via social media that fall within category (4) of the guidelines except those charged by CPSD out of hours. The case will be reviewed for "grossness" and returned to Area to prosecute and/or communicate the decision.

ix) For further details, see the full guidance here

g) Public Interest Stage

i) Prosecutors should apply section 4 of the Code for Crown Prosecutors and all factors in favour and against a prosecution should be carefully balanced. Relevant factors to consider in this type of case might include:

ii) A prosecution is (also) more likely if the offence has been committed against a victim who was at the time a person serving the public.

iii) It is more likely that prosecution is required if the offence was motivated by any form of prejudice against the victims actual or presumed ethnic or national origin, gender, disability, age, religion or belief, sexual orientation or gender identity; or if the suspect targeted or exploited the victim, or demonstrated hostility towards the victim, based on any of those characteristics.

iv) Impact of the Community which is not restricted to communities defined by location and may relate to a group of people who share certain characteristics, experiences or backgrounds, including an occupational group.

v) Further factors tending in favour of a prosecution in the public interest include:

(1) Violent acts were committed that caused injury or it is reasonable to believe they could have caused injury;

(2) The suspect took a leading role in and/or encouraged others to commit violent acts;

(3) The suspect was in possession of a weapon at the time of the offence;

(4) The suspect took steps to conceal their identity;

(5) Significant disruption was caused to the public and businesses;

(6) Significant damage was caused to property

(7) The suspect has a previous history of causing violence, damage, disruption or making threats at public protests;

(8) Threats were made against an individual or business that caused or it is reasonable to believe they could have caused alarm, fear or distress.

(9) Further factors tending against a prosecution in the public interest include:

(10) The public protest was essentially peaceful;

(11) The suspect had no more than a minor role;

(12) The suspect has no previous relevant history of offending at public protests or in general;

(13) The act committed was minor;

(14) The act committed was instinctive and in the heat of the moment.

h) ECHR stage

i) The first step is to consider whether the activity involve freedom of expression and/or freedom of assembly and association. If it does, prosecutors should consider whether the activity is aimed at the destruction or limitation of any rights and freedoms in Schedule 1 of the Human Rights Act 1998. If protections of freedoms are engaged, the prosecution must be necessary and proportionate.

i) Conclusion

i) This guidance cannot cover every eventuality but intends to address in outline some of the possible criminal offences that may be encountered. Although each case must be considered on its own facts and on its own merits, there are general principles that apply in every case. All decision making must be in line with the Code for Crown Prosecutors, CPS policy and guidance and in particular, where freedoms are protected elsewhere in law, justification for interference with them must be established. A prosecution may only proceed if necessary and proportionate.

I&S

I&S

I&S

ANNEX 11: PROSECUTING RACIST & RELIGIOUS HATE CRIMES

1) This ANNEX sets out the factors to be considered when reviewing cases and prosecuting offences classified as racist or religious hate crime – a situation that can arise quite frequently within PCM (Channel and PLP). It also addresses the approach to be taken in other cases where race or religion are a factor. CTCOs should read this guidance along with the CPS's Public Statement on Racist and Religious Hate Crime, as it provides greater detail on some of the key areas of the policy. CTCOs should also familiarise themselves with stirring up hatred on the grounds of race or religion, the hate crime material on the Knowledge Hub and the Hate Crime page on the CPS website.

2) **Referral of Racist and Religious hate crime cases to CPS**

   a) The Director's Guidance on Charging requires offences classified as hate crime under CPS policies to be referred to a CTCO for early consultation and a charging decision, whether admitted by the suspect or not.

3) **Identification of racially and religiously aggravated crime**

   a) The CPS uses definitions agreed with the National Police Chiefs' Council to identify racist or religious incidents/crimes and to monitor the decisions and outcomes:

      i) "*Any incident/crime which is perceived by the victim or any other person to be motivated by hostility or prejudice based on a person's race or perceived race*", or;

      ii) "*Any incident/crime which is perceived by the victim or any other person to be motivated by a hostility or prejudice based on a person's religion or perceived religion.*"

   b) Some cases may need more than one flag, for example, cases that also involve domestic violence, rape, or homophobic, biphobic, transphobic or disability elements. Accurate flagging of cases is important: it means that CPS can monitor how these cases are handled and can report back to communities on our performance in tackling these types of hate crime.

4) **Case Building**

   a) CTCOs must adopt a proactive approach to seeking information to help them to decide if a case can be prosecuted as a racially or religiously aggravated hate crime and that there is evidence that should be presented to the court at sentence. If building a case involving racially and religiously aggravated crime, CTCOs should consider the following non-exhaustive set of issues:

   b) **Incident**

      i) Was there any use of derogatory language towards ethnicity, race, nationality or religion, (including caste, converts and those of no faith)?

      ii) Was it a sustained attack?

      iii) Did it involve excessive violence?

      iv) Was cruelty, humiliation or degradation involved?

      v) Was the area in which the incident occurred particularly associated with a specific community defined by race or religion or was this in response to or undertaken at a time coinciding with a specific festival, carnival or ceremony associated with a specific community and its ethnicity, race, nationality or religion?

   c) **Perpetrators**

      i) Was hostility based on the victim's race or religion (or presumed race or religion) demonstrated by the perpetrator?

      ii) Have there been any previous incidents involving the offender and hostility or targeted anti-social behaviour?

      iii) If so, what was the nature and location of previous incidents?

      iv) Have the incidents escalated in severity and frequency?

      v) Has opportunistic offending become systematic and regular targeting?

      vi) What was the role of any bystanders?

      vii) Were there multiple perpetrators condoning and encouraging, taking photos/videos?

viii) What evidence is there to suggest this is **not** a racially or religiously aggravated crime?

ix) If satisfied that there is sufficient evidence to prove that the offence is aggravated by hostility on the grounds of race or religion, CTCOs should make it clear to in any case papers.

5) **Racist and religious crime - the legislation**

a) Parliament has passed specific legislation aimed at outlawing crime where the offender is motivated by hostility or hatred towards the victim's race or religious beliefs (actual or perceived). It is important that CTCOs are aware of the full range of available offences when deciding on the most appropriate charge to prosecute in a particular case.

6) **Crime and Disorder Act 1998 (as amended)**

a) This Act created a number of specific offences of racially aggravated crime, based on offences of wounding, assault, damage, harassment and threatening/abusive behaviour. An amendment (December 2001) extended the scope of the Act by creating new specific religiously aggravated offences. The Act defines "religious group" as a group of persons defined by reference to religious belief or lack of religious belief.

7) **S145 Criminal Justice Act 2003**

a) S145 of the Criminal Justice Act 2003 imposes a duty upon courts to increase the sentence for any offence committed that involves either:

i) the offender demonstrating towards the victim of the offence hostility based on the victim's membership (or presumed membership) of a racial or religious group; or

ii) the offence being motivated (wholly or partly) by hostility towards members of a racial or religious group based on their membership of that group.

iii) Note that these are alternatives. This means that in a case where a demonstration of hostility can be proved, there is no need also to prove motivation, and vice versa.

8) **Definition of a "racial group"**

a) The Act says a "racial group" means a "group of persons defined by reference to race, colour, nationality (including citizenship) or ethnic or national origins."

b) The definition is wide and victims may come within the definition under more than one of the references. Gypsies and some Travellers, refugees or asylum seekers or others from less visible minorities would be included within this definition. While Romany gypsies have long been recognised as an ethnic racial group (*Commission for Racial Equality v Dutton* [1989] QB 783), in more recent times and certainly since the first instance discrimination case of *O'Leary v Punch Retail* (HHJ Goldstein, Westminster County Court, 29 August 2000), Irish Travellers have also been considered an ethnic racial group. Whilst this has not been considered by an appellate criminal court, the O'Leary case is regarded as being persuasive if the point is ever taken.

c) Whilst there has been no case law around Roma in the UK, the European Court of Human Rights recognises that the community forms a distinct ethnic group and CTCOs are recommended to apply the definition provided by the legislation to argue for inclusion.

d) Various cases in the past have considered what constitutes membership of a racial group. Some decisions have concluded that persons associated by their religious beliefs may also be part of a racial group. CTCOs should consider on the facts of each case if the aggravating feature arises from hostility towards a religious belief or a racial group (or a combination of both).

e) There has been a legal ruling that Sikhs can be included in the definition of a racial group (*Mandla v Dowell-Lee* [1983] 2 AC 548). In the Mandla case, reference is made to the judgment in *King-Ansell v Police* [1979] 2 NZLR 531 as being a persuasive authority for Jews being included in the definition of a racial group as well as a religious group. Although not criminal cases, further support for this proposition can be found in the cases of *R v JFS* [2009] UKSC 15 which related to the legality of the

admission policy of a Jewish secondary school and *Seide v Gillette Industries Ltd* [1980] IRLR 427 in which an Employment Appeal Tribunal ruled that anti-Semitic comments made by a fellow-worker were made because he was a member of the Jewish race, not because of his religion.

9) Definition of a "religious group"

a) The Act defines a religious group as, "a group of persons defined by reference to religious belief or lack of religious belief." This includes Muslims, Hindus and Christians, and different sects within a religion. It also includes people who do not hold any religious beliefs at all. Sectarian hostility is covered by this definition and hostility towards converts and apostates.

10) How to prove an offence was racially or religiously aggravated within the meaning of the Crime and Disorder Act 1998 and section 145 of the Criminal Justice Act 2003.

a) To assist CTCOs to build cases that will satisfy the criteria for an increased sentence under s145, the elements of each subsection that need to be satisfied are set out below, followed by the evidence that will be necessary or useful to establish those elements.

11) Demonstrating hostility:

a) The elements to be satisfied are that:

i) The offence to be sentenced has one or more identifiable victims.

ii) The victim (or one of them) belongs to a particular racial or religious group or there is evidence that the offender presumed that he or she did so at the time of the offence (whether or not that was in fact correct).

iii) The offender, by words or deeds or other indication, demonstrated (i.e. actually manifested or indicated) some hostility towards the victim based on the actual or presumed membership of a racial or religious group. Where the offence itself involves some hostile act towards the victim (i.e. an offence of assault) there must additionally be some evidence of a demonstration of hostility on grounds of actual or perceived membership of a racial or religious group. It need not be proved that the offender was actually motivated by any malevolence on grounds of the race or religion but it must be shown that, viewed objectively, he did in fact make some outward indication of hostility on that ground. Verbal abuse, referring to the membership of that group or a feature of it, will suffice provided it actually demonstrates hostility towards the victim. Expressions of, or behaviour consistent with, contempt for the individual victim is unlikely alone to suffice, unless it can be shown to amount to the necessary demonstration of hostility based on the actual or presumed membership.

iv) The demonstration of hostility must have occurred at the time of or immediately before or after the conduct element of the substantive offence.

v) In any case involving multiple offenders, consider first whether there is evidence that each offender, by his behaviour in committing the conduct element of the substantive offence, associated himself with the demonstration of hostility proved (in which case all will be liable for the aggravating feature). If there is no such evidence, can it be shown that the individual offender was himself responsible for the demonstration of hostility relied upon.

b) The following evidence will be necessary:

i) Evidence of the utterance, doing or showing of any indication of hostility towards the victim. The evidence should be as particular as possible as to the terms of the indication of hostility.

ii) The victim (or one of them) belongs to a particular racial or religious group or there is evidence that the offender presumed that he or she did so at the time of the offence (whether or not that was in fact correct).

iii) Alternatively and/or additionally, evidence that the offender either knew or presumed that the victim belonged to a racial or religious group.

iv) Evidence that the hostility referred to in (1) was based on the actual, known or presumed membership of a race or religion.

v) Evidence that the demonstration of hostility relied upon was more or less contemporaneous with the conduct element of the offence, or that it can immediately be related to it in time.

vi) In addition, evidence of some malevolence towards the victim based on his or her actual or presumed race or religion, although not necessary, will be useful. This need not necessarily be contemporaneous to the substantive offence.

c) It should be noted that mere evidence of the commission of the substantive offence against a victim who identifies with a race or religion will not suffice. That is not to say that it is irrelevant: evidence of the commission of an assault offence or one that involves the use or threat of violence may well be good evidence of the relevant hostility being present or demonstrated. Typically however there will be another explanation for the commission of the offence and so further evidence of a specific, express demonstration of hostility based on presumed or actual race or religion will be required.

12) Motivated by hostility:

a) The elements to be satisfied are that:

i) The offender can be shown to harbour a hostility towards a person or persons who belong to, or are presumed to belong to, a religious or racial group.

ii) At least one reason why the offender committed the offence was his hostility towards that person or such persons who belong to, or are perceived to belong to, this group i.e. his purpose or incentive for committing the substantive offence included that hostility, even if it was also motivated by other reasons. It need not be shown that it was his sole or main motivation.

b) It need not necessarily be the case that the immediate victim of the offence belongs to this group. Indeed, it is not necessary that there is one, or more than one, individual victim of the offence, provided that the directed hostility is one of the motivations. For example, an offence may be directed at:

i) A friend or associate;

ii) A Synagogue, Temple, Church or Mosque;

iii) An organisation known to support members of ethnic or religious groups.

13) The following evidence will be necessary:

a) Primary evidence, whether direct or circumstantial, from which it can be deduced or inferred that the offender has a hostility towards people (or one person) of a particular race or religion. The kind of evidence will vary from case to case but may well include, for instance:

i) words, whether contemporaneous or not;

ii) writings;

iii) social media postings;

iv) insignia;

v) membership of far right groups

vi) presence with others promoting such hostility or association with them;

vii) previous incidents of hostility, e.g. targeting only persons of a particular religion as the victims of criminal attacks or forms of abuse, such as a Jewish person's house for criminal damage but no other houses in the same street; and

viii) previous convictions for offences directed at similar victims.

b) Evidence from which it can be inferred that the current offence is motivated by the hostility referred to. In some cases the existence of the hostility and the fact of its contribution to motivation may derive from the same evidence and may be direct and simple: for example, the words accompanying the conduct element of the offence, as reported by the victim, may make clear the hostility of the offender for persons of a particular race or religion and the association of the feeling with the commission of the offence. In other cases a more determined search for such evidence will be necessary.

c) In cases where the obvious motivation for the commission of the offence is common to all such offending (theft, robbery, sexual offending, drugs offending, etc.) there will have to be discrete, additional evidence of motivation which displaces the obvious inference.

d) In cases where the offence charged usually has a fact specific motive (public order offences directed at individuals, offences against the person, etc.) it may be that the primary evidence readily gives rise to the conclusion that the hostility is based on race or religion. If not, some further, secondary evidence of motive will be necessary.

14) Incitement to Racial Hatred - Part III Public Order Act 1986

a) The Act defines "racial hatred" as hatred against a group of persons defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins). For an offence to be committed under any of these sections of the Public Order Act 1986, there has to be one of the acts described therein: it has to be "threatening, abusive or insulting", and it has to be intended to or likely in all the circumstances to stir up racial hatred. The words "threatening, abusive or insulting" are to be given their ordinary meaning and case law dealing with other provisions of the Public Order Act 1986 can assist with this.

b) Racial hatred is defined in section 17 of the Act. The prosecution must prove that hatred was intended to be stirred up or that it was likely to be stirred up. "Likely" does not mean that racial hatred was simply possible. We therefore have to examine the context of any behaviour very carefully, in particular the likely audience, as this will be highly relevant.

c) Article 10 of the European Convention on Human Rights [ECHR] allows freedom of expression save in certain limited circumstances. These circumstances include the offences contained within Part III of the Public Order Act 1986 (ss18-23).

d) Additionally, Article 17 of the Convention states: "Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention." Relevant case law includes *Glimmerveen and Hagenbeek v Netherlands* 18 DR [1987] and *Kuhnen v Germany* 56 DR [1988].

e) In deciding upon the public interest of charging these offences it is essential that CTCOs keep in mind that in a free, democratic and tolerant society people are able to robustly exchange views, even when these may cause offence. However, the rights of the individual to freedom of expression must be balanced against the duty of the state to act proportionately in the interests of public safety, to prevent disorder and crime, and to protect the rights of others.

f) All such allegations are by their very nature highly sensitive. For that reason, and to ensure a consistent approach, any allegation under this legislation, must be referred by the relevant CPS Area to **the Special Crime & Counter Terrorism Division (SCCTD)**. Referral means the submission of a report by the Area to enable SCCTD and the Area to have an informed discussion about where the responsibility for the case should lie.

g) When an Area becomes aware of such a case, it should be referred to SCCTD within seven days. If it is decided that the case should be prosecuted as an offence of incitement to racial hatred, SCCTD will take over the conduct of the case from the Area. If SCCTD considers that it is clearly a case where incitement to racial hatred does not apply, the case should be returned to the Area within seven days of that decision being made.

h) If SCCTD decides to deal with a case, the file is held there and dealt with there. Thereafter, cases can only proceed with the consent of the Attorney General.

15) Racial and Religious Hatred Act 2006 - Stirring Up Religious Hatred

a) The Racial and Religious Hatred Act 2006 came into force on 1 October 2007. It created new offences of stirring up religious hatred, which are significantly different from the race hate offences contained within Part III of the Public Order Act 1986. The Act defines "religious hatred" as hatred against a group of persons defined by reference to religious belief or lack of religious belief.

b) The offence is committed if a person uses threatening words or behaviour, or displays any written material, which is threatening, if he intends thereby to stir up religious hatred. Threatening is the operative word, not abusive or insulting. Possession, publication or distribution of inflammatory material is also an offence. The offence can be committed in a public or private place, but not within a dwelling, unless the offending words and behaviour were heard outside the dwelling, and were intended to be heard. The defendant must intend to stir up religious hatred; recklessness is not enough.

c) There is a freedom of expression defence contained in Section 29J, which confirms that nothing in the Act "... prohibits or restricts discussion, criticism or expressions of antipathy, dislike, ridicule, insult, or abuse of particular religions, or the beliefs or practices of its adherents."

d) Prosecutions for this offence require the consent of the Attorney General and are dealt with under the same arrangements as offences of inciting racial hatred. However, CPS Areas are required to carry out an initial review and prepare a report if the case is to be referred to SCCTD confirming that there is at least on the face of it evidence of the required legal elements.

16) Racialist chanting at football matches - Section 3 Football Offences Act 1991 (as amended)

a) This offence is committed when a group of people, or one person acting alone, chants something of a racialist nature at a designated football match. "Racialist" means the same as "racist". To prove this offence, the prosecution has to show that the chanting, which means the repeated uttering of words or sounds, was threatening, abusive or insulting to another person because of that person's colour, race, nationality (including citizenship) or ethnic or national origin. It is not necessary to prove that the chanting was directed at a particular individual or group, although it will often be directed at a player or players from Black and minority ethnic communities.

b) The offence only applies to a "designated" match as specified in the Football (Offences) (Designation of Football Matches) Order 2004, namely, one involving a club that it a member of the Football League, the Football Association Premier League, the Football Conference or the Scottish Football League or the Welsh Premier League, or whose home ground is for the time being situated outside England and Wales, or represents a country or territory. The definition also includes a match in competition for the Football Association Cup (other than in a preliminary or qualifying round).

c) If convicted, the accused person can be fined (level 3), and, in addition to any other penalty, banned from attending football matches both in this country and abroad. Even when a person is not charged with an offence, a magistrates' court may issue a similar banning order against a person who has been involved in violent behaviour before, if the court is satisfied that this would help to prevent violence or disorder at football matches in the future. The police (and not the CPS) have the power to apply to the court for a banning order in these circumstances. Breach of a banning order is punishable by a maximum penalty of up to six months' imprisonment. The crime does not apply to chanting which is of a religious nature. In such circumstances, it may be appropriate to charge religiously aggravated public order offences.

d) This offence is aimed at specific behaviour within football grounds at designated matches and was introduced to combat the problem of mass racist chanting. However, this offence should not be seen in isolation and it is not the only legislative tool available to deal with racist or religious football related crime.

e) In some situations, it might be more appropriate to charge other offences, such as specific racially or religiously aggravated public order offences. This may be the case, for example, where:

- **i)** the offence is committed outside the stadium at a designated football match;
- **ii)** a public order offence is committed where religious as opposed to racist hostility is demonstrated to the victim or victims; or
- **iii)** racial abuse and harassment of black and minority ethnic players takes place at a non-designated football match, such as at an amateur game.

17) Other religious offences

a) In addition to the religiously aggravated offences, CTCOs should be aware that there are several other statutory offences designed to protect acts of worship of various kinds which may be useful offences for CTCOs to bear in mind.

b) Section 2 of the Ecclesiastical Courts Jurisdiction Act 1860 creates an offence of violent or indecent behaviour in any place of worship that has been certified under the Places of Worship Registration Act 1855 and the Act also affords protection to a person preaching or carrying out other religious duties. Mosques and synagogues are certified and are therefore covered by this legislation.

c) The penalty on conviction is a level 1 fine or up to two months' imprisonment. CTCOs should consider if another charge with a higher maximum penalty is more appropriate to deal with the kind of criminal behaviour which could be covered by section 2 of the 1860 Act. There might be circumstances, however, in which a section 2 offence is more appropriate simply to mark the anti-religious nature of the offence and where the court's sentencing powers for that offence are considered sufficient.

d) Section 36 of the Offences Against the Person Act 1861 creates an offence of assaulting 'a clergyman or other minister' or preventing them from officiating at religious services. This is an either way offence which carries a maximum penalty of two years' imprisonment on indictment.

e) There are also specific offences under the Cemeteries Clauses Act 1847 and the Burial Laws Amendment Act 1880 of causing disturbances in cemeteries and disrupting or obstructing burials respectively.

18) Victim and Witness Issues

a) To ensure that 'vulnerable' and 'intimidated' witnesses have access to the support they need, it is important for CTCOs to be familiar with CPS Operational Guidance in relation to the Victims' Code and with legal guidance on Special Measures.

b) The use of Victim Personal Statements should be encouraged in all hate crime prosecutions and requests should be made to the police at the earliest opportunity. A Community Impact Statement (CIS) may also be made to show the impact of offending on the wider community. For more information, please see the CPS guidelines on the use of CIS in hate crime cases.

c) Victims of hate crime are entitled to an enhanced service under the Victims' Code and in the event of a decision to end the case or to substantially alter charges, the victim must be notified of the reasons within one day. The victim should also be advised how they can access further information from the CPS and seek a review of the decision.

d) A meeting must be offered to the victim in hate crime cases in accordance with the Victims' Code. The meeting could be a dedicated teleconference or a face-to-face meeting. A meeting is not required when the CPS makes a decision not to prosecute during a charging consultation save for in homicide cases.

19) Withdrawal

a) In cases with a racist or religious element - as in all cases - the reviewing CTCO should consider the Code for Crown Prosecutors with regard to the determination of the public interest. The CPS prosecutes on behalf of the public at large and not just in the interest of any particular individual. However, when considering the public interest, CTCOs should always take into account the consequences for the victim of the decision whether or not to prosecute, and any views expressed by the victim.

b) Many members of BAME communities and faith communities do not report racist or religious crime to the police because of a lack of confidence in the criminal justice system. When offences are eventually reported, previous failures to report should not be seen as diminishing a witness's credibility.

c) In cases where the victim or witness has reported a case to the police, the defendant has been charged, and the victim or witness then decides that they no longer wish to give evidence, it is essential that Police make full enquiries into why support for the prosecution has been withdrawn. In these cases, the CPS will:

i) ask the police to take a written statement from the victim explaining the reasons for that withdrawal, confirming whether the original complaint was true and identifying whether the victim has been put under any pressure to withdraw support;

ii) ask the police to give their views and, where appropriate, consult the Area Hate Crime Co-ordinator.

d) The College of Policing Hate Crime Operational Guidance (2014) contains guidance on the information the police should provide to the CPS to accompany a withdrawal statement. As a result of receiving the withdrawal statement and accompanying police report, CTCOs and their Supervisors may need to consider whether further charges, for example, witness intimidation or harassment are appropriate. It may also be appropriate to ask the police to offer the victim the services of a specialist support agency if this has not already been done. The CTCO should also liaise closely with the Witness Care Officer to establish what support has been provided to the victim and to establish whether it would be appropriate to offer the victim the services of a specialist support agency if this has not already been done. The CTCO must also have regard to any special measures that may help the victim or witness to give evidence.

20) Continuing a case where the victim indicates a withdrawal of support

a) If a special measures application is not possible or the victim remains unwilling to give evidence, consideration must be given to whether any of the following options is possible and appropriate:

i) proceeding without using the victim's evidence; for example, by relying on statements from other witnesses, 999 call recordings, admissions in interview, CCTV evidence, scientific evidence, photographs and officers' statements;

ii) making a hearsay application under section 116 of the Criminal Justice Act 2003;

iii) compelling the victim to give evidence; or

iv) discontinuing as a result of the victim withdrawing support for the prosecution.

b) In addition to the evidence of the nature and seriousness of the offence, background information is crucial in helping a CTCO to make the correct decision about how to proceed in a case where the victim has withdrawn their support for the prosecution. Some factors that should be considered include:

i) the ability of the victim to give evidence;

ii) whether there is an on-going relationship between the victim and the defendant;

iii) if there is an on-going relationship, the history of that relationship and any previous incidents;

iv) the likelihood of the defendant offending again;

v) the impact on the victim of proceeding or not proceeding with the case; and

vi) whether there have been any threats made since the incident.

21) Witness Summons

a) Section 169 of the Serious Organised Crime and Police Act 2005 allows the court to issue a witness summons if it considers it to be in the interests of justice to do so.

b) Before taking a decision to issue a summons to require the victim to give evidence, CTCOs must make enquiries to satisfy themselves as far as possible that the safety of the victim will not be endangered by their decision. The safety of the victim is a prime consideration. If the reason for a victim or witness's withdrawal is based on fear or intimidation, the CTCO needs to demonstrate such evidence. This will allow appropriate decisions to be made about any applications under section 116(2)(e) of the Criminal Justice Act 2003. Such applications are only likely to succeed where there is other evidence to put before the court. Section 116 applications are often unsuccessful when the victim is the only witness to the offence, because in such cases it is very difficult to satisfy the court that justice is being served when the defence cannot cross-examine the only witness against them.

c) If there is insufficient evidence to continue without the evidence of the witness or victim, the reviewing CTCO will need to weigh up whether the facts of the case are sufficiently serious to require the victim or witness to attend court under a witness summons .The final decision is that of the CTCO, but the decision to compel a witness to give evidence may be construed negatively, so every attempt should be made to regain the victim's or witness's support for the prosecution wherever possible.

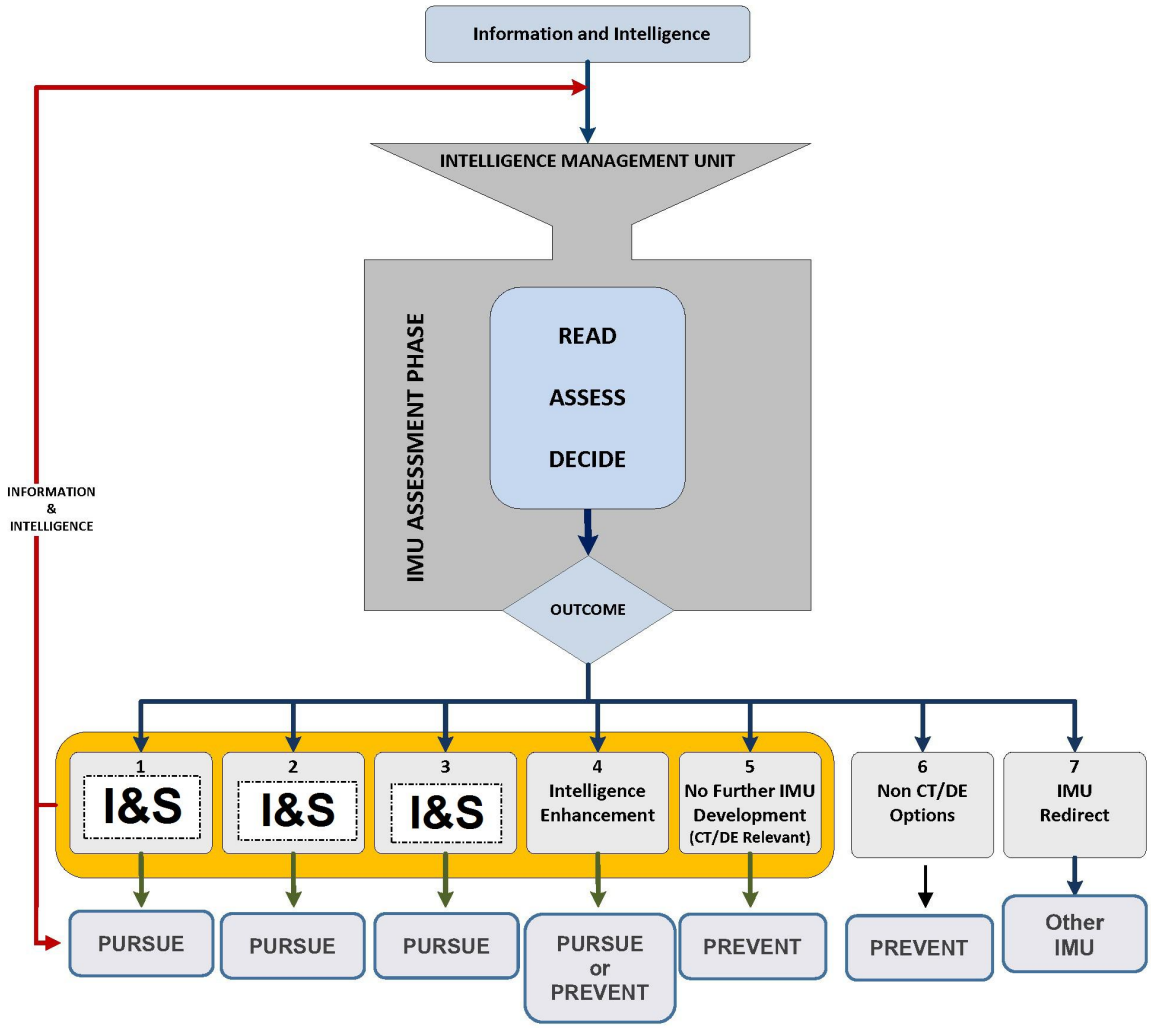
ANNEX 12: RADO ASSESSMENT OUTCOMES & PREVENT

1. CTCOs should bear in mind that the NSIM Guidance is being updated, and references to "CT/DE" will be changed simply to "CT" in lines with the rest of the network.
2. The current version of the NSIM Assessment Model and the PREVENT Annex of thr NSIM Guidance are available here:

NSIM-IMU-Assessment-Model.pdf

NSIM Prevent Guidance for FIMUs.pdf

3. RADO outcome flowchart and PREVENT:



4) ANNEX 13: GLOSSARY OF TERMS & CONTENTS

1) In this section we provide a list of the key terms used throughout this document and in the PREVENT network, along with explanations and further details of what is meant by them in the CTP PREVENT context.

Baseline Beliefs & Behaviours

1) Wherever possible, try to establish a Subject's "baseline beliefs and behaviours". This will help assess the incoming risk & vulnerability associated with a Subject, & can also help identify escalations, de-escalations & the most appropriate interventions to address them.

- **a)** A Subject may appear to be relatively low risk or low vulnerability, but changes in personal circumstances may have an aggravating or "force-multiplying" effect on engagement factors / indicators, propelling Subjects into riskier behaviour or more acute vulnerability.
- **b)** Escalations & de-escalations are demonstrated through a Subject's changing attitudes & behaviours in relation to his/her baseline behaviour, perhaps due to changes in his/her circumstances or the effects of interventions. For example:
  - **i)** Depending on their context, a Subject with long standing, hateful or bigoted beliefs might demonstrate behaviours that, whilst offensive & possibly indicative of "lower-level" offending, are not necessarily extremist & do not automatically suggest mobilisation towards unlawful extremist conduct or TACT offences.
- **c)** Factors to be considered when establishing a baseline should include the nature, context, frequency, duration & "fixation" of activities & behaviours that might be of concern in terms of CT /DE, including changes in relation to:
  - **i)** Vulnerability / complex needs, ideology, exposure to individuals or institutions of concern, engagement, grievance, intent, capability, opportunity, & particularly any Mobilisation Identity, fixated, or trigger behaviours.

Capability

1) "Capability", as used throughout this guidance document, refers to the extent of the power or ability of a Subject to commit terrorism connected offences.

2) Relevant Offences play a prominent role here.

- **a)** Plots to cause widespread harm with bombs or through rampaging-shooter attacks are relatively difficult to resource, or need specific training or practice. These sorts of attacks tend to require a relatively high level of capability, a lot of time to plan & execute.
- **b)** These requirements are lessened dramatically if Subjects choose to conduct "lower level" or more technically primitive attacks. Many of the most "successful" terrorist actions in recent years have involved low-tech, low skill, low-resource, opportunistic attacks using weaponised cars, kitchen knives & noxious materials.
- **c)** So what Subjects are capable of **psychologically**, and what they **believe** they are capable of, is often as relevant as what their **physical** or **technical** capabilities are when considering potential risk.

3) **Capability & the VAF:**

- **a)** Although information suggesting the development of specific terrorist capabilities (like bomb making) might probably render an Individual unsuitable for the Local Authority led programme of Channel, it would be inappropriate to overlook this dimension entirely when completing VAF assessments. To the extent that the Individual possesses generic capabilities such as intelligence, persuasive communication skills or advanced IT skills, these bear on the potential to commit terrorism connected offences if the Individual is radicalising. They may also provide clues as to what sort of intervention may be effective and where protective influences may need to be put in place.

Data vs. Information vs. Intelligence in PREVENT

1) **Data, Information & Intelligence:**

   a) These terms are referred to within legislation and within the various policies and procedures used by Police, and there is sometimes confusion as to what is meant by each instance. The precise boundaries between "data", "information" and "intelligence" can be quite hazy, depending on context. For the purposes of CTP PREVENT, as long as CTCOs obey any data, information & intelligence handling rules relevant to the specific matter in hand, CTCOs should not worry overmuch about the grey areas between data, information and intelligence. Data and information tend to be used interchangeably by our PREVENT Partners, for instance – hence our use of "**Data Sharing Agreements**", which can, have and should (in some cases) include various combinations of data, information and intelligence.

2) **NSIM:**

   a) The NSIM Guidance (see the NSIM Annex in this document) defines information very broadly as being **all forms** of information obtained, recorded or processed, including personal data and intelligence generated or supplied by a partner or third party. So in NSIM, "information" is a combination of what we define below as data, information and intelligence. Essentially, FIMUs may at different time require any and all of these, hence they use this catch-all phrase for them to keep things simple.

   b) However, NSIM also refers separately to intelligence, because although intelligence generated by third parties may still count as information when it is supplied to a FIMU, it is essentially not yet counted as **FIMU intelligence.** Hence FIMUs define intelligence as information (as described above) that they have obtained and subjected to their defined evaluation and risk assessment process in order to assist with decision making.

3) **Breaking it Down for Partnership Working:** Because CTP PREVENT may deal with other agencies and units that refer to data, information and intelligence differently, here follows a very basic, non-legislative guidance around the differences between **data**, **information** and **intelligence**.

   a) **Data:**

      i) Data is the rawest form of recorded material. It is the unadulterated, factual detail around a circumstance. Data is an presentation of something that has been recorded, or that is viewable, **"as-is"**, without any narrative or context around it, or without an interpretation or assessment of what has happened, but where it is still recorded in a manner that can be reviewed if necessary.

         (1) In simplistic terms, data could be described as factual recordings of "what" and "where", without further context, narrative or pattern.

            (a) Example: A recording of CCTV with sound of **everything** that happens at a specific desk in an office, 24 hours a day, for a full year, along with a key-stroke log of every single computer terminal in the building for that same week.

   b) **Information**:

      i) **Information** is generated by the simple process of bringing related elements of data together within a context. So "information" is what we have when have we take cold data around an event or Individual and put it into a "narrative" to inform us about a particular matter.

      ii) "Information" is the **context** around data that assists us in answering a specific question.

         (1) In simple terms, information could be described the factual recordings of "what" and "where", along with "when" and "how".

         (2) So "information" is data put within a **context**, a uniting narrative or a pattern, in order to answer a simple question.

            (a) Example: The same recording of CCTV with sound for everything that happens at a specific desk in an office, 24 hours a day, for a specific week, **filtered** to show only the comings, goings and all activities of one particular

employee, along with the computer key-stroke log filtered to show only what the that same employee did for that same week.

(b) All this answers the simple question: what did that employee do at his desk in the office for that week?

c) Intelligence:

i) Contrary to popular depictions, intelligence is not only highly-protected or clandestinely-collected material, (although obviously it *can* involve this as well).

ii) "Intelligence", for our purposes here, is any information that has been formally **assessed** in a structured way and/or any information that has been **analysed** in order to **make plans** or drive **decisions**.

iii) So intelligence is the **development** of already collected information, with the intention of deciding upon some sort of action (or wider assessment) around what has been learnt.

(1) In simple terms, intelligence could be described the factual recordings of "what", "where", "when" and "how", along with explorations of "why".

(2) So this is data, contextualised into information, then interrogated / analysed in order to extrapolate meaning; to tell a story; to identify an understand a specific patterns; to conclude something very particular from the information at hand, and of course the deductive reasoning around it.

(a) Example: The filtered CCTV and key-log record focused on one particular employee, analysed and compared with other records in order to assess a claim that the employee has been involved in fraudulent activities, and if so, to help devise an investigation and a disruption and prosecution plan around the Case.

2) Hard Copy, Verbal, & Soft Copy:

a) These can enter into the PREVENT Network from a variety of sources and in a number of formats. All potentially PREVENT or wider CT relevant material must be directed to a FIMU for assessment. Information and intelligence received in **hard copy** or **verbally** should be converted to **soft copy** as soon as practicable.

i) Hard Copy: Potentially relevant material received in a physical format, e.g.: printed photographs, documents or written correspondence.

ii) Verbal: potentially relevant material received by any other "non-durable" means, e.g.: through a telephone conversation or other personal communication.

iii) Soft Copy: potentially relevant material received in an electronic format, e.g.: system messaging, email, Word documents and digital images.

DDP – The Desistance & Disengagement Programme

1) The PREVENT strand of CONTEST 2018 details additional targeted support through the Desistance and Disengagement Programme (DDP), which focuses on rehabilitating those who have been involved in terrorism or terrorism-related activity and reducing the risk they pose to the UK. The programme provides support to individuals who have been convicted of a Terrorism Act (TACT) or TACT-related offence, as well as those subject to Terrorism Prevention Investigation Measures (TPIMs) and those who have returned from conflict zones and are subject to Temporary Exclusion Orders (TEOs). Further information is available on the Home Office website.

Dynamic Investigation Framework

1) The DIF is CTP PREVENT's bespoke vulnerability, risk and threat assessment. It is a dynamic reflexive system, designed to be improved and updated as new research arises, issues are identified or circumstances change. It was created to address the reality that PREVENT does not "only" look to deter, divert and desist the mass-killings and murders of the more obvious kinds of

terrorism. PREVENT also seeks to identify people who are at risk of being drawn into committing **any** terrorism offences. (See the terrorism legislation section near the start of this document for details).

2) The DIF is designed specifically for UK CTP PREVENT to identify extremist grooming, radicalisation or escalation towards ANY terrorism offences, not just murder or massacre. It was built upon the VAF and it attempts, as far as is possible, to replicate the language in the VAF in order to enable consistency across PREVENT, inside and outside of the Police. All the VAF considerations are included in the DIF, but the DIF unpicks some of the VAF's considerations into more granular detail, whilst also drawing upon:

- **a)** Other vulnerability and risk assessments used by UK Police outside of extremism & CT.
- **b)** Criminological research, such as criminal opportunity, grooming patterns & tactics, and notions of motive (to name a few).
- **c)** The published research underpinning other CT and extremism risk assessment tools, including, but not limited to:
  - **i)** ERG 22+ & VAF.
  - **ii)** CTP Disruption Guide.
  - **iii)** NCA Disruption Manual.
  - **iv)** CTP Threat Finance Toolkit.
  - **v)** TRAP-18, VERA II & REGULUS.
  - **vi)** College of Policing: Menu of Tactics.
  - **vii)** North West CTU Intervention Toolkit.
  - **viii)** CPS Guidance for Policing & Prosecuting Political Protests.
- **d)** Up-to-date academic & practitioner research concerning Preventing Violent Extremism (PVE) & Countering Violent Extremism (CVE), particularly, but not limited to:
  - **i)** Terrorism "Triggers" & "tipping points".
  - **ii)** Escalation, Mobilisation & Warning Behaviours.
  - **iii)** "Lone Actor" Terrorism (particularly the **PRIME** research).
  - **iv)** Radicalisation "Pathways" & vulnerability indicators (incl. **PERICLES, CREST** & **RAN** publications).

Engagement Factors & Indicators

1) "Engagement Factors", as used throughout this guidance document, are the various **factors** and **indicators** that can help illuminate the **reasons** or **motivations** for a Subject's attraction to, involvement in, extremists / extremism and terrorism offences.

2) Motivations may be opportunistic, criminal or political, but is also always personal. It is the personal nature of the motivation that is important to understand in order to map how the Individual became engaged and to be able to make intervention relevant. The true motivation may be masked by political rhetoric and/or can operate outside of awareness such that it may not be fully understood even by the Individual himself. Unmasking this can help to unhook the Individual from his ideology, group or cause.

3) Although extremism & terrorism offences are **our** problems with a Subject, the Subject may perceive them as **answers** to whatever problems they themselves may be facing. These underlying issues are the various vulnerabilities, complex needs, risk factors and other contextual influences that form the **push-and-pull** factors, or even triggers, on an Subject's pathway towards terrorism.

4) Engagement factors are sometimes referred to as "psychological hooks". These are the parts that need to be reached for an intervention to be personally relevant to an Individual and to be effective. They include needs, susceptibilities, motivations and contextual influences and together map the Individual pathway into extremism.

5) The **Radicalisation Awareness Network** (**RAN**) provides a very helpful overview[27] of nine **thematic risk areas** that have been adapted and re-presented below. These are relevant to our understanding of where engagement factors / indicators might emerge, and where (and how) they can develop or be "groomed":

[27] "Protective & promotive factors building resilience against violent radicalisation"; Stijn Sieckelinck & Amy-Jane Gielen; RAN ISSUE PAPER, April 2018.

a) Social media,

b) Social factors, e.g. marginalisation, discrimination,

c) Psychological trauma, e.g. post-traumatic stress disorder (PTSD),

d) Group dynamics, e.g. friends who are active in extremist networks,

e) Recruitment strategies, e.g. being actively and deliberately groomed,

f) Individual social-psychological factors, e.g. anger, a sense of injustice,

g) Ideological factors, e.g. Salafi-jihadi interpretations of Islam, or "White Supremacy",

h) Political factors, e.g. narratives of "us versus them", dissatisfaction with governmental policies,

i) Culture and identity crises reinforced by occupying the indistinct space between cultures, e.g. uncertainty around "self" and where one belongs in society.

Exposure to Extremism & Radicalisers

1) "Exposure", as used throughout this guidance document, refers to the **type** of contact, connections or associations between a Subject and extremists / TACT offenders, their ideologies or other Individuals or institutions of concern.

2) There is often crossover between types of exposure, although it is **sustained** or **acutely influential** or **traumatising** exposure that is of most relevance to CTP PREVENT. The nature and extent of concerning exposure experienced by a PREVENT Subject needs to be explored very carefully by CTCOs. Exposure can be:

a) **Self-Instigated** (for the **"self-radicalised"**):

i) Subjects searching out by and for themselves, and/or, directly identifying with, and/or becoming obsessed with,

(1) Terrorists / TACT offenders,

(2) Proscribed organisations,

(3) Extremists or extremism,

(4) Causes or movement associated with any of these.

ii) **NB:** "self-instigated" exposure may be exacerbated by some symptoms of an MH or developmental issue, a combination of other complex needs, or an entrenched fascination that risks going beyond fascination into the realms of emulation.

b) **Groomed:**

i) Involving the targeted radicalisation of the Subject by someone else.

ii) This is the deliberate manipulation of an Individual by another party, in order to draw the target into support for terrorism and/or the extremism and/or proscribed organisations. Grooming in this context aims to create emotional connections that deepen engagement factors and the personal identification between a Subject and an extremist group, cause or ideology, eventually building intent and capability within the Subject, and in the most acute Cases pushing a Subject into actual mobilisation towards terrorism offences.

c) **Coercive**:

i) Vulnerable Subjects do not necessarily have to "like" or identify with terrorists, extremists or radicalisers that they have been exposed to in order to be influenced or controlled by them. Sometimes even **victims** of terrorists or extremists may themselves develop concerning engagement factors in some form:

(1) Consider intimidation, coercion, blackmail or even "Stockholm Syndrome"[28].

(2) Bonds between captors & captives could form as a sort of psychological defence mechanism to cope with trauma. People held in helpless states may sometimes develop sympathy for the goals of their captors and/or negative feelings towards authorities. Seek advice wherever there are concerns.

[28] Where there is a potential concern around any complex MH issue, CTCOs must seek the advice and support of MH professionals from the VS Hubs as soon as possible.

(3) This could apply to victims of sexual abuse, forced prostitution, slavery, trafficking, cults, prisoners of war, or people held in concentration camps, hard labour camps, or terrorist training camps.

d) Extra-Curricular:

i) This refers to Subjects who are students or teachers at concerning educational establishments that follow unlawful curricula, or without oversight by the relevant authorities, or Subjects who are **home educated** by extremists.

(1) Note that the study of current or historical terrorism, extremism or proscribed groups but within a supervised classroom environment as part of a lawful curriculum within the UK should not be a problem to PREVENT, although obviously each referral and Subject must be judged on its merits and on a Case-by-Case basis.

(2) Individuals and groups operating **within** legitimate institutions like universities, colleges or student unions, may still be targeted by extremist groomers, e.g.: within political, religious, or social activist student groups, etc..

e) Accidental or **Incidental:**

i) Although it should not be assumed without a wider context or other PREVENT concerns, persistent or particularly traumatising exposure to extremists or their material **could** generate engagement factors in a Subject, even if there is no direct or deliberate grooming or coercion involved.

ii) This may have particular relevance when considering Subjects suffering from trauma / PTSD.

Extremism – CTP PREVENT Operational Guidance

1) Until "extremism" has a definition linked to legislation, CTCOs should consider the following operational guidance:

a) Although professional judgement around the context of behaviours is always required, for our purposes within PREVENT, **"EXTREMISM"** & **"EXTREMIST"** *may* be suggested by any of the following:

i) Someone whom a **Vulnerability Support Hub**, or another relevant MH professional within PREVENT, has identified to CTP PREVENT as being of concern in relation to "extremism".

ii) Someone who **encourages**, **supports**, **defends** or seeks to **emulate**:

(1) Terrorists, terrorism or any other offences within UK terrorism legislation, or;

(2) Serial killers where there was a stated political or hate-based motivation, or;

(3) Mass murderers of any kind or for any reason, or;

(4) Political assassins or hostile-State actors.

iii) Someone who, for **political**, **religious**, **racial** or other single-issue **ideological** reasons, **encourages**, **defends**, **threatens** or **enacts** any of the following:

(1) Behaviour that would fall within UK terrorism legislation,

(2) High level aggravated activism, or other criminal or antisocial behaviour with a deliberate hate element,

(3) Even without a hate element: Murder; Wounding or GBH; Rape or Assault-by-Penetration; Arson or Aggravated Criminal Damage; Riot, Violent Disorder, or Affray.

iv) Membership in, pursuit for membership in, or deliberately promoting, supporting or defending a **proscribed organisation**, or any other **political**, **religious**, **racial** or single-issue **ideological** group or movement or cause, which **advocates**, **threatens**, **requires** or **enacts** anything mentioned above, in **iii) (1)-(3)**.

3) **NOTES:**

a) "Mass Murderers" vs. "Serial Killers":

i) These terms are not defined separately within UK criminal legislation. For our purposes here, a "mass murderer" can be considered distinct from a "serial killer":

(1) **Mass Murderer:** this refers to someone responsible for the murder of a number of people, simultaneously or consecutively, within a single, ongoing "event", or over a relatively short period of time, often (but not uniquely)

where the victims are also in relatively close geographic proximity. In our working definition, a mass murderer is *less* likely to be secretive during the killings, and, ultimately, will be less concerned about being seen by the public or identified by authorities.

(a) Mass murders can be indiscriminate (i.e.: a "massacre", where the specific targets do not seem to matter), or quite selective (i.e.: the killer has carefully chosen a very specific group to kill). Examples include (but are not limited to) "rampaging-shooter" & "rampaging-knifer" attacks, public bombings, and public CBRN attacks.

(b) For the purposes of PREVENT relevance, we consider **all** mass murderers as "extremist", irrespective of any other factors, although care must be taken around PREVENT assessments of mass murders enacted solely for financial or economic gain, with no **political**, **religious**, **racial** or **ideological**[29] element.

(2) Serial Killer: this refers to someone who has murdered a number of people in separate events, over a more extended period of time and (possibly) distance. In our working definition, a serial-killer is probably *more* likely to be secretive during the killings, and will likely expend more effort to not be seen by the public or identified by authorities.

(a) We consider serial killers to be "extremist" and "PREVENT relevant" **only** if their killings are intended to advance a **political**, **religious**, **racial** or **ideological** cause, particularly if they use firearms or explosives in their attacks. In these cases, a serial killer would likely fall within the definition of terrorists provided in TACT 2000.

a) Political Assassins & Hostile State Actors:

i) For example, the operatives alleged to have been responsible for the assassination of **Sergei Viktorovich Skripal**.

b) "Murder, Wounding or GBH, etc…":

i) The serious criminal offences mentioned in **iii) (3)** of the extremism guidance above do not necessarily have to be called for **by name**. It is enough that the legal 'points to prove' for the offences themselves would likely be made out within UK legislation if the activities being called for were enacted.

c) "Out-Groups":

i) See the separate entry in this glossary section for a more detailed exploration of this term.

ii) Identification of an "out-group" can be summarised as the tendency to:

(1) Perceive a group as both **existing** & **different** from a group that we associate ourselves with (the "in-group"), and;

(2) To view members of this out-group as being more similar, more homogeneous, than members of our own in-group, but in a **negative** and/or **destructive** sense.

iii) Consider Subjects who identify any lawful group as deserving unlawful, hateful, abusive or violent treatment, particularly if Subjects characterise the target group by a protected characteristic (as per the 2010 Equality Act & similar), such as age, disability, sex, gender identity, marriage & civil partnership, pregnancy & maternity, race, religion or belief, and sexual orientation.

iv) Also pay attention to Individuals targeting groups due to their perceived social class ("class war") or due to the nature of their lawful employment (animal-testing or abortion-clinic workers, civil-servants, politicians, Police, military, etc.).

Fixation & Fixated Behaviours

1) "Fixation", as used throughout this guidance document, refers to what a Subject is **thinking obsessively** about – so it is behaviour that indicates an obsessive or almost "fanatical" preoccupation with something. For advice around whether an Individual is exhibiting PREVENT-relevant fixated behaviour, seek advice from the Vulnerability Support Hub.

[29] Perhaps InCel violence for instance, or environmentalist or "eco-terrorism", should such a circumstance arise.

a) In its most general (and benign) terms, fixation is common within human activity. Consider people who seem utterly obsessed with their hobby and rarely care to speak about anything else.

b) The sort of fixation relevant to PREVENT is where the obsession is for extremists or something extremism related, as per the definition of extremism given in this document.

c) Particular consideration should be given to Subjects where the fixation becomes so obsessive that it begins to have a negative impact on the Subjects' lives: so perhaps their careers, education, family or other relationships.

d) This obsessiveness is likely to manifest in out-of-place circumstances, such as preaching an ideology at inappropriate moments without caring who it offends or hurts.

e) A fixated Subject will likely seek out (or produce) concerning material (or activities), online and/or offline.

f) Fixation will most likely be exposed by "leakage" to those around the Subject or through interaction with other Individuals of concern, friends or family members and/or online community members[30].

g) CTCOs should generally regard PREVENT-relevant fixation as a potential "red flag" in terms of radicalised behaviour.

Force

1) "Force", as used throughout this guidance document, refers to:

a) the **threat** or **use** of physical violence,

b) or any other form of deliberate **intimidation**, **coercion** or **compulsion**,

c) against or upon anyone, or against or upon anything that someone holds dear or perceives as vital to their wellbeing.

Grievance Narratives

1) "Grievance Narratives", as used throughout this guidance document, refer to causes for complaint or senses of resentment that Subjects may feel over things they deem unfair or threatening.

a) Relevant grievance narratives can take many forms and manifest in myriad combinations, although they frequently involve feelings of **injustice**, **humiliation**, **powerlessness** and/or **victimisation,** and often **acute moral outrage.** Ostensibly at least, almost **any** vulnerability could grow into a personal grievance narrative, or serve to exacerbate an already existing grievance narrative for an "at-risk" person, if left unaddressed. Grievance narratives can become triggers for radicalisation, or even direct TACT offending, if left to escalate, particularly if Subjects believe their grievances are urgent or have no credible non-violent solutions.

b) Relevant grievance narratives can be:

i) Real or imagined,

ii) Moral or immoral,

iii) Practical or impractical,

iv) Justifiable or unjustifiable,

v) Personal or relating to groups,

vi) Calm and rational or hyperbolic and irrational,

vii) Political, racial, religious, sex or gender based, class based, or with another specific single-issue ideology.

c) CTCOs should not disregard a grievance narrative because it seems either entirely "reasonable" or "too crazy". When it comes to vulnerability towards radicalisation, the personal context and behaviours of the Subject around the grievance are at least as important as the grievance narrative itself can be. An understandable and justifiable grievance over a genuine injustice

[30] Consider all open-source research returns & any input from family, friends or close-associates of the Subject.

does not preclude the potential for the Individual feeling that grievance to make incomprehensible decisions towards truly unjust, immoral and illegal behaviour. CTCOs must bear in mind that there is often a difference between:

i) The justifiability of **end goals** (e.g. "protect innocent and vulnerable animals from cruelty"), and;

ii) The justifiability of the **means** used to address those causes (e.g. "planning to fire-bomb a busy laboratory that tests on animals").

iii) **The ends do not automatically justify the means**.

d) Grievance narratives can include, but are not limited to:

i) **Personal Grievances:**

(1) Relationship or financial problems.

(2) Acute dissatisfaction with authorities.

(3) Occupational or educational setbacks.

(4) Being a victim of bullying, hate or discrimination.

(5) Family or friends directly affected by armed conflicts.

ii) **Hyperbolic & Group Grievances:**

(1) Delusions or conspiracy theories[31].

(2) Mystical, apocalyptic or religious imperatives.[32]

(3) General victimisation or persecution narratives involving any territory / nation / race / class / culture /ideology, etc..[33]

(4) The vicarious personalisation of any suffering or political unrest caused by current or historical events, policies or conflicts that otherwise have no direct affect upon Subjects or their friends or families.

iii) **Threat Grievances:**

(1) These are of particular concern as potential trigger factors for mobilisation or imminent action.

(2) They can include perceptions that Subjects or their loved-ones face **imminent** or **direct** threats to life or safety of any kind, perhaps which only drastic or violent action can resolve properly.

Freedom of Information (FOI), Subject Access & Media Requests

1) Information Requests: General

a) When considering information requests, it is important that local organisational information governance leads, and legal teams are consulted and are satisfied that compliance with legal requirements and organisational policy are adhered to.

2) Freedom of Information Act Requests

a) All recorded information held by a public authority is covered by the right to information under the Freedom of Information Act 2000 (FOI Act). Within the FOI Act, there is a presumption in favour of disclosure to enhance greater openness in the public sector and thus enable members of the public to better understand the decisions of public authorities and ensure that services provided by the public sector are seen to be efficiently and properly delivered. We want, as far as possible, to be open and transparent about the Channel process.

b) The CTSA recommends that it is good practice to consider the implications of the release of the information on third parties when complying with FOI legislation. In the context of Channel, third parties may include local and national delivery partners.

---

[31] For example: "White genocide"; "The Great Replacement"; "Muslim rape gangs"; "Crusades Against Muslims"; personal beliefs being suppressed or attacked by a corrupt / controlled / biased media; Plots by a "Liberal Elite"; The 'New World Order' / international Zionist / Jewish plots.

[32] For example: holy wars; crusades; jihad; "Heavenly rewards"; racial or political manifest-destiny; cultic belief or practice, etc.

[33] For example: justifying extremism by referencing other political or criminal injustices around the world; "ethno-cultural identity politics"; "we're surrounded by kafir / criminal immigrants"; "we can't get any job or housing because of XYZ group"; "the government / Police / this country hates Muslims"; "illegal immigrants are claiming all our benefit money", "government committing genocide just for oil", "fight the Islamification of Europe"; "Muslims must fight against Crusaders", "this used to be a white-Christian country", etc..

The Code of Practice of the FOI Act facilitates consideration by public authorities of the interests of third parties and stakeholders who may be affected by any decision to disclose information by setting standards for consultation. All public authority partners involved in Channel may receive FOI requests. If an FOI request is made all information will need to be assessed against FOI legislation to see if it is disclosable or not. All requests for the release of information held must be assessed on a case- by-case basis.

c) To achieve a consistent approach in responding to FOI requests relevant to Channel panels and assessments of individuals, and to protect third parties, all local partners who receive such an FOI request should bring it to the attention of their local panel. The chair should notify the Channel Case Officer and the Office for Security and Counter Terrorism in the Home Office, who will advise if any further consultation is necessary, for instance with other central government departments.

3) Subject Access Requests

a) Under Section 45 of the Data Protection Act 2018, individuals can also make a Subject Access Request (SAR) to see data held about them, or children they have parental responsibility for. The individual can request information on any records held about them. As with FOI, any organisation holding personal data can be subject to these requests. The right to make a SAR is described in the GDPR Article 15 , Rights of access by the data subject. Exemptions to these rights are found in the DPA 2018 Schedule 2 Part 4.

b) There are a limited number of exemptions, and not all personal information needs to be released in all circumstances. Exemptions to these rights are listed and described in the DPA 2018 Schedule 2 Part 4. As with FOI Act requests, to achieve consistency in responses, any requests for Subject Access Requests should be brought to the attention of the Channel panel chair.

4) Media Enquiries

a) Please note that national, international and specialist media queries about Channel are managed by the Home Office Press Office and should be referred to directly on the following number:

5) Home Office Press Office

a) 020 7035 3535

b) It is also helpful if you can make the Home Office Press Office aware, at an early stage, of any local media interest you receive.

Hate

1) "Hate", as used throughout this guidance document, refers to the demonstration of motivation of unlawful hostility (see separate entry below), malice, contempt, loathing or unlawful force directed towards anyone due to any lawful and ostensibly "static" or demographic factors including, but not necessarily limited to:

a) Age,

b) "Class",

c) Nationality,

d) Disabilities,

e) Race/ethnicity,

f) Citizenship-status,

g) Religious beliefs or lack thereof,

h) Sex, gender, sexual orientation, gender-identity.

2) **Hate Offences** here include any antisocial behaviour or criminal offences motivated to some degree by these factors, as per the relevant legislation, including, but not necessarily limited to the:

a) Public Order Act 1986,

b) Crime & Disorder Act 1998,

c) Football Offences Act 1991,

d) Racial and Religious Hatred Act 2006,

e) Offences Against the Person Act 1861,

f) Criminal Justice & Immigration Act 2008.

3) **Hate Speech** or preaching refer in this guidance to the use of words & utterances that:

a) Cause deliberate harassment, alarm or distress to anyone, & that are also,

i) Threatening, or;

ii) Intended to promote unlawful discrimination, or;

iii) Intended to incite the unlawful use of force, and;

iv) That are perceived by someone as being motivated by any of the aforementioned hate factors.

b) These "words and utterances" also include:

i) relevant material that is displayed in written form,

ii) or the publishing or distribution of it in written form,

iii) or its public performance as a play,

iv) or the distribution of such material through other means, such as:

(1) showing it directly,

(2) or playing a recording of it,

(3) or broadcasting it,

(4) or including it within a programme.

"Have Due Regard…"

1) According to the PREVENT Duty Guidance, "having due regard" means that the authorities should place an appropriate amount of weight on the need to prevent people being drawn into terrorism when they consider all the other factors relevant to how they carry out their usual functions.

Hostility

1) Hostility is not defined in UK legislation, although the word is used in much of the legislation around hate offences. Consideration should be given to ordinary dictionary definitions, which include ill-will, ill-feeling, spite, prejudice, unfriendliness, antagonism, resentment, and dislike. The following sub-heading give examples of the uses of "hostility" in UK legislation.

2) **Demonstrating hostility**

a) Legislation requires an indication by the offender of hostility towards the victim based on race or religion. The demonstration of hostility must be nearly contemporaneous to the conduct element of the offence (at the time of the offence or immediately before or after). The demonstration of hostility is likely, in many cases, to be something different from and additional to the conduct element of the offence. Mere evidence of the commission of the substantive offence against a victim is not sufficient.

3) **Motivated by hostility**

a) Motive can be established by evidence relating to what the defendant may have said or done on other occasions or prior to the current incident. In some cases, background evidence could well be important if relevant to establish motive, for example, evidence of membership of, or association with, a racist group, or evidence of expressed racist views in the past might, depending on the facts, be admissible in evidence. With reference to interpretation, it should be noted that section 28(1)(b) of the Crime and Disorder Act 1998, which refers to racial hostility, has been held to be wide enough to include

hostility towards one member of such a group, since section 6(c) of the Interpretation Act 1978 provides that "words in the plural include the singular" unless the contrary intention appears, and no such contrary intention appears in the provision.

b) In addition, the circumstances include those where an offence is motivated by hostility towards a third party, based on the relevant characteristic, who is not present: see *Taylor v DPP* [2006] EWHC 1202 (Admin). Accordingly, an offence committed against one person (or many persons) but motivated by hostility towards another person or persons on the basis of their perceived disability would seem to satisfy the statutory test.

4) Examples in Case law:

a) Evidence of words (spoken or written) or actions that show hostility towards the victim will be required. "Demonstrations" of hostility often involve swear words, for example: "black bastard" (*R v Woods* [2002] EWHC 85) or "African bitch" (*R v White* [2001] EWCA Crim 216). In *RG & LT v DPP* [2004] EWHC 183 May LJ said "It may be possible to demonstrate racial hostility by, for instance, holding up a banner with racially offensive language on it".

b) In *R v Rogers* (2007) 2 W.L.R. 280, the defendant was involved in an altercation with three Spanish women during the course of which he called them "bloody foreigners" and told them to "go back to your own country". The House of Lords, in upholding the defendant's conviction, held that the definition of a racial group clearly went beyond groups defined by their colour, race, or ethnic origin. It encompassed both nationality (including citizenship) and national origins. The statute intended a broad non-technical approach. Furthermore the victim might be presumed by the offender to be a member of a particular group, even if that was not correct. The House of Lords added that the fact that the offender's hostility was based on other factors in addition to racist hostility or xenophobia was irrelevant. The court also observed that the necessary hostility could be demonstrated by the wearing of swastikas or the singing of certain songs.

c) The demonstration of hostility need not be based on any malevolence towards the group in question. Disposition at the time is irrelevant: see *DPP v Green* [2004] EWHC 1225 (Admin.) and *R v Woods*, in which it was irrelevant that the offender, who used racially abusive language to a doorman after being refused admission, might well have abused anyone standing in the victim's place by reference to any obvious physical characteristic.

d) The motivation based on hostility need not be the sole or main motivation for the offence; it may also be motivated by other reasons. In *DPP v McFarlane* [2002] EWHC 485 (Admin), the defendant shouted threatening and racist abuse at the victim after finding the victim parked in a disabled bay in which the defendant was entitled to park. It was immaterial that the defendant may have had an additional reason for uttering the racial words in question.

e) The victim's reaction to the hostility is not relevant. See *R v Woods*, in which the victim was called a "black bastard" but said in evidence that he was "not bothered" by such comments. The Administrative Court found that the use of racist abuse during the commission of the basic offence made out the test for racial aggravation.

5) Demonstrated: multiple offenders

a) Prosecutors will need to analyse carefully the facts of a particular case to determine whether a particular offender can be said to have participated in a demonstration of hostility. This is particularly relevant in prosecutions arising from the policing of protests.

b) In *R v Davies and Ely* [2004] 2 Cr App R (S) 148 (29), a joint allegation of wounding with intent, the fact that one offender uttered words of racial abuse during the attack did not make all guilty of the aggravated offence, on the facts of the case, and the defendants should not be so sentenced when the evidence did not identify the one who uttered the words.

c) However, in *RG and LT v DPP* May LJ said that, "an offender may demonstrate racial hostility by joining in the activities of a group of people where a sufficient number of members of the group are themselves demonstrating racial hostility, and where the defendant's adherence to the group is such as to go beyond mere presence within the group, but so as to associate himself or herself with the demonstration of racial hostility which the group as a whole is displaying".

Ideology (relevant to PREVENT)

1) See also Ideologies under the **PREVENT Subjects** section.

2) **Ideology:**

   a) As used throughout this guidance document, "ideology" refers to any system of beliefs, ideas, ideals or causes that form the basis of:

      i) A political system or social philosophy,

      ii) A moral, spiritual or religious framework,

      iii) Any other communal, cultural or "racial" belief-system or movement.

2) **Extremist Ideologies:**

   a) Frequently, the adoption of an extremist ideology or cause tends to represent a Subject's **answer** to whatever problems they may already have, rather than the **cause** of their problems. So in order to rehabilitate Subjects, PREVENT needs to understand the personal, contextual, conscious and unconscious reasons why a person has adopted an extremist ideology.

   b) **Proscribed Groups:**

      i) The extremist ideologies that are most obviously and immediately concerning are those that belong to **proscribed organisations**, e.g.: ALM, ISIL, PKK, Irish National Liberation Army, National Action, Al-Qaeda, Tamil Tigers, Orange Volunteers, etc.. These are of concern precisely because they belong to (and have the "branding" of) illegal terrorist groups, irrespectively of whether some of their underlying aims or grievances may seem rational or relatable.

   c) **Hateful, Violent & Toxic Ideologies:**

      i) These ideologies do not necessarily belong to proscribed organisations. They are ideologies that are extremist in and of themselves, such as the unremittingly hateful, violent and criminal beliefs of the Order of Nine Angles. These sorts of ideologies tend to present exaggerated and almost always hateful narratives concerning identity, race, politics, history, sociology, class or religion, often woven together with elaborate conspiracy theories or narratives of apocalyptic nihilism or social despair, often calling for a "race war" or a social "purging" of some kind.

   d) **Extremist Expressions of Ideology:**

      i) PREVENT is also concerned with extremist **expressions** of otherwise "normal" ideologies. Extremism is often as much what people **do** as it is what they **believe**.

      i) Any political, religious, racial or other single-issue ideology or cause can be "weaponised" by extremists. A justifiable (legal, "moral", "considered") cause, like safeguarding animals or the environment, can still be fought for in a way that is entirely unjustifiable (illegal, "immoral", "ill-considered").

      ii) In very simple terms, CTP PREVENT recognises that lawful or peaceful **ends** do not automatically justify criminal or violent **means**. PREVENT-relevant expressions of ideology tend to be those where an **in-group**'s success or survival is perceived by that in-group as being inseparable from (or even dependent upon) acutely **harmful**, or even **criminal**, acts against a perceived **out-group**.

      iii) These ideological expressions are likely to encourage hate, unlawful violence or even terrorism offences by their adherents. Adherents may characterise this as being for "defensive" or "pre-emptive" reasons against an existential threat, but whatever the Case, the inseparability between the ideology & the need for unlawful aggression against the "out-group" is key. This aggression tends to be the "tell-tale" indicator: as long as you are part of the "out-group", you are a legitimate target for unlawful abuse and/or aggression, irrespective of any other factors.

   h) **Fanaticism is a contextual behaviour & mind-set, not just a symptom of specific ideologies:**

      i) Fanatics and extremists can emerge from practically any social, religious or political movement, irrespective of how benign these ideologies may be in themselves. It depends on the personal circumstances of the Individuals concerned

and their wider social context. Generally speaking, we can judge this by what Individuals **say** and what they **do** in order to **achieve** their stated goals, regardless of whether those goals seem justifiable or not, i.e.:

ii) All mainstream Christian denominations agree that Christianity requires "loving one's neighbour", "turning the other cheek", and "forgiving those who hate you". Even so, this has not prevented the existence of murderous Christian extremists. There have been (in Canada, the USA and Australasia) bombings of abortion clinics and attempted murders of clinic staff by people claiming that they are acting as "good Christians" on behalf of unborn children. Something similar applies to religious terrorists who define themselves as Muslim, Hindu or Buddhist, etc..

i) Subconscious Bias:

i) Be aware of otherwise **lawful** ideologies that may seem like they might be dangerous (due to personal subconscious bias or cultural "baggage" associated with the ideology) but which are expressed and practiced in benign fashions. Other than the obvious of not misjudging all Muslims because of the existence of Al-Qaeda and ISIS, a good example might be self-declared "Satanists".

ii) A common perception around Satanism tends to be that it is fundamentally unwholesome, abusive and dangerous **in and of itself**. This can certainly be true, as we have seen with the **Order of Nine Angles** neo-Nazi Satanist group/proto-militia, which actively promotes religious imperatives around Satan-worship, extreme cruelty, paedophilia, violent rape, "race war" and societal collapse. However, a "Satanist" could also be a member of the Church of Satan, a largely secular, atheistic "new religion" that does not espouse any forms of violence or abuse, and which is not necessarily or automatically unlawful, abusive or extremist.

iii) This emphasises how PREVENT assessors must be thorough and careful in their investigations into the tenants of beliefs and to not allow their own cultural baggage to influence their assessments unduly. One religion or ideology being inherently "distasteful" to members of another religion or ideology does not automatically make it criminal, dangerous, PREVENT-relevant or extremist.

iv) If a group calls for serious criminal activity as a fundamental part of membership, or if it is extremist as per the operational guidance for extremism contained within the document, then it is potentially relevant for PREVENT. Do not assume just based on the name or title of the group.

3) "Policing Ideology":

a) CTCOs must focus upon mitigating the promotion of ideologies that are extremist in themselves (as per the operational guidance on extremism presented within this document), or extremist behaviours around otherwise benign, legitimate, non-extremist, ideologies.

b) Police must focus upon prevention of criminal behaviours, and also other high-risk behaviours that suggest safeguarding needs, as per the usual Police responsibilities in this area.

6) Conflicted / Mixed Ideologies:

a) Ideology in TACT –

i) TACT does not define or limit what is meant by "**political, religious, racial or ideological cause**", nor does it restrict "**ideological cause**" to being only political, religious or racial, or to being solely those ideologies held or promoted by proscribed organisations.

ii) TACT also does not stipulate that a terrorist has to have a long-standing or deep-seated belief in the ideology or cause that he or she is ostensibly supporting by committing a TACT offence.

iii) Some Individuals seek to support or enact TACT offences without a clear understanding of the ideology or cause they are ostensibly supporting. Therefore Individuals whose ideological motivations are unclear, mixed or unstable, but who still demonstrate a connection to, or personal interest in, extremism, terrorism or mass murder, should be given the same consideration for support as those whose concerning ideological motivations are more consistent and obvious.

b) Switching Ideologies –

i) Those who are drawn to extremist ideologies sometimes switch from one extremist ideology to another – supporting Islamist extremism one month & extreme-right neo-Nazism the next.

ii) This may be because in some Subjects it is not a specific extremist ideology that has caused their problematic behaviours, but rather they are experiencing other issues that have prompted them to seek out various extremist ideologies or processes to "try them on for size", so they can express the social pressures or MH issues that they are **already** feeling.

iii) For instance, we have seen many similar and often overlapping PREVENT Case examples with Individuals who:

(1) demonstrate an interest in multiple extremist ideologies in parallel, such as Salafist militant jihadism and "white supremacy";

(2) Switch from one ideology to another over time;

(3) Target a 'perceived other' of some kind (perhaps based upon gender or another protected characteristic), but do not otherwise identify with one specific terrorist ideology or cause;

(4) Are obsessed with massacre, or extreme or mass violence, without specifically targeting a particular group (e.g.: "high school shootings");

(5) May be vulnerable to being drawn into any terrorism activity out of a sense of duty, or a desire for belonging, rather than out of any strongly held beliefs.

7) Unclear Ideologies:

a) It is possible for a Subject to fixate upon an extremist ideology without committing terrorism offences. Similarly, not all terrorists have been ideological "true believers". Some have been coerced into action, others have been nihilistic & self-destructive mass-shooters, or else seeking various forms of non-ideological excitement or self-gratification, or suffering from mental health problems, etc..

b) Some terrorists have used ideology to explain & justify their actions **after the fact**.

c) Nihilistic, suicidal or self-destructive Subjects may want to express their resentments by killing multiple people, and also seek "death by Police" for themselves in a mass shootout (or equivalent). They may simply cite an extremist ideology / cause almost as an afterthought to excuse, explain or give momentum to their own personal desire to die or kill for whatever other reason.

d) In such cases, ideology may not flag up so clearly as an issue for the Subjects involved prior to an attack – hence the reason that although identifying a Subject's involvement with potentially "toxic", PREVENT-relevant ideologies is important, CTCOs must give equally careful consideration to the "mobilising" behaviours of Subjects around any ideologies or movements associated with the Subject. The explicitly ideological element of the destructive behaviour may not manifest in a way that is detectable until it is too late.

Immigration Enforcement

1) Determining a person's immigration status and the process of navigating the immigration system can prove complex and challenging. Specialist advice and support regarding immigration is available to Channel panels for addressing queries, sourcing information and advice, and where appropriate, seeking immigration representation on Channel panels. The service can be accessed via: CTCoordinator@homeoffice.gov.uk.

Individuals & Institutions (of Concern to PREVENT)

1) See also **PREVENT Subjects.**

2) Individuals & Institutions, as used throughout this guidance document, refer to people, groups & organisations that have some sort of observable PREVENT-relevant context and who are of interest to either PREVENT, or potentially PURSUE. This term does not refer **only** to people who are Subject to CT investigations by the Police or Security Service.

3) They can include:
   - **a)** Known TACT offenders, SOIs, RSOIs, PCM Subjects.
   - **b)** Proscribed organisations (and derivatives).
   - **c)** Extremists (domestic or foreign).
   - **d)** Hate speakers / preachers.
   - **e)** Religious, political, educational, social or sporting establishments already identified by the CT network as being of concern.

4) In terms of who poses the greatest risk-potential of grooming, coercing or radicalising a Subject, attention should always be paid to the **type** & **extent** of the Subject's exposure to the people, groups or institutions in question, including Subjects' family members or close friends who are, or have been, any of the aforementioned.

5) **INDIVIDUALS:**
   - **a)** PREVENT deals with **People** – Individuals.
   - **b)** Whatever the Case at hand, we must **always** first look for the Individuals behind the issues referred to PREVENT.
     - **i)** If you are faced with a referral about an Institution, try to find who the concerning people are currently associated with that Institution. The Institution does not exist without people to support and populate it.
     - **ii)** If you are faced with an Ideology report, first try to find the Individuals who are formulating and/or propagating the concerning expression of ideology that has been referred to PREVENT (such as extremist leafleting or "stickering" in an area).

6) **INSTITUTIONS:**
   - **a)** PREVENT referrals around Institutions are automatically referred into the PLP space, if the PGA Decision is that there is a reasonable suspicion that there is a genuine PREVENT concern around that Institution.
   - **b)** An Institution is a kind of organisation founded for a **religious**, **educational**, **professional**, **political,** or other **social** purpose (such as a sporting or youth club, perhaps).
   - **c)** They can be formally registered charities or private businesses. They can be "pop-up" establishments or stands. They can be focused around a particular premises. They can supra-territorial (spread across multiple locations or moveable between locations), and they can be online "virtual" institutions.
   - **d)** An Institution should only really be considered for PREVENT management where:
     - **i)** There is a PREVENT-relevant concern around it, even if the Individuals comprising it join and leave with great rapidity, or,
     - **ii)** The Individuals making up the PREVENT-relevant Institution cannot be identified.
   - **e)** Consider any premises or organisations linked to:
     - **i)** Extremism or any terrorism related activity, or,
     - **ii)** That have hosted, accommodated or attracted terrorism offenders, SOIs, current PREVENT Subjects, proscribed organisations, extremists (domestic or foreign), or hate speakers / preachers.
   - **f)** Consider whether they have **produced**, **promoted**, **permitted** or **disseminated**:
     - **i)** Hate speeches, extremist material or graphic & serious violent material of any kind, or,
     - **ii)** Propaganda material produced by or for proscribed organisations, **without reasonable excuse** (such as for legitimate academic study within any lawful UK educational establishment).

Intent (to Commit Offences)

1) "Intent", as used throughout this guidance document, refers to an apparent inclination, desire, plan, aim, or deliberate purpose towards the commission of any unlawful extremist conduct or, ultimately, terrorism offences. Intent indicators and factors describe a mind-set associated with a present or growing desire or readiness to commit terrorism offences, or the mobilisation process towards that desire. Not everyone with extremist engagement factors goes on to develop an intent to commit offences.

Intervention Providers

1) Intervention Providers (IPs) are ideological and theological specialists. They are experienced in assessing ideological drivers, possess a high level of understanding around extremist narratives, and the ability to counter this. They receive comprehensive training in support of their roles through the IP Professionalisation Programme, are subject to a rigorous recruitment process, with all receiving Ministerial approval to work on the programme.
2) Where the individual has a need for theological/ideological support, to address extremist views, or possesses an unclear, mixed or unstable ideology, Home Office approved IPs must be commissioned. The IP aims to increase theological understanding and challenge extremist ideas or fixated thinking where they are used to legitimise terrorism, or to otherwise understand the extent of concerns relating to ideology. Use of a Home Office IP must always be a consideration for live cases and kept under review where not commissioned. A record must be kept detailing the Panel's decision and its basis. Where the Channel Panel identifies that the individual would benefit from an IP, the CTCO will be responsible for arranging the provision of that service.
3) Where a Home Office IP has been commissioned, written reports on progress will be prepared and returned to the CTCO within five working days of the intervention session being completed. The CTCO will use this report to provide a verbal update to the Channel Panel and update the VAF when needed. The Channel Panel chair and standing Panel members may see the IP report on request via the CTCO. The IP Reports are produced for the specific purpose of informing Channel Panels of the risks of radicalisation and the vulnerabilities present, therefore should not be shared beyond standing Panel members. Further details on disclosure are referenced in paragraphs 62-66. In England and Wales, IPs must first have been approved by the Home Office. With all other services provided as part of the support package, the chair and Police must be satisfied that these providers are suitable to deliver these interventions. Individuals and organisations holding extremist views or supporting terrorist-related activity of any kind, in this country or overseas, have no place in delivering support through Channel nor will they be given public funding to do so. This applies irrespective of the source of the funding: central government, local government, policing or other publicly funded bodies. Where support is through Home Office approved IPs, the CTCO is responsible for liaison with the support provider and for funding and monitoring the delivery of that element of the support package.

Interventions

1) 'Interventions' are specific planned engagements between an Individual and an Intervention Provider or Police, intended to divert, deter or desist he PREVENT-issues of people who are vulnerable to being drawn towards terrorism-related activity. Interventions can include mentoring, counselling, theological support, encouraging civic engagement, developing support networks (family and peer structures) or providing mainstream services (education, employment, health, finance or housing), or other more overtly disruptive activities.
2) **Types of intervention:** the CTP Disruption Manual is the first port of call for advice around interventions and their targets. The following is simply a very general overview of the types of interventions CTCOs and IPs may have to :
    a) **Primary**: Work with individuals vulnerable to being drawn, groomed, coerced or self-radicalised towards any terrorism related offences, with activities such as one-to one mentoring, psycho-social care and group interventions. Generally speaking, such interventions require the individual's consensual engagement, with a few exceptions (perhaps such as being sectioned under mental health legislation).

b) **Secondary:** Work with people around the individual who is being groomed, coerced or self-radicalised into extremism or towards terrorism related activity, so their immediate families, schools, perhaps place of work or close friends (where appropriate), providing activities such as family counselling, welfare, general support or access to other resources.

c) **Tertiary:** Activities with an individual's wider spheres of influence such as institutions and the wider community, which often seek to engage, protect or divert individuals who may be exposed to heightened risk factors. Depending on the circumstances and lawful goals, these kinds of interventions might not have to reference the individual in person (with respect to privacy laws), or they may be disruptive in nature.

d) **Rehabilitation:** Working with high-risk groups (e.g. offenders while in prison, on remand, probation, returnees and foreign fighters) to disengage, and where possible, de-radicalise them away from extremism.

Investigations within Channel

1) Circumstances may arise where an individual who is in receipt of Channel support is the subject of an investigation by Police for a non-terrorism related offence. In this instance, the individual is not precluded from accessing Channel support. Channel can continue to provide support, with any information shared between Channel partners used to assess individual vulnerabilities, risk and support needs; however, where information is exchanged which suggests criminal activity, the Police are duty bound to investigate.

Leakage

1) "Leakage", as used throughout this guidance document, refers to situations where, intentionally or otherwise, a Subject expresses views or plans that are of justifiable concern in terms of PREVENT or even PURSUE. During their radicalisation or mobilisation process, potential terrorists often interact with (i.e.: "leak to") co-ideologues or communities they are involved with, perhaps to seek legitimisation or approval for their intended actions, or perhaps sometimes in a subconscious effort to be talked out of them. Speaking very generally, "leakage" tends **not** to include **directly communicated threats** to a potential target, at least in the more recent forms of terrorism in the UK.

   a) At the height of the "Troubles", the IRA frequently sent code-words to the authorities, sometimes along with a general location, immediately prior to an attack. The reasons for these warnings are complex, but could perhaps be seen to involve issues surrounding the self-perception within the IRA that it was a "freedom fighting army", with a geographically settled constituency of ordinary civilians that they ostensibly had to keep "on-side" in terms of their moral legitimacy.

2) All of that said, it is unusual for potential lone-actor terrorists to warn their intended victims. Hence directly communicated threats are generally more likely to be malicious communications or simple "trolling".

   a) Obviously, no direct death-threats should ignored by Police without *some* level of investigation. Direct threats from unknown sources, or from a known extremist group or proscribed organisations, or from people with a history of relevant offences, or in some Cases from people with acute mental ill health, should always be taken seriously and investigated appropriately.

3) Indirect threats & "leakage" from Subjects to third parties about an intent to inflict harm should **always** be regarded as concerning, as these are generally more likely to be a genuine signal of imminent action. Whatever the content or forum of such "leakage", it is generally a Subject's family, friends, online & offline community members, & possibly work associates, who are most likely to witness it rather than the authorities. Identifying baseline beliefs & behaviour is vital to assessing the difference between "leakage" as a warning signal for imminent violence of TAT offending, & "leakage" simply of extremist rhetoric.

4) **Relevant "leakage" can include:**

   a) Communicating grievance narratives or vulnerabilities as reasons or "triggers" for action.

   b) Expressions of a Subject's intentions, capabilities, opportunities or mobilisation behaviours.

c) Coded discussions where the content of the conversation might be largely unknown, but where the other people in the conversation are indivdiuals or institutions of concern.

d) Divulging details of, or seeking support for, unlawful extremist conduct or terrorism offences by the Subject, that:

i) **have** happened,

ii) or that are **currently underway**,

iii) or that are being planned, or considered or that are simply **going to** happen.

MAPPA – Multi-Agency Public Protection Arrangements

1) Multi-Agency Public Protection Arrangements (MAPPA) are reserved for those who present the highest risk of harm in their local community. Most people are managed within MAPPA because of the nature of their offending. In some cases, agencies may determine that an Individual's vulnerability is such that it is best managed through the MAPPA process.

2) Where this is the case, the multi-agency public protection Panel can, if necessary, seek the advice of a relevant CTCO. It should be noted that all offenders convicted of TACT offences will be managed via MAPPA. However, where an offender is managed through Ordinary Agency MAPPA meetings for other, **non-terrorism related**, offences, and yet is also deemed to be potentially vulnerable to being radicalised or otherwise drawn into any terrorism related activity, **a PREVENT referral should be made**. It will then be for the lead agency to liaise with the local Channel Panel (if they accept the case) to determine how these vulnerabilities and risks should best be managed.

3) **NB:** Ordinary Agency Management Level 1 is where the risks posed by the offender can be managed by the agency responsible for the supervision or case management of the offender. This does not mean that other agencies will not be involved, only that it is not considered necessary to refer the case to a level 2 or 3 MAPPA meeting.

Mobilisation Behaviours, Signals & Activities

1) "Mobilisation", as used throughout this guidance document, refers to the behaviours of Subjects who have reached a point where thoughts & words are shifting towards action or even combat-readiness. For our purposes this would include all TACT offences & any other terrorism connected offences.

2) Very generally, changes in an Individual's life circumstances, mental wellbeing, financial situations, & countless other factors, can all tip the balance of a Subject's risk-reward calculation about whether they **should**, **can**, or **will** commit higher-level terrorism offences. Mobilisation, then, can be regarded as a "triggered" behaviour, where a Subject escalates from their "normal" baseline behaviour to the active pursuit of offences. Mobilisation can also include "last-resort" or "finishing" behaviours where the Subject does things that give the appearance of a preparation to "go away" (e.g.: abroad or to prison) or to die; perhaps such as visiting extended family to say goodbye, paying off debts or suddenly running up huge debts, getting married or even shaving off all body hair (not uncommon for Islamist terrorists).

3) **NB:** CTCOs should bear in mind that nihilistic, suicidal or self-destructive Subjects may sometimes seek "death by Police" in a shootout (or equivalent), or may simply adopt an extremist ideology or cause to excuse, explain or give momentum to a pre-existing personal desire to die or kill for whatever other reason. Subjects such as these may not flag up as potential terrorism-risks if CTCOs are looking for ideology whilst ignoring wider signalling behaviours. The ideological element of the destructive behaviour may not manifest in a way that can be detected until it is too late to PREVENT their actions.

Mobilisation Identity

1) "Mobilisation Identity", as used throughout this guidance document, refers to when and how Subjects begin to identify themselves as possessing "warrior", "soldier", "crusader", "assassin", "killer" or even "martyr" characteristics. In other words, they are identifying themselves as pseudo commandoes of some sort.

2) So where fixation refers to what Subjects are **thinking about**, mobilisation behaviour refers to **what they wish to be** or **who they wish to emulate**. Mobilisation Identities are here divided into three loose subcategories of identification (although there is often crossover):
   a) **Identification with extremist action** – in order to signal their self-perceived "warrior" identity, Subjects escalating towards violent extremism & terrorism may present themselves as being a kind of warrior, soldier or "pseudo-commando", either by directly describing themselves in these terms or perhaps by photographing themselves posing with weapons (real & replica) or otherwise dressed as a warrior, soldier, guerrilla or pseudo-commando of some kind, sometimes long before they escalate to an attack. Anders Breivik is a case in point. He posted pictures of himself across his social media posing with military grade weapons and dressed in combat gear, but also (and no less significantly) wearing formal military-style "dress uniform" without weapons, signalling his self-perception as being a "soldier" of his cause.
   b) **Identification with an extremist role model** – Subjects may be influenced by, or identify themselves with, a specific extremist thinker or leader, or another terrorist or killer (either known to them personally or else "popularised" through the media), signalling their mobilisation towards action by seeking to emulate the style, ideals or actions of their role-model. This can also apply to young InCel people aligning themselves with the attitudes, behaviour and even physical appearance of previous "school-shooters".
   c) **Identification with an extremist group/movement** – even if acting alone, extremists and terrorists often see themselves as being connected to a larger group or movement, and they can demonstrate a strong sense of moral obligation towards this group or movement even if they've never had direct contact. This can be construed as identification with an ideological cause or movement. Moral commitment to the group, or values associated with the group's identity, appear to be strong indicators of the Subject's potential to escalate towards extremist violence.
3) They can do any of this directly and obviously, or less obviously by associating themselves closely with other such "warriors" (etc.). This behaviour can also be deliberate and conscious, or unintentional and subconscious. One way or another, CTCOs should regard these sorts of Mobilisation Identities behaviours as a potential "**red flag**" in terms of radicalised behaviour.

Opportunity (to Plan or Commit Offences)

1) "Opportunity", as used throughout this guidance document, refers to any time or set of circumstances within which a Subject can mobilise towards, or actually execute, TACT offences or any other terrorism-connected offences.
2) As a general rule, having the **intent** & **capability** to offend does not automatically grant the **opportunity** to do so. Whereas some terrorist attacks may seem very ad-hoc & low skill, the vast majority of attacks are rarely sudden, unplanned or completely impulsive. They tend to emerge from amongst other changes in observable behaviours. We work on the principle that those wishing to commit terrorist offences *tend* to make choices about actions & targets that offer, from their perspectives, the highest reward for the least necessary risk to success – although bear in mind that mental ill health may complicate this. MH problems aside, even if Subjects fully intend to die during their attack, they will generally still wish to be successful by some measure before they are stopped or killed.[34] Working on the principle that all prospective terrorists require an opportunity to be able to act on their intentions, it is important to identify & consider how a Subject's lifestyle, routine or interests affect, generate or signify such opportunities.

Othering People – "In-Group" vs. "Out-Group"

1) This process is a key concern to PREVENT.
2) **QUICK OVERVIEW:**

[34] **If** they are behaving rationally. It is worth bearing in mind that "rationality" is often relative to the life-context & psychological wellbeing of the Individual in question.

a) For our Purposes in PREVENT, consider Subjects who:

i) identify **any** group as deserving unlawful, hateful or physically abusive treatment,

ii) **Particularly** if that group is based upon a protected characteristic, such as age, disability, sex, gender reassignment, marriage & civil Partnership, pregnancy & maternity, race, religion or belief, or sexual orientation.

iii) Also pay attention to Subjects targeting groups due to their perceived **social class** ("class war") or nature of their **lawful employment** (animal-testing or abortion-clinic workers, civil-servants, politicians, Police, military, etc.).

3) UNPACKING THE CONCEPTS:

a) Research into torture, murder, terrorism, genocide and other mass-killings, tends to show relatively consistently that humans tend to "other" or "dehumanise" their victims to some degree, before they enact acute violence.

b) What that means is that all things being equal we are less likely to want to harm those who we feel are a welcome part of our group, our community, or our common identity, even if that common identity is something as basic as our shared humanity. Very generally speaking, to enact acute violence or physical abuse or cruelty against other humans, most people will at some level need to feel some or all of the following:

i) under direct, personal and/or existential threat by the target, or;

ii) that the target needs to be overcome in general in order to assure communal survival, or;

iii) that the target intrinsically deserves such treatment because the target is "disgusting" or "evil" in some profound way, or;

iv) that the target is fundamentally less human than us, perhaps because of perceptions around their behaviour or culture, their "race" or skin colour, or any other demographic traits[35], and is therefore not part of our community or group identity and are little more than a nuisance to be removed or vermin to be exterminated.

c) People who we **perceive** are hurting or threatening us, or who we believe are causing us to fear for our safety and the safety of those we care about, are consciously and subconsciously placed outside of our common sense of security and community. They stop being "like us" and become a threatening (or hated or disgusting) "other". Our sense of being threatened or being under attack, and our desire to protect ourselves, tends to trump our desire and ability to empathise with those we regard as being responsible for the violence or the perceived threat. So, in simplistic terms, an "in-group" could be considered a group of people who are perceived as sharing **some degree** of common empathy, common identity and communal safety with each other.

d) Identification of an "out-group" is the tendency to:

i) Perceive a group as both **existing** & **different** from the "in-group" that we associate ourselves with, and,

ii) To view members of this out-group as being more similar, more homogeneous or "the same", than members of our own in-group, but generally in a negative way.

e) **For Example**:

i) For whatever reasons, Bob perceives non-"white" immigrants as being "pretty much all the same" and "a big problem". So he has identified "non-white" immigrants as being, in his estimation, an **"out-group"**.

ii) He perceives "white", native English speaking, non-immigrants (his **"in-group"**) as being like him, and so "better", "safer", & not a problem when viewed as a whole.

iii) To Bob, "white", native English speaking, non-immigrants who are criminals are the exceptions to the rule. They are delinquents, "bad eggs", or perhaps even "tainted" by the out-group he dislikes, but their behaviour has nothing to do with their skin colour, culture, nationality-at-birth or first language.

iv) However, Bob perceives that "non-white", non-native English speaking immigrants who become criminals are probably like that precisely **because** they are "non-white", non-native English speaking immigrants.

[35] Particularly any protected traits like sex, sexuality, gender identity, age and so on.

f) Identifying out-groups is not necessarily a concerning behaviour in every context. Benign supporters of different sports teams do it all the time (i.e.: "my team & supporters are better than your team & supporters, BECAUSE they are my team and supporters"). This only becomes toxic if the "othering" of the "out-group" starts to involve hateful or threatening language (as per legislation), violence, or calls for these.

Pathways Towards Terrorism

1) For guidance around criminal pathways towards terrorism offending, refer to the Relevant Offences section of this document.

2) Those who are motivated by a misguided form of "idealism", believing their cause and actions to be "noble", may not have a criminal history (in terms of relevant offences), and their motivations may seem entirely personal and ideological. Subjects like these may come to believe they can solve their personal problems or meet personal needs by projecting them into an ideological cause or movement. Others may become involved for opportunistic reasons. They may see some opportunity for criminal or personal gain by adopting an extremist identity and contributing to a terrorist offence, but have no particular interest in the cause.

3) For those without a criminal background, a process of conditioning is necessary for them to overcome their inhibitions about committing terrorist offences, or at least the ones involving extremes of violence. This may be achieved through self-conditioning or grooming by others and can take many hours of exposure to rhetoric, propaganda and/or group pressure to shape beliefs and attitudes to the support and/or use of such tactics.

4) Those with criminal backgrounds, particularly involving persistent violence, this grooming / conditioning may not be necessary, as the Subject may already hold attitudes supportive of violence or the types of thinking that absolve them of responsibility or guilt.

Prevention

1) 'Prevention' in the context of this document means reducing or eliminating the risk of Individuals becoming involved in terrorism offending. PREVENT includes (but is not confined to) the identification of those at risk of being drawn into terrorism, and referral towards appropriate interventions. These interventions aim to disengage vulnerable people from radicalisation, or to divert, deter or desist any relationships, behaviours, contexts or other processes that are otherwise grooming, coercing or self-propelling someone towards **any** terrorism related activities.

PREVENT Subjects – Individuals, Institutions & Ideologies

1) See also the separate entries for **Ideologies** and **Individuals & Institutions** in this Glossary.

2) **INDIVIDUALS:**

a) First and foremost, PREVENT deals with **People** – Individuals. Whatever the Case at hand, we must **always** first look for the Individuals behind the issues referred to PREVENT.

i) If you are faced with a referral about an Institution, try to find who the concerning people are currently associated with that Institution. The Institution does not exist without people to support and populate it.

ii) If you are faced with an Ideology report, first try to find the Individuals who are formulating and/or propagating the concerning expression of ideology that has been referred to PREVENT (such as extremist leafleting or "stickering" in an area).

7) **INSITUTIONS**: PREVENT referrals around Institutions are automatically referred into the PLP space, if the PGA Decision is that there is a reasonable suspicion that there is a genuine PREVENT concern around that Institution.

a) An Institution is a kind of organisation founded for a **religious**, **educational**, **professional**, **political,** or other **social** purpose (such as a sporting or youth club, perhaps).

b) They can be formally registered charities or private businesses. They can be "pop-up" establishments or stands. They can be focused around a particular premises. They can supra-territorial (spread across multiple locations or moveable between locations), and they can be online "virtual" institutions.

c) An Institution should only really be considered for PREVENT management where:

i) There is a PREVENT-relevant concern around it, even if the Individuals comprising it join and leave with great rapidity, or,

ii) The Individuals making up the PREVENT-relevant Institution cannot be identified.

g) Consider any premises or organisations linked to:

i) Extremism or any terrorism related activity, or,

ii) That have hosted, accommodated or attracted terrorism offenders, SOIs, current PREVENT Subjects, proscribed organisations, extremists (domestic or foreign), or hate speakers / preachers.

h) Consider whether they have **produced**, **promoted**, **permitted** or **disseminated**:

i) Hate speeches, extremist material or graphic & serious violent material of any kind, or,

ii) Propaganda material produced by or for proscribed organisations, **without reasonable excuse** (such as for legitimate academic study within any lawful UK educational establishment).

7) **IDEOLOGIES:** Ideologies, in this context, can refer to well-known and clearly established ideologies themselves (Nazism / National Socialism, militant Salaafist Jihadism, etc.), but may also refer to other specific beliefs, causes, motivations and popular movements, depending upon their stated goals and the behaviour of their members.

a) PREVENT-relevant Ideologies are automatically referred into the PLP space, but this is only really an option where an **Individual** or an **Institution** propagating these ideologies cannot be identified or cannot managed through PREVENT – so perhaps extremist or terrorism-related stickers, signs, or other material appearing in an area, but which cannot be linked to an Individual or Institution in the first instance.

b) An Ideology can be **any** system of beliefs, ideas or ideals that form the basis of:

i) A moral framework,

ii) A religious or political system,

iii) Any other social or spiritual philosophy or belief-system.

c) The ideologies and/or causes of most obvious concern are those directly associated with **proscribed organisations**, e.g.: ISIL, National Action, Al-Qaeda, etc..

d) Other than the stated ideologies and goals of proscribed organisations, PREVENT is also concerned with **extremist expressions** of otherwise lawful ideologies.

i) Rather than attempting to designate whether every ideology is "acceptable" or "unacceptable" in themselves, PREVENT will seek to assess whether the specific expression of an otherwise legitimate ideology is relevant within the specific context we are presented with.

ii) In simple terms, CTP PREVENT recognises that "good" or lawful ends do not automatically justify "evil" or criminal means.

e) A justifiable (legal, considered, benign) cause, like pursuing a religion, or safeguarding animals or the environment, can still be fought for in a way that is entirely unjustifiable (illegal, ill-considered, malignant).

f) Ostensibly at least, any political, religious, racial or other single-issue ideology or cause can be "weaponised" by extremists - see the PREVENT CTP working definition of "extremism" for details.

g) PREVENT-relevant expressions of beliefs tend to be those where an **in-group**'s success or survival is perceived by that in-group as being inseparable from (or dependent upon) negative (and probably illegal) acts against a perceived **out-group**.

h) These ideological expressions are likely to encourage hate, unlawful violence or even terrorism offences by their adherents. These adherents may characterise this "ideological expression" as being for "defensive" or "pre-emptive" reasons.

i) Whatever the Case, the inseparability between the ideological expression & the **need** for criminality or unlawful aggression against an "out-group" is key. The overt aggression tends to be the "tell-tale" indicator: as long as you are part of the "out-group", you are a legitimate target for abuse and/or aggression, irrespective of any other factors.

j) In a nutshell then, there can be fanatics and extremists within practically every social, religious or political movement, irrespective of how benign these ideologies may be in themselves. Generally speaking, we can judge this by what Individuals **say** and what they **do** in order to **achieve** their stated goals, rather than because of what we believe we understand about the more "mainstream", benign expressions of their ideology.

k) Be aware of otherwise **lawful** ideologies that may seem like they might be dangerous due to "cultural baggage" associated with them, but which are expressed and practiced in benign fashions:

- **i)** Take the case of self-declared "Satanists" and "demonologists".
- **ii)** Within living memory there was a common perception around these ideologies had been (in the UK and USA at least) that they were dangerous and/or abusive **in and of themselves**, because of culturally driven connotations around their self-adopted names.
- **iii)** Investigation into the tenants of their beliefs and the actual practices demonstrated that many of these self-declared "Satanists" were not necessarily and automatically unlawful, abusive or extremist.
- **iv)** One religion or ideology being inherently "distasteful" to members of some other religions or ideologies, does not automatically make the former religion or ideology criminal, dangerous, PREVENT-relevant or extremist.
- **v)** In terms of "policing ideology", CTCOs must focus upon managing the promotion of ideologies that are extremist in themselves (as per the operational guidance on extremism presented within this document), or extremist behaviours around otherwise benign, legitimate, non-extremist, ideologies.
- **vi)** Police must focus upon prevention of criminal behaviours, and also other high-risk behaviours that suggest safeguarding needs, as per the usual Police responsibilities in this area.

Prisons

1) PCM (usually Channel) can be used, where appropriate, to provide support to individuals vulnerable to radicalisation or being drawn into terrorism related activity for other reasons who are serving custodial sentences and who are referred as part of internal risk management processes. This can apply in cases whereby individuals are due to be released from prison and there is a need for some form of intervention or support prior to (or following) release, in order to address identified vulnerabilities. Police and Probation will continue to have a role in assessing risk, vulnerability and the influence of potential radicalisation sources.

2) The decision to refer an offender to PREVENT must be agreed in close consultation with Prison staff and the National Probation Service.

Probation & Youth Offending Services

1) Offenders that are supervised in the community by a provider of probation or youth offending services and are at risk of being radicalised and drawn into terrorism, may be managed by both the appropriate offender management service and Prevent.

Proscribed Organisations & Hate Groups

1) Under the 2000 Terrorism Act[36] (TACT), the Home Secretary may proscribe an organisation if he/she believes it is "concerned in terrorism", and it is judged proportionate to proscribe the group. See HM Government's **Proscribed Terrorist Organisations** webpage for a list. For the purposes of the Act, "concerned in terrorism" means that the group or organisation:
   - **a)** Prepares for terrorism,
   - **b)** Commits or participates in acts of terrorism,
   - **c)** Promotes or encourages terrorism (including the glorification of terrorism), or,
   - **d)** Is otherwise concerned in terrorism.
2) A comprehensive list of organisations and groups proscribed under UK law is available on the Government's website, which is regularly updated by the Home Office. At time of writing, the web address of this site is as shown in the next entry, however if this changes before this guidance document has been updated, CTCOs are encouraged to simply run and internet search for "UK Proscribed Organisation list", and follow the relevant links to the **UK Gov.** Website.

Protective Factors

1) "Protective Factors" can be described as characteristics at the level of biology or psychology, family or community (including peers and culture), which are associated with **lowering** the likelihood of problem-outcomes, or that reduce the negative impact of risk factors upon problem-outcomes.
2) Protective factors are not always merely the positive opposites of risk factors — they act as buffers or mechanisms against undesirable behaviour. For example:
   - **a)** "Anger" is an element of almost all adolescent transitions.
   - **b)** Where adolescents are concerned, when we consider **whether** anger needs managing in a particular Case, or **how** it might be managed, CTCOs should bear in mind that unless it is absolutely necessary, "medicalising" or "criminalising" adolescent anger will often prove counter-productive, and may simply exacerbate the problem.
   - **c)** Hence it might be worth considering mentors that can provide anger-management training, or perhaps redirect the youthful anger through more constructive (or at least less destructive) avenues.
3) Identified risk factors can also help us identify protective factors.
   - **a)** For example, the gap between educational achievement and subsequent professional attainment (leading to high levels of frustration) was identified as a risk factor for young males going to fight for ISIL.
   - **b)** So alongside ideological mentorship to counter the extremist narratives they may have been exposed to, it would may have been reasonable to explore whether expectation- management support and guidance on how to access job opportunities might have made a difference to young males considering travel to Syria.
   - **c)** These may well have constituted protective factors, if they could also be measured in terms of their effectiveness.
4) Positive family and/or social networks can help mediate and decrease various risk factors at Individual, social, political, ideological and cultural levels, including grievances, feelings of alienation and other forms of social exclusion or marginalisation.
5) Linking Individual risk factors to possible protective factors allows for a positive, action-based approach to building a Case management plan. This is the foundation for a genuine preventive outlook in which all kind of risks of radicalisation are mitigated.
6) **Practical considerations:**
   - **a)** You need to be able to **evidence** and **evaluate** the success or failure of any protective factors (and any disruptive tactics for that matter), in order for them to be useful.

[36] United Kingdom: The Terrorism Act 2000 [United Kingdom of Great Britain & Northern Ireland], 2000 Chapter 11, 20 July 2000. Other primary legislation includes: Terrorism Act 2006 & Schedule 18 of the Criminal Justice & Courts Act 2015.

b) If you cannot assess whether an intervention is succeeding or failing in helping to mitigate one of your Case priorities, you should not assume that it is making a difference, or worth the continued time, effort and money put into it.

c) It is often the Case that the mere existence of something (like supportive parents who are pro-Police & pro-PREVENT) is a protective factor. This is no necessarily the Case. Supportive parents were supportive before and during the referral of a Subject into PREVENT, so their presence is not enough to be considered a protective factor by itself. In that circumstance, parents could be described as a potential protective factor, if given appropriate advice / support. CTCOs need to be able to unpack how otherwise supportive parents (or anything else) can be empowered to become a measurable protective factor.

d) Following the implementation of an intervention, different risks and vulnerabilities may escalate, de-escalate, or stay the same. In the Case where one escalates, CTCOs should consider whether other, currently unaddressed, factors may be causing the escalation.

e) Also, a Subject may be responding well to some supportive interventions and may be succeeding at various "healthy" activities, but if there are still **any** escalating or mobilisation factors present, or, depending on their context, potentially any other complex needs, risks or vulnerabilities identified (or not) through the DIF that have not been mitigated through interventions, then these protective factors cannot be regarded as automatically sufficient protection, by themselves, without further evidence of their effectiveness.

Radicalisation

1) "Radicalisation", as used throughout this guidance document, refers to the process by which a person comes to defend, support, or take part in violent extremism, or indeed any offences under UK terrorism legislation.

2) There are different degrees and speeds of radicalisation and there appears to be no single or consistent pathway to becoming a terrorist. In general terms, radicalisation can be regarded as arising from an interplay between "push" and "pull" factors connected to Individuals within their unique life contexts. Radicalising Individuals may be identifiable through their increasingly strident, simplistic or absolutist behaviour, where debating and arguing is replaced with proselytising and contempt for the beliefs of others, and humour and persuasion are replaced with aggressiveness, a desire to impose, or disgust for a target group, potentially culminating in a willingness to physically harm them. Radicalising Individuals may not fully realise or care about the detrimental effects caused to themselves or others by their escalating behaviour. Such awareness may be eclipsed by the sense of belonging and mutual support that their extremist activities might bring.

a) **NB:** Although there are frequently crossovers between the two, not all extremists are terrorists, and not all terrorists have appeared "extremist" by the working definition of this document. So it would be incautious to assume that radicalisation always requires the Individual to be an extremist, as per the definition of extremism given in this guidance document.

b) It is possible for an Individual to identify with and even fixate upon an extremist ideology without going on to commit terrorism offences. Similarly, not all terrorists have been passionate "true believers". Some may feel coerced into action, others may be despairing, nihilistic or self-destructive, others again might be suffering from mental health problems, or else seeking various other non-explicitly ideological forms of violent and narcissistic self-gratification, and so on. Hence the identification of radicalisation (and the prevention of its misidentification) requires careful consideration of a wide range of indicators connected to the Individual in question.

c) CTCOs should bear in mind that nihilistic, suicidal or self-destructive Individuals may sometimes seek "death by Police" in a shootout (or equivalent), or may simply adopt an extremist ideology or cause simply to excuse, or explain, or to give momentum to a more personal and idiosyncratic desire to kill or die for whatever other reason. Individuals such as these may not flag in advance as "radicalised" and potential terrorism-risks if CTCOs prioritise ideology above other risk indicators. The ideological element of the destructive behaviour may not manifest in a way that can be detected until it is too late to PREVENT the destructive actions.

Reasonable Suspicion vs. Reasonable Belief

1) At different stages of the PCM process CTCOs are required to decide and justify whether there is a reasonable suspicion of a PREVENT Relevant concerns or a reasonable belief of the same.
2) "**Reasonable Belief**" and "**Reasonable Suspicion**" are used here in the in the manner that is common parlance to other forms of UK Policing.
3) S.36 (3) of the CTSA stipulates that the Police may:
   a) *"[…] refer an Individual to a Panel only if there are **reasonable grounds to believe** that the Individual is vulnerable to being drawn into terrorism."*
4) However, if this **reasonable belief** is not held at the completion of the Gateway Assessment stage, but there is a **reasonable suspicion** of the same, the Police must ascertain through further information gathering whether this suspicion would be raised to a belief, and therefore requiring safeguarding procedures.
5) The Police may also decide **not** to refer the Subject to a Channel Panel, if they believe it unlikely that more information will become available by doing so that would support making this decision.
6) A "Reasonable Belief" is an inherently higher standard than a "Reasonable Suspicion". It requires a greater level of certainty in order to make out.
7) "Reasonable Belief" is a level of certainty that may be hard to develop within the 5 working days of the PGA phase, even for Cases that may turn out to have distinct vulnerabilities or risks towards terrorism offending.
   a) For CTCOs to keep a Case **open** in PREVENT (or to escalate to PURSUE) after **any use of the DIF** requires a:
      i) **Reasonable Suspicion** that there may be an issue relevant to the PREVENT Duty (or a PURSUE lead) that needs managing or investigating further, one way or another.
   b) For CTCOs to **close** a Case from PREVENT after **any use of the DIF requires** a:
      i) **Reasonable Belief** that there is no PREVENT issue – no vulnerabilities or risks towards terrorism offending – that need investigating further or managing within the PREVENT context, one way or another.
8) **"Reasonable Suspicion" unpacked:**
      i) Firstly, the CTCO / CTCO Supervisor must have formed a **genuine suspicion** in their own minds that, on the **balance of probabilities**, a Subject is vulnerable in some sense to being drawn towards TACT offences if left unsupported by PREVENT, bearing in mind that being "drawn" in this context could include being coerced, groomed or self-propelled through radicalisation, and,
      ii) Secondly, the CTCO's / CTCO Supervisor's suspicion must be **reasonable** after all the processes of the PGA are completed. This means that there must be an objective basis for that suspicion based on **facts**, **information** and/or **intelligence**, which are relevant to the likelihood that an above-described vulnerability is present, so that a reasonable person of similar professional experience to the CTCO would be likely reach the same conclusion based on the same facts and information and/or intelligence.
      iii) CTCOs must therefore be able to explain the basis for these suspicions by reference to these facts, information and/or intelligence about the Subject, the Subject's circumstances, or some specific behaviour by the Subject.
   b) **"Reasonable Belief" unpacked:**
      i) This is a higher level of certainty than above, but it is still a **Subjective** standard, based upon the **balance of probabilities**. It does not mean "beyond reasonable doubt".
      ii) Firstly, the CTCO / CTCO Supervisor must have formed a **genuine belief** in their own minds that, on the **balance of probabilities**, a Subject is vulnerable in some sense to being drawn towards TACT offences if left unsupported by

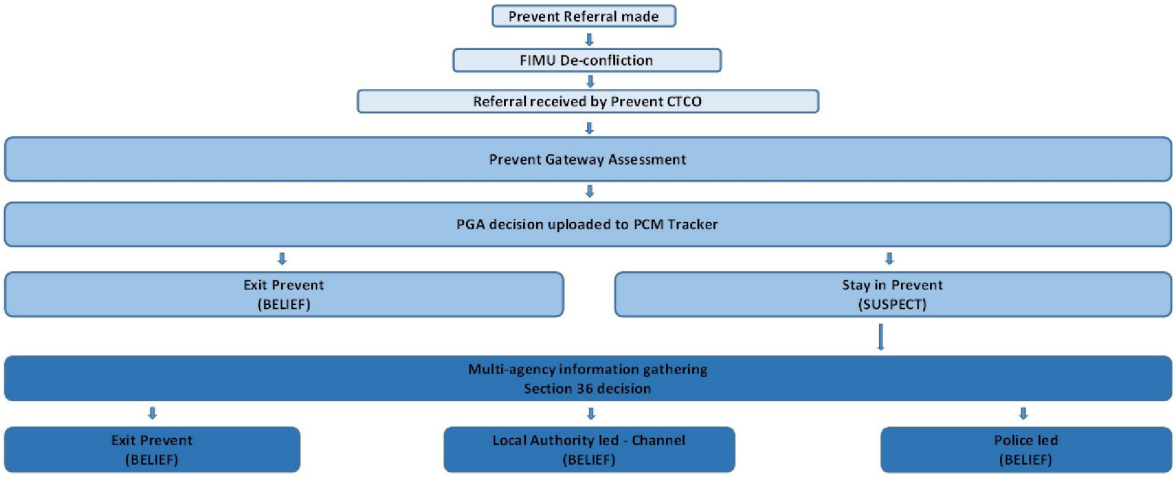
PREVENT, bearing in mind that being "drawn" in this context could include being coerced, groomed or self-propelled towards radicalisation, and,

iii) Secondly, the CTCO's / CTCO Supervisor's belief must be **reasonable** after all the processes of the PGA (and information gather stages) are completed. This means that there must be an objective basis for that suspicion based on **facts**, **information** and/or **intelligence**, which are relevant to the likelihood that an above-described vulnerability is present, so that a reasonable person of similar professional experience to the CTCO would be likely reach the same conclusion based on the same facts and information and/or intelligence.

iv) CTCOs must therefore be able to explain the basis for these beliefs by reference to these facts, information and/or intelligence about the Subject, the Subject's circumstances, or some specific behaviour by the Subject. Belief requires clearer (or more extensive) "proofs", within the balance of probabilities.

9) **NB:** even at this higher level of certainty, CTCO Supervisors and CTCOs should be careful not to slip into looking for proofs that are "beyond reasonable doubt". This is not a criminal standard required for the conviction of offences at court, it is a "balance of probabilities" standard for safeguarding and/or disruptive interventions.

10) **FLOWCHART:**



Referring to Alternative Forms of Support

1) Information sharing between partners will sometimes reveal no evidence that the individual is vulnerable to being drawn into terrorism related activity. It may identify other personal vulnerabilities, which need to be addressed, such as substance misuse or MH issues. Under section 36(6) of the CTSA , where it is determined that support via Channel is not appropriate, the panel must consider whether an individual should be referred to other more appropriate forms of support, which may include support from health providers or Social Care services, and, if so, make such arrangements as the panel considers necessary. It is good practice for the Channel panel chair to consider inviting these partners to panel meetings. Once a decision on managing the case has been reached by the panel, the Channel Panel chair should confirm the recommendation and ensure that the decision is properly recorded, and that arrangements are made to refer the individual.

2) All the same considerations apply to cases within the PLP process for whatever reason.

Reviewing Closed Cases

1) All cases that have been adopted into the PLP process must be reviewed by the CTCO (and the PLP Panel if one was convened for the Case), and approved by the CTCO Supervisor, at 6 months and 12 months from the point of closure. At the point of closure, it is the responsibility of the CTCO to accurately record the closure on the PCMT to ensure review triggers are flagged at the

appropriate time. This review process must be undertaken for all PCM Cases adopted by PLP. This includes those PLP cases that are adopted but are subsequently referred elsewhere. The review process should be informed by relevant information from PLP Partners to Police intelligence systems. Reviews should be completed within five working days of the request being made and should include Police checks, change of circumstances, current social care involvement, any concerns since case closure and contact with the Initial Referrer and/or the last person or organisation that handled the referral prior to in arriving with CTP PREVENT.

Relevant Offences

1) These are not just offences that fall within the breadth of the UK's terrorism legislation.

2) They are also offences that may be more likely than others to signify a potentially greater **vulnerability**, or psychological **capability,** or **propensity,** or even trajectory, towards or TACT offences, for Subjects also identified as possessing a PREVENT issue or concern.

3) They can be regarded as "aggravating factors" to an existing a PREVENT concern.

4) Very generally speaking, previous TACT offences, predatory offences, serious violence and persistent lesser-violence offences tend to be the most directly concerning offences, although CTCOs refer to the DIF questions for a detailed list.

5) Note that relevant offences are "aggravating indicators", not guaranteed "aggravating factors", and as such they need to be considered within their context and in relation to the baseline behaviours and beliefs of the Subject concerned.

6) It is important to take note of the **dates** & **frequency** of any relevant criminal & antisocial behaviour. This can help establish the baseline behaviour for a Subject & therefore highlight "triggered" or mobilising behaviour.

7) **Convictions** for relevant offences *may* increase risk even further, not only reflecting a Subject's confirmed ability to commit such offences, but also the potential that a conviction might create or exacerbate a grievance narratives.

8) Relevant offences include any recorded unlawful extremist conduct or TACT offences or terrorism connected offences, and offences involving **violence**.

Risk Within PCM

1) Risk is a theme that runs through the entire PCM process, thorough both Channel and PLP, whether this is risk to the individual, risk to the public, or risk to Partners or organisations providing support to the individual (including any IPs).

2) Channel Panels in their entirety hold responsibility for the terrorism-related vulnerabilities of a case, meaning the adequate provision and review of supportive interventions around the complex needs and causes of the terrorism-related concern.

3) Statutory partners are responsible for the safeguarding around an Individual's intrinsic and contextual vulnerabilities that can be exploited by others, or that may exacerbate the complex needs of an Individual, to the extent that this Individual may be drawn increasingly towards terrorism offending.

4) Support offered for some individuals could span several agencies and each agency involved will own the element of risk they are responsible for addressing through the support plan. However, the Police, CTCOs, are responsible for the identification and mitigation of imminent risks of Individuals mobilising towards any terrorism offences, and the desistance of such high risk and/or criminal behaviours.

5) The risks of an Individual's involvement in terrorism offending could be posed **by** the individual to themselves and/or to society through their escalating or potentially active involvement in any criminality associated with terrorism legislation. The Police are the most appropriate agency throughout the entire life of each Channel case to assess and manage this risk.

6) The risk relating to the Individuals' terrorism vulnerability, of an Individual being drawn into terrorism and wider safeguarding harms, is addressed and reduced by the Channel Panel.

7) In assessing the terrorism vulnerability, consideration should be given to:

c) the risk posed to the Individual of being radicalised and exploited, and;

d) wider vulnerabilities and needs of the Individual.

8) At this point, Panel members in attendance at a meeting should collectively assess the risk and decide whether the person:

c) is vulnerable to being drawn into terrorism and, therefore, appropriate for Channel;

d) should be referred to a different support mechanism, or;

e) should exit the process (Channel, PLP or PCM altogether).

9) There is a clear expectation that PCM cases remain open until:

c) it is deemed by the Panel, CTCO & Supervisor that the terrorism vulnerability has sufficiently reduced to warrant exit, or:

d) if the terrorism risk has increased, that the case is escalated (either to PLP or PURSUE) for consideration.

10) If consent to receive support is not ultimately secured, or consent is withdrawn, the case will be closed to Channel.

11) Information sharing should also highlight any wider risks posed, which professionals need to be aware of in advance of any visits being undertaken. This could include but is not limited to recording where there is a history of violence, threatening behaviour or use of weapons. All Partners within PREVENT must satisfy themselves that their own processes for undertaking risk assessments to ensure the safety of staff and others are in place and adhered to whilst fulfilling their duties.

Risk Factors & Indicators

1) "Risk Indicators", as used throughout this guidance document, refer to anything that create or suggest potential hazards either **to** a Subject or **by** a Subject.

a) Risk indicators (like vulnerabilities and complex needs) are broad & interconnected. Relevant here are risk indicators pertaining to radicalisation, escalations, triggers & mobilisation indicators. All risks need to be judged in relation to the baseline of the Subject.

b) As a rule of thumb, the presence of **any** risks relevant to PREVENT should also be considered for their potential to become or cause vulnerabilities.

c) So: **potential risk = potential vulnerability = potential risk**.

d) Unresolved vulnerabilities can become risk indicators very quickly, or they can aggravate already existing risk indicators.

Safeguarding

1) The NSIM definition of "safeguarding" [37] suggests that it is the term that describes the function of promoting the welfare of children and vulnerable adults and protecting them from harm. All statutory partners including the Police Service have an Individual and collective responsibility to safeguard and promote the welfare of children and vulnerable adults. Generally speaking, safeguarding relates to the need to protect children and adults who may be in vulnerable circumstances, may have additional needs or may be at risk of abuse or neglect, due to the actions (or lack of action) of another person. In these circumstances it is critical that statutory partners work together to identify people at risk, and put in place interventions to help prevent abuse or neglect, and to protect vulnerable children and adults.

2) In the context of PREVENT, safeguarding can also refer to the process of protecting identified Individuals people who are vulnerable for whatever reason (i.e.: there various and complex needs) in relation to extremism or radicalisation, and supporting them in order to divert, deter or desist them from being drawn towards any terrorism offences or terrorism related activity. Whilst there is no threshold to make a PREVENT referral for an Individual to access assessment and specialist support, it is recognised that there will be occasions where the assessment and support provided through Channel (primarily) to prevent individuals at risk of being drawn into terrorism will run alongside safeguarding processes. A brief overview of the safeguarding frameworks for adults and children are outlined here for reference.

[37] NSIM Guidance 2017, pp. 17-18.

3) Whilst safeguarding and promoting the welfare of children, young people and adults is everyone's responsibility, safeguarding partners, as defined under the Children Act 2004 (and amended by the Children and Social Work Act, 2017), have a statutory duty to work with relevant appropriate agencies within their locality to safeguard and protect children. A safeguarding partner in relation to a local authority area in England is:
   a) the local authority,
   b) a clinical commissioning group for an area any part of which falls within the local authority area,
   c) the chief officer of Police for an area any part of which falls within the local authority area.
4) All three Safeguarding Partners have equal responsibility for fulfilling the role and for selecting the relevant agencies they will work with to safeguard and protect children in each locality, and to publish their local arrangements.
5) Statutory guidance **'Working Together to Safeguard Children 2018'**, sets out the legislative requirements and expectations on inter-agency working to safeguard and promote the welfare of children in England. In Wales, the **"Keeping Learners Safe"** guidance should be referred to which includes advice on radicalisation. The **"Let's Talk About It"** website and the CTnet also contain useful information around radicalisation and safeguarding.
6) Safeguarding adults is also a key role for local authorities. Under the Care Act 2014, local authorities are required to have Safeguarding Adults Boards in their area. These boards provide strategic leadership to the work of the local authority, and partner agencies, on the development of policy and practice in relation to safeguarding adults at risk. Guidance on safeguarding adults, is relevant in England in this context.
7) Under the Social Services and Well-being (Wales) Act 2014, there is a duty on relevant partners to report suspected cases of adults at risk and a complementary duty for the local authority to make enquiries into whether that adult is at risk of a safeguarding harm, and to determine if any action needs to be taken in response. Provision is overseen by six Safeguarding Children Boards and six Safeguarding Adults Boards in accordance with Part 7 of the Social Services and Well-being (Wales) Act 2014.
8) It is essential that Channel Panel members, partners to local Panels and other professionals ensure that children, young people and adults are protected from harm. Whilst the Channel provisions in Chapter 2 of Part 5 of the CTSA are counter-terrorism measures (since their ultimate objective is to prevent terrorism), the way in which Channel will be delivered may often overlap with implementation of the wider safeguarding duty, especially where vulnerabilities have been identified that require intervention from Social Services, or where the individual is already known to Social Services.
9) It is imperative that PREVENT referrals are considered by the local authority and Panel partners alongside their work to safeguard vulnerable individuals. Key links should be established with social services and other Panel partners to ensure that an Individual receives the most appropriate support available. Where a child or an adult is in receipt of Channel support, the Social Worker relevant to that local authority should be present at the Panel and be involved in all decisions. Channel can run in tandem with other safeguarding meetings where safeguarding thresholds have been met.

Sensitive Cases

1) If the case has a Subject considered sensitive due to their occupation (or for any other reason), then CTCOs and Supervisors must consider how best to manage the details

Terrorism

1) In the Terrorism Act 2000 (TACT), terrorism is the use or threat of action, both in & outside of the UK, designed to influence the UK government or any other international governmental organisation, or to intimidate the public or a specific section of the public. This "action" must also be for the purpose of advancing a political, religious, racial or ideological cause. Examples include:
   a) Serious violence against a person or damage to property,
   b) Endangering a person's life (other than that of the person committing the action),
   c) Creating a serious risk to the health or safety of the public or a section of the public,

d) Action designed to seriously interfere with or seriously to disrupt an electronic system.

Terrorism-Connected Offences

1) These are any offences contained within the breadth of UK terrorism legislation.

2) These offences are not restricted to terrorist attacks. Planning, assisting & even collecting information on how to commit terrorist acts are all crimes under British legislation. These offences can be prosecuted as having a "terrorist connection". Examples include:

a) Schedule 18 Criminal Justice & Courts Act 2015: provides a list of offences with terrorist connections, including murder or causing an explosion.

b) Section 5 TACT 2006: Preparing or attempting of terrorist acts.

c) Section 2 TACT 2006**:** Distributing terrorist material intending to encourage it.

d) Section 58 TACT 2000**:** Possessing, collecting or making documents / records useful to preparing or committing terrorist acts.

e) Sections 38B (1) & (2) of TACT 2000**:** Not informing Police of someone preparing terrorism.

f) Section 11 TACT 2000**:** Membership in a proscribed organisation.

g) Section 12 TACT 2000**:** Supporting a proscribed organisation.

h) Section 13 TACT 2000**:** Wearing a Uniform (in the sense relevant to the Act).

i) Sections 15-17 TACT 2000**:** Finance & Money Laundering in relation to Terrorism acts.

j) Section 54 of TACT 2000**:** Weapons Training (in the sense relevant to the Act).

k) Section 56 TACT 2000**:** Directing a Terrorist Organisation.

l) Section 57 TACT 2000**:** Possession of an article for Terrorist Purposes.

m) Section 1 TACT 2006**:** Encouragement of Terrorism.

n) Section 2 TACT 2006**:** Dissemination of Terrorist Publications.

o) Section 6 TACT 2006**:** Providing or Receiving Instruction or Training for Terrorism.

p) Section 8 TACT 2006**:** Attendance at a place for Terrorist Training.

Transferring Cases

1) In the event of a case transfer between areas, the outgoing force must contact the new force at the point at which the move or potential move first becomes known. The general principle is that cases should be managed where the risk is and the NSIM multi-equity principles should be applied. In cases where a Subject is detained under mental health or immigration legislation in an area outside of their normal place of residence, the relevant areas should discuss the case and decide upon the area must suited to continue management of the case on the basis of risk. Where such cases are under Channel, transfers are not a Police decision and instead sit with the Channel Panel. In such cases Home Office Channel Guidance must be followed. Any case transferring between areas must have an up-to-date DIF/VAF completed at the point of transfer by the outgoing force (with the exception of Dovetail cases in which the LACC will complete an outgoing VAF if appropriate). The receiving force must complete a new DIF/VAF upon receipt of the case (with the exception of Channel cases in Dovetail area cases) and if it is a PLP case a new Panel should be organised and a new CMP must be completed and supervised reflecting the change in circumstances arising from the move between areas.

Triggers & Tipping Points

1) "Triggers", as used throughout this guidance document, refer to "tipping points", or significant changes of any sort that may prompt a Subject to move from general stability towards mobilisation behaviours. The focus should be on identifying these shifts as (or preferably before) they happen.

2) Although triggers can be very idiosyncratic & contextual, triggers are likely to be recent or imminent transitions involving loss or crisis, or moves from security & stability to insecurity & instability, e.g.: being the perceived victim of abuse or persecution; withdrawal or rejection of asylum, refugee or residence status; bereavement; loss of job; loss of Partner or children; a major international event prompting moral outrage; a significant & meaningful disappointment, etc..
3) Attacks or high-visibility actions by other extremists / terrorists may become a trigger for a higher-risk PREVENT Subject's own decision to act. An intention towards a "copycat" attack may be identifiable by mental health professionals working with the Subject, or perhaps through an observed escalation in fixated or Mobilisation Identity behaviours by the Subject, or indeed through sudden shifts in a Subject's capabilities, leaked intentions or apparent pursuit of opportunity.
4) It is also worth noting that depending on a Subject's Individual context, a gainful transition (e.g.: an inheritance, a positive change in employment, a new baby or successful medical treatment) might also be a trigger towards mobilisation, in some Subjects, (e.g.: a sense of gratitude or of a debt owed; a feeling of invulnerability; "survivor's guilt", etc.). Sometimes the only thing preventing a Subject from committing a TACT offences are their personal problems, which, if addressed, may actually cause them to mobilise.
5) Triggers must be judged on a Case by Case basis after careful consideration of a Subject's baseline norms & personal contexts.

Unlawful Extremist Conduct

1) Whereas terrorism & terrorism connected offences are described within legislation & official CPS guidelines, the term "unlawful extremist conduct" is used within this document only as guidance.
2) Extremists can, of course, commit TACT offences and other terrorism-connected offences, as described in the previous section dealing with legislation.
3) That said, not all extremists are terrorists (and vice-versa), and within PREVENT we look to disrupt the illegal activities of extremists, falling short of the planning or execution of TACT offences, which fall within the purview of PURSUE.
4) "Unlawful conduct" refers here to behaviour occurring in any part of the UK that is unlawful under UK criminal laws. However, this also includes conduct by UK citizens & residents that occurs **outside** of the UK, providing that the conduct in question would be unlawful under UK laws if it occurred within any part of the UK or its sovereign territories.
5) Unlawful extremist conduct is intended to encompass any ASB & criminal offences that are outside of UK terrorism legislation, but which are initiated by Subjects as **deliberate** & **demonstrable** expressions of their extremist beliefs, or to further an extremist racial, political, religious or single-issue ideological goal or cause.
6) This broad definition is not so much concerned with the specific **nature** of offences as it is their apparent **intentions,** or their extremist **contexts**. Unlawful extremist conduct is established here in order to help CTCOs identify persistent or escalating **courses of conduct** by Subjects within their contexts, & in order to better identify, deter, divert or disrupt escalation towards TACT offences. Unlawful extremist conduct is therefore defined by the **stated extremist rationales** of those committing them.

"Vulnerable to being drawn into terrorism…"

1) This is the wording of the CTSA 2015 and it is the legal basis of what we are supposed to try to identify and mitigate within. Vulnerabilities are discussed in the next few glossary entries, but by "drawn into terrorism" means being groomed, encouraged, coerced, or radicalised into any terrorism related offending, as per the UK's terrorism legislation.

Vulnerabilities & Complex Needs

1) **Vulnerabilities & Complex Needs** are broad & interconnected in terms of the potential of a Subject being drawn, coerced, groomed or otherwise radicalised into extremism or any TACT offences, or exploited in other ways by extremists or terrorists.
2) The PREVENT Duty Guidance defines "vulnerability" in the following terms:

a) *"[…] the condition of being capable of being injured; difficult to defend; open to moral or ideological attack. Within Prevent, the word describes factors and characteristics associated with being susceptible to radicalisation."*

3) If there is absolutely no PREVENT-relevant footprint associated with Subjects or their contexts (meaning that there are no "factors and characteristics associated with being susceptible to radicalisation") the Case is not appropriate for management within PREVENT, although CTCOs must bear in mind their statutory duties in relation to other forms of public safeguarding, & should refer non-PREVENT vulnerable people to the appropriate agencies.

4) As a rule of thumb, the presence of **any** PREVENT risk indicators should also be considered potential **vulnerabilities**.

5) So: **potential risk = potential vulnerability = potential risk**.

6) If left unaddressed, almost any vulnerability could serve to exacerbate an existing grievance narrative, creating a "hook" or "radicalising opportunity" for an extremist-groomer to exploit with an at-risk person. In some Cases they may even become triggers for mobilisation.

7) Similarly, some Subjects not regarded as particularly vulnerable, may actually **become** genuinely vulnerable whilst being managed within PREVENT.

8) We can divide vulnerabilities and complex needs *very generally* into **static** & **dynamic** indicators. This separation is of relevance whilst devising **Case Management Plans** for Subjects.

9) CTCOs must consider what may or may not be achievable in terms of managing or mitigating a Subject's vulnerabilities & complex needs within the timeframe of a Case.

10) Wherever there is any doubt around a vulnerability or need, always seek further professional advice from the **Vulnerability Support Hubs**, particularly with regard to diagnoses or appropriate supportive measures for complex conditions.

Vulnerability Support Hubs

1) The **Vulnerability Support Hubs** help CTCOs in assessing the complex needs of Subjects and the development of intervention plans around them:

   a) The Hubs use a formulation-based approach to support the understanding, management and mitigation of vulnerabilities and risks towards terrorism offending (underpinned by the PREVENT Duty).

   b) The Hubs jointly triage referrals (Police and health) to rate the concern and urgency of each Case based on the referral information and clarifying whether Individuals are known to Mental Health services.

   c) The Hubs then identify, understand and assist in the management the mental health and psychological needs that impact on the risk of terrorism offending and assesses, formulating and recommending further interventions to complex Cases or where interventions to date have failed to mitigate risk.

2) **The Hubs do not replace the CTCO in the Case**, nor do their processes sit outside Channel or PLP.

3) The help the Hubs give is designed to be taken by the CTCO to safeguarding / disruption Panels, Local Authority led or PLP, as bespoke and CT specific, expert advice. In fact the DIF was specifically designed to work in conjunction with the Hubs, so that there is an even greater opportunity of identifying vulnerabilities, risks and threats.

4) Currently each of the Hubs operate in a regional-specific way, so CTCOs must be up-to-date with how referrals to the Hubs works in their area.

5) The Hub process is evolving and will certainly change over the coming months as a standardised national process is developed.

6) **This guidance document will be updated as these changes come into effect.**