COUNTER TERRORISM POLICING

PREVENT STANDARD OPERATING PROCEDURE (SOP)

Owner	CTPHQ-Interventions National Coordinator's Office
Owning Capability	Interventions
Author	CTPHQ Prevent Delivery
Publication Date	25/05/2026
Review Date	25/05/2027
Document Type	Policy
Version	1.0
Contact Details (SPOC)	T1E
Tags	Prevent Channel Interventions
☒	I confirm this document has been subject and passed: - An Equality Impact Assessment - Peer review & De-confliction - A Governance Process

COUNTER TERRORISM POLICING | Prevent

Prevent Standard Operating Procedure (SOP)

May 2026

CTPHQ | Interventions

CONTENTS:

1.INTRODUCTION

2.LANGUAGE

3.COUNTER TERRORISM CASE OFFICERS (CTCO)

4.CTCO SUPERVISOR

5.PREVENT INSPECTOR

6.REGIONAL PREVENT COORDINATORS (RPCS)

7.THE PREVENT CASE MANAGEMENT TRACKER (PCMT)

8.PREVENT REFERRALS

9.FIMU DECONFLICTION

10.PREVENT GATEWAY ASSESSMENT (PGA)

11.MULTI-AGENCY INFORMATION GATHERING

12.THE CTSA SECTION 36(3) DECISION

13.CHANNEL - CTCO DUTIES

14.POLICE LED PARTNERSHIP (PLP)

15.THE NATIONAL DECISION MODEL IN PCM

16. THE PREVENT RISK SCREEN (PRS)

17.PGA AND PRS – MAKING THE GATEWAY DECISION

18.CTSA AND PRS – MAKING THE SECTION 36(3) DECISION

19.CASE CLOSURE

20.SPECIAL CONSIDERATIONS IN PCM

21. MULTIPLE REFERRAL CASES

22.FASCINATION WITH COMMITTING AN EXTREME VIOLENCE OR MASS-CASUALTY ATTACK

23 T1E

24. SUICIDE RISK AND MENTAL HEALTH

25.MULTI-AGENCY PUBLIC PROTECTION ARRANGEMENTS (MAPPA)

26.INTERVENTIONS CENTRE OF EXPERTISE (ICE)

27.OTHER SPECIAL CONSIDERATIONS

28.SIGNPOSTING AND ONWARD REFERRALS

29 T2D T2D NBTC TRAVEL REQUESTS

30 T2D T2D

31.ASYLUM, IMMIGRATION, AND TRAVEL CHECKS

32.SUICIDAL IDEATION, RISK AND SAFEGUARDING

33.SAFEGUARDING MARKERS T2E T2E

ANNEX 1 - PERMISSIVE ENVIRONMENTS

ANNEX 2 - CLINICAL CONSULTANCY SERVICE (CCS)

ANNEX 3 - SUBJECT VISITS

ANNEX 4 - PURSUE SUBJECTS OF INTEREST IN PCM

ANNEX 5 - INFORMATION AND DATA SHARING IN PCM

ANNEX 6 - PREVENT INTELLIGENCE HANDLING ON LOCAL POLICE SYSTEMS

ANNEX 7 - GUIDANCE FOR FORCE DBS TEAMS AND PREVENT POLICE

ANNEX 8 - FALSE COMPLIANCE / DISGUISED COMPLIANCE / INSINCERITY OF CHANGE

ANNEX 9 - REVIEW, RETAIN & DELETE (RRD)

ANNEX 10 – SIX- AND TWELVE-MONTH REVIEWS

ANNEX 11 – SUPPORT AND CASE MANAGEMENT PLANS

COUNTER TERRORISM POLICE: DELIVERING ON THE PREVENT DUTY

CTP-PREVENT STANDARD OPERATING PROCEDURES 2026

FOREWORD

The SOP translates policy principles into clear, repeatable processes to support consistency, accountability and confidence across Prevent activity. It describes the steps colleagues are expected to follow, the points at which decisions are made and the roles and responsibilities involved at each stage.

By providing a common operational approach, the SOP helps ensure that Prevent is delivered fairly and proportionately, regardless of geography, role, or experience. This consistency is essential in maintaining public confidence, managing risk effectively and enabling colleagues to make timely decisions that are robust and defensible.

The SOP should be used as the primary reference for day-to-day practice and governance, ensuring that Prevent activity is carried out in a way that is both operationally effective and aligned to our safeguarding obligations.

Kamal Patel
T/Detective Chief Superintendent
Head of Interventions (CTP-Prevent and Nominal Management)

1.INTRODUCTION

Context: Prevent is a vital part of the UK's Counter Terrorism strategy. Its goal is to stop people from becoming terrorists or supporting terrorism. The world is changing quickly and so are the risks we face; Prevent is evolving to meet these new and more complex challenges. This includes continually improving how we manage cases for both Individuals and Permissive Environments, working more closely with partners, and ensuring staff have the right training and support. CTP Prevent focuses on managing risk in a supportive and effective way, working with our Prevent Duty statutory partners – local authorities, schools, health services, communities and the wider policing family – to identify individuals who are vulnerable to being drawn into any terrorism related offending, spotting the early signs of radicalisation, and intervening before harm occurs.

About this document: This **CTP-Prevent Standard Operating Procedures** (**CTP-Prevent SOP**) document supports and complements the **CTP-Prevent Policy 2026**. It applies to all Counter Terrorism Police (CTP) officers, staff and units with direct responsibility in both Prevent Delivery and **Prevent Case Management** (**PCM**).

Standards: This SOP sets out national standards for PCM. It provides clear, practical steps to help staff make strong, fair, and evidence-based decisions. While it is directed primarily for personnel at CTCO and CTCO Supervisor level, CTP-Prevent staff of all ranks should have a good understanding of these procedures. This document should also be read in the context of:

CTP-Prevent Policy 2026 which outlines the strategic aims and responsibilities of CTP-Prevent delivery,

- Part 5 of the **Counter-Terrorism and Security Act 2015** (**CTSA 2015**), specifically in Sections 26-41.
- The **Terrorism Act 2000** and its updates (henceforth: TACT) for the definition of terrorism and its various offences. "Terrorism," when used in the context of this policy, refers to any terrorism-related offending, violent and non-violent, defined within UK terrorism legislation.
- The **Prevent Duty Guidance 2023**, which sets out the wider requirements of the Prevent Duty for all partners to the Prevent Duty, particularly paras. 246-275, pertaining to Police.
- The **Channel Duty Guidance 2023**, which explains policing's role at Channel panels in England and Wales, or the **Prevent Multi-Agency Panel Duty Guidance 2023 (PMAP)** in Scotland.
- The **Counter Terrorism Policing National Strategy 2025-2030**, which sets out the vision for CTP-UK's development from 2025 to 2030 and includes specific "transformational priorities" for CTP-Prevent.

Core Features: To manage cases well, we must clearly understand the threats and risks involved. This means using the **Prevent Assessment Framework** (**PAF**) to guide our decisions and recording all actions in the **Prevent Case Management Tracker** (**PCMT**). These tools help ensure our work is consistent, accountable, and focused on keeping people and communities safe.

2.LANGUAGE

In this document:

- "**Must**" means the action is mandatory in the stated context.
- "**Should**" means the course of action is recommended, but not mandatory. It implies a best practice that is expected to be followed unless there is a good reason not to. A full rationale must be recorded if it is not followed.
- "**May**" means officers have permission to do the thing described, but **discretion** is available. There may also be other lawful and appropriate options available. For example, s.36(3) of the CTSA states that officers "may" refer an individual who is "vulnerable to being drawn into terrorism" to a multi-agency panel (i.e. Channel), however it is not mandatory to do so. There are other lawful options, e.g., PLP, escalation out of PCM altogether into the Pursue space, other non-PCM support.
- **"Prevent-relevance"** is a practical shorthand used at the Prevent Gateway Assessment (**PGA**) stage to encapsulate all information that broadly indicates a referral subject may be "susceptible to radicalisation" or may be "vulnerable to being drawn into terrorism," or is being influenced by extremism.

  It supports the PGA's lower, triage-stage decision about whether there are reasonable grounds to **suspect** that a Prevent-related concern may be present and therefore requiring information gathering and further assessment.

  A concern may be Prevent-relevant where there is an identifiable link to terrorist ideology, terrorist-supporting activity, terrorist material, radicalisation, or extremist ideology or direct extremist influence / coercion / exploitation / grooming, or any other plausible pathway by which the referral subject may be drawn towards any terrorism-related offending.

  A Prevent-relevant terrorism link may be emerging, unclear or mixed. The PGA does not require a fully formed ideology or a clear terrorist affiliation. The Channel Duty Guidance recognises that there is "no single pathway" to radicalisation and that factors may include exposure to radicalising influences, grievances and susceptibility. It also recognises that Prevent includes early intervention to stop people **becoming** terrorists or **supporting** terrorism.

  However, general safeguarding concerns, mental health issues, neurodivergence, criminality, hateful views, public order concerns, or vulnerability in isolation are not Prevent-relevant unless they are 'aggravating' an identifiable Prevent-relevant link.

  Prevent-relevance is **not** a statutory test and must not be treated as a substitute for the legal threshold in CTSA s.36(3). Where a case progresses beyond PGA to the s.36(3) decision, officers must only use the statutory threshold itself: "there are reasonable grounds to believe that the individual is vulnerable to being drawn into terrorism."

3.COUNTER TERRORISM CASE OFFICERS (CTCO) – ROLE PROFILE

Basic Requirements

- **Rank:** Constable/Detective Constable or equivalent staff
- **Experience:** Multi-agency work; risk management; investigation experience; preferably also experience assessing intelligence.
- **Security Clearance:** Must hold at least SC (Enhanced) vetting.
- **Training:** Up-to-date force-led safety and first aid training. See Interventions Training QRG for latest CT requirements.
- **T2E - Various management and Intelligence databases**
- Maintain current operational knowledge of Prevent legislation, policy, and procedures.

Prevent Case Management (PCM)

- Manage Prevent cases and mitigate risk through all stages from the Prevent Gateway Assessment (PGA) to closure.
- Complete relevant and timely enquiries to complete the PAF (PRS / SA) at every stage of PCM.
- Use the Channel Support Plan and PLP Case Management Plan functions within PCMT to ensure all PCM activity is recorded clearly, accurately and contemporaneously (insofar as is practicable). This includes documenting officer rationale, activities undertaken, and ongoing updates within PCMT.
- Demonstrate professional curiosity, evidence-led decision-making and multi-agency assurance in relation to all PCM's operational concerns. This includes practitioners being alive to, and endeavouring to **corroborate** – and where necessary, **mitigate** – any concerns around "disguised compliance", "false compliance" and "insincerity of change." All concerns must be discussed with supervisors, multi-agency panel members and IPs, with the intention of devising a common approach to mitigate the issue. All concerns and actions around them must be recorded on the PCMT.
- Submit new intelligence to FIMU for Pursue Assessment and de-confliction – this includes new intelligence from the community and partners and also updating FIMUs on any relevant changes to risk during PCM.
- Collaborate with partners to deter and prosecute extremist activity.
- Close cases when the s.36 CTSA threshold is not met, or risks are mitigated, or all options exhausted.
- Ensure appropriate onward signposting has been completed on cases exiting PCM. Consider onward referrals to relevant agencies / third parties for safeguarding, law enforcement and mitigation of other risks.
- Where directed by a supervisor, provide operational advice and support to Pursue operations where they intersect with PCM.

Channel Duties

- Refer and present cases to Channel panels, providing monthly CTP updates to live cases and at 6/12-month reviews.
- Act as SME on CT offending risk, owning this risk, and advising the panel on management of said risk.
- Along with the panel, identify the most relevant Intervention Provider (IP) for the case, then task and risk assess deployment.
- Should there be an escalation of risk, the CTCO may remove a case from Channel if appropriate.
- Update PCMT on behalf of Channel panel with Support Plan, updates and minutes.

Police-led Partnership (PLP)

- Attend and present cases to PLP panel.
- Update PCMT with Case Management Plans (CMPs) and updates.
- Where possible, deliver interventions (supportive or disruptive) and risk assess IP deployment where relevant to the case.

Partnership Working

- Provide updates to Prevent Boards, or local equivalent, where approved by supervisors.
- Contribute to CTLP development and delivery.
- Utilise police powers to manage Permissive Environment referrals alongside the Local Authority.
- Assist in raising awareness of the Prevent Duty to police forces, and assist in raising awareness of best practice for Prevent referrals.

4.CTCO SUPERVISOR – ROLE PROFILE

Basic Requirements

- **Rank:** Sergeant/Detective Sergeant or equivalent staff.
- **Experience:** Investigative work, ability to assess intelligence and conduct risk assessments.
- **Security Clearance:** Must hold at least SC (Enhanced) vetting. Should attain DV where possible within the regional context.
- **Training:** Up-to-date force-led safety and first aid training. Ensure staff meet mandatory training and CPD requirements (see Interventions Training QRG).
- **T2E - Various management and Intelligence databases**
- Maintain current operational knowledge of Prevent legislation, policy, and procedures.

CTPHQ000410_0008

Prevent Case Management

- Supervise Prevent case management and mitigation of risk from PGA to closure.
- Set and review Activities, Channel Support Plans and PLP Case Management Plans for the CTCO to conduct.
- Review and supervise PAF reports for quality and timeliness.
- Quality assure PCMT entries for categorisation, clarity, accuracy, and completeness.
- Ensure intelligence is submitted to FIMU appropriately.
- Support CTCOs with case progression to make appropriate case decisions, closures and signposting.
- Update and, in consideration with CTCO's findings, refer to Inspector where Multiple Referral or a complex case requires special consideration.
- Provide operational advice and support to Pursue operations where Prevent intersects.

Channel Duties

- Oversee referrals and presentations to Channel panels.
- Can include CTCO duties, as operational demands dictate.
- Ensure CTP-Prevent attendance at every local Channel Panel.
- Support CTCOs in IP deployment decisions and risk assessments.
- Review, approve and ensure implementation of CTCO specific elements of Channel Support Plans.
- Ensure PCMT updates reflect Channel panel decisions and Support Plans.
- Where necessary, challenge decisions and activities by partner agencies.

Police-led Partnership

- Review, approve and ensure implementation of Case Management Plans.
- Support the delivery and evaluation of interventions.
- Continually review the suitability of transferring the case to Channel for support.
- Act as Deputy Chair for PLP panels, reviewing actions and updates provided by police and partner agencies. Supervisors should not chair cases in which they have acted as a decision-maker, although resourcing constraints may mean this is not always possible. As Channel Chairs already exercise oversight of the Channel cases for which they are responsible, the PLP SOPs recognise that, where necessary, there is a legitimate operational precedent for the same approach to be adopted in PLP cases.

Partnership Working

- May provide updates to strategic meetings and Prevent Boards, or local equivalent, where approved by Prevent Inspectors.
- Lead CTLP development and ensure delivery of police objectives aligned to the LA Prevent plan.

- Utilise police powers to manage "Permissive Environment" referrals alongside the Local Authority.
- Promote Prevent Duty awareness and referral pathways across police forces.
- Liaise and support local police Prevent leads.

Performance and Development

- Manage staff and monitor team performance, ensuring delivery against Prevent objectives and operational standards.
- Support staff welfare and identify development needs of CTCOs.

5.PREVENT INSPECTOR – ROLE PROFILE

Basic Requirements

- **Rank:** Inspector/Detective Inspector or equivalent staff.
- **Experience:** Investigative work, ability to assess intelligence and conduct risk assessments.
- **Security Clearance:** Must hold DV, in order to maintain the 'firewall' between CTP-Prevent and Pursue, T2D.
- **Training:** Up-to-date force-led safety and first aid training. Ensure staff meet mandatory training and CPD requirements (see Interventions Training QRG).
- **T2E - Various management and Intelligence databases**
- Maintain current operational knowledge of Prevent legislation, policy, and procedures.

Strategic Oversight of Prevent Case Management

- Provide leadership and strategic direction for Prevent casework across CTCO and Supervisor teams.
- Ensure consistency and quality in PAF application and PCMT usage.
- Provide strategic advice and support to Pursue activities where they intersect with CTP-Prevent.
- Authorise case closures for Multiple Referral cases and when CTP-Prevent policy and SOPs dictate.
- Review complex or high-risk cases upon request by CTCO Supervisors, providing enhanced oversight for cases requiring it – T1E, or fascination with committing extreme violence or mass casualty attack cases, etc.

Channel and PLP Governance

- Support Supervisors in ensuring CTP-Prevent representation at every local Channel panel.
- Resolve escalations or disputes arising from PLP panels, and, where appropriate, Channel panels.

- Ensure Supervisors are effectively chairing PLP panels, implementing CMPs and managing risk appropriately.

Partnership Leadership

- Represent Prevent policing at strategic multi-agency boards (e.g. Prevent Boards, Contest Boards).
- Lead development and delivery of CTLPs in collaboration with partners.
- Ensure police contributions to LA Prevent plans are aligned and effective.
- Promote Prevent Duty compliance across policing and partner agencies.
- Support Supervisors in managing Permissive Environments referrals and safeguarding escalations.

Performance and Development

- Monitor team performance, ensuring delivery against Prevent objectives and operational standards.
- Identify training needs and support professional development of CTCOs and Supervisors.
- Support organisational learning and quality assurance processes for Prevent casework and partnership activity.

6.REGIONAL PREVENT COORDINATORS (RPCS) – ROLE PROFILE

Strategic Leadership and Governance

- Lead the regional CTP-Prevent function, ensuring delivery of strategic objectives across Prevent teams.
- Strategic link between regional CTP-Prevent delivery and CTPHQ, contributing to national policy development and ensuring alignment with overarching CTP priorities.
- Set direction and priorities for CTP-Prevent casework, partnership engagement, and operational delivery.
- Ensure regional CTP compliance with the CTSA 2015, the Channel Duty Guidance and the Prevent Duty Guidance, **Counter Terrorism Policing National Strategy 2025-2030**.
- Represent Prevent at Regional and national governance boards, including CONTEST and Prevent Boards.

Operational Oversight

- Oversee performance and quality assurance across all levels of CTP-Prevent casework.
- Ensure regional consistency in the application of PAFs, PCMT usage, and PLP cases.
- Provide strategic input into complex or high-risk cases.
- Ensure PLP cases across the region have CMPs completed and that subject visits are risk assessed. Refer to the **RISK ASSESSMENT AND SAFETY** paragraphs in the **SUBJECT VISITS** section of this document.

- Ensure appropriate escalation and resolution of operational issues across the region. Provide oversight on closure of cases where risk remains but no further mitigation is available or where continued management by CTP-Prevent is deemed disproportionate.

Workforce Management

- Lead and manage a multi-tiered team of CTCOs, Supervisors, and Inspectors.
- Oversee recruitment, training, and professional development across the Prevent workforce.
- Promote a culture of continuous improvement, safeguarding, and ethical policing.
- Ensure staff welfare and resilience are supported across the Prevent network.

Partnership Engagement

- Develop and maintain strategic relationships with LAs, education, health, and other statutory partners.
- Where possible, assist in regional engagement with external stakeholders to promote effective referrals.
- Coordinate with Police Force Prevent Strategic Leads (FPSL) for regional police adherence to the Prevent Duty.
- Ensure delivery of CTLPs and alignment with local Prevent plans.

Performance and Risk Management

- Monitor regional performance against national Prevent KPIs and objectives.
- Identify emerging risks, trends, and threats, and ensure appropriate operational and strategic response.
- Identify appropriate cases for Organisational Learning Reviews.
- Lead internal audits and contribute to national reviews and inspections.
- Ensure intelligence-led decision-making and integration with Pursue, Protect and Prepare strands of CT policing.

7.THE PREVENT CASE MANAGEMENT TRACKER (PCMT)

Overview:

- **The PCMT** is the national CTP-Prevent case-management system used to record and manage Prevent referrals through the full lifecycle of PCM.
- The system must be used to record case details, assessment activity, support and management plans, actions, information gathering, decision rationales, supervisory approvals, Channel/PMAP and PLP activity, closure outcomes, signposting and relevant post-closure review activity.
- The PCMT is not simply an administrative database: it is the primary auditable record of what was known, what was done, what decisions were made, who approved them, and why.
- All entries must be accurate, timely, proportionate and sufficiently clear to support supervision, assurance, review, disclosure and lawful information management.

Using the System:

- This SOP is designed to be a "how-to" document for the principles and purposes of PCM. It is not a step-by-step "click here" guide to using the PCMT.
- CTCOs and Supervisors should familiarise themselves with the PCMT's step-by-step user guides, available through the PCMT's opening page, but listed below for convenience, with hyperlinks directly to them. Use your NHOP common sign-in details to access the guides when prompted.

PCMT User-Guidance Homepage: PCMT Training and Guidance Home

Prevent Documents and Support:

- Logging into PCMT and Page Layout
- Searching and Viewing Prevent Cases on the PCMT
- Creating a New Case
- Editing a Subject
- Uploading a File
- Allocating a Case
- Creating a Note
- Conducting a PRS (PAF)
- Managing PRS Assessments for Supervisors
- Conducting an SA (PAF)
- Managing SA Assessments for Supervisors
- Create and Manage Support Plans
- Create and Manage Case Management Plans
- Managing RRD Approval Requests
- Creating and Managing Activities
- **PCMT How-to Guides**
  - Recording Consent Contact
  - PCMT - Progressing Cases
  - PCMT - Recording Reviews
  - PCMT - Creating and Managing Activities
  - PCMT - Viewing Case History
  - PCMT - Dashboard for CTP Users

8.PREVENT REFERRALS

Overview:

- A Prevent referral is any information sent specifically to CTP-Prevent that suggests that a named individual may be susceptible to radicalisation or otherwise vulnerable to being drawn into any terrorism related offending, violent or non-violent.

Referral Sources:

- Referrals may come from anywhere within the UK, including Northern Ireland (NI) – even though NI authorities are not otherwise obligated under the Prevent Duty. The three main sources of referrals are:
  - Members of the public – e.g. direct reporting, Act Early, etc.,
  - Non-Police statutory partners listed under Schedule 6 of the CTSA 2015,
  - Policing and law enforcement partners, inc.:
  - CT policing, e.g., officers from CTP-Prevent, Pursue, Protect or Prepare units.
  - Non-CT policing, e.g., local policing, emergency response, specialist investigation units, other Forces mentioned under s.6 CTSA, etc.

Prevent Referrals:

Any information received about an individual will be treated as a Prevent referral if one of the following applies:

- The National Referral Form (NRF), or any regional Prevent referral form, has been used,
- The information is marked as being a Prevent referral, even though a referral form has not been used.

Other Prevent-relevant information:

Information that is not a Prevent referral, which may or may not be treated as a referral by CTP-Prevent, at the discretion of CTCO-Supervisors, e.g.:

- Information pertaining to institutions and “permissive environment” concerns.
- Information about an individual that is marked as being suitable for CTP-Prevent review, but which is not a Prevent referral, could just be "further information" that adds to an existing case.
- There is information that may contain terrorism, extremism, radicalisation concerns, or an indication that an individual may be “vulnerable to being drawn into terrorism”, but the FIMU assess the information as potentially Prevent relevant and do not wish to retain the referral solely in the Pursue space.

Multiple Referrals:

- These are often indicative of heightened cumulative risk and involves special considerations.
- For more detail concerning what information is in-scope as a "multiple referral" (as opposed to duplicate referrals or intelligence reports), please to the Multiple Referral paragraphs in the **SPECIAL CONSIDERATIONS IN PCM** section of this document.

T1E

Referrals from Pursue:

- Officers in the Pursue space may wish to refer one of their Subjects of Interest (SOIs) or a T2D. There is a process to follow for this. Refer to the **PURSUE SUBJECTS IN PCM** section of this document for more details.

9.FIMU DECONFLICTION

Deconfliction:

- This is the process by which a FIMU, potentially in communication with an OIMU or an SIO, establishes whether the subject of a referral is already being managed in the Pursue space, or **should** be managed in the Pursue space.
- All referrals, regardless of their 'type' or source, **must** be assessed by a FIMU before any Prevent-specific information gathering, assessment or case management can begin. This T2D ensures decisions are made with the full intelligence picture.
- If a referral arrives directly with CTCOs without FIMU deconfliction, CTCOs must record basic biographical details of the referral subject and a summary of the concerns onto the PCMT and then send the referral straight to the FIMU.
- The FIMU checks the name and address of the referral subject against T2D T2D - CTP Intelligence system, "de-conflicting" the referral for Pursue relevance – such as live investigations, active CT interest, or immediate intelligence leads.
- The FIMU also checks T1E local police systems, the findings of which should be sent to CTCOs if the referral is passed to Prevent.

RADO Numbers:

- FIMUs deconflict referrals through the *Receive, Assess, Decide, Outcome* (RADO) process and assigns the referral a number (1-6). The majority of referrals passed on to Prevent will be RADO 5 and 6. The assigned number by FIMU should be entered into the PCMT in the corresponding drop-down field:
  - **RADO 1-3** = primarily retained by Pursue as leads or investigations. *May* be compatible with Prevent management on a case-by-case basis, decided between the SIO and CTCO Supervisor. Refer to the Pursue Subjects in PCM section of this document for more details.
  - **RADO 4** = CTP-relevant intelligence enhancement. May be compatible with Prevent management on a case-by-case basis.
  - **RADO 5** = CTP Relevant but no further IMU actions or development - deemed suitable for Prevent assessment.
  - **RADO 6** = no CTP relevance identified – still potentially suitable for Prevent assessment if on an NRF.

Visiting the subject pre-deconfliction:

- CTCOs must not contact the referral subject prior to de-confliction. Please refer to the **SUBJECT VISITS** section of this document.

10.PREVENT GATEWAY ASSESSMENT (PGA)

Overview:

- The Prevent Gateway Assessment (PGA) is the CTP-Prevent triage stage carried out on all deconflicted referrals to establish the presence of a current Prevent-relevant issue.
- For PRS decision-making and the "reasonable suspicion" threshold, refer to the **PGA and PRS – Making the Gateway Decision** section of this SOP. For the National Decision Model in PCM, refer to the **Decision-Making** section.

Supervisor responsibilities:

- Supervisors must ensure all referrals have been submitted to FIMU for deconfliction before any Prevent-specific work begins, except for recording a skeleton casefile with biographical details and a summary of the concerns;
- allocate deconflicted referrals to CTCOs and ensure regular updates on PCM activity and decisions are recorded on the PCMT;
- ensure PCM processes are followed, demonstrating professional curiosity while gathering and assessing information;
- ensure national police data-recording standards are followed, with relevant details recorded in the correct PCMT fields with accuracy, clarity and professionalism;
- supervise the PRS and agree the Gateway Decision, ensuring the rationale is consistent, justifiable, based on the best information available, and reached through using the PRS tool;
- assess suitability for closure and apply the appropriate closure code on the PCMT;
- manage cases in Pending Closure, checking the Pending Closure queue to quality assure cases submitted for closure by CTCOs;
- ensure external safeguarding or investigatory referrals are made and recorded in adequate detail;
- come to a joint PGA decision with the CTCO and Supervisor. If unresolved differences of opinion remain, the Supervisor must provide a clear summary of the disagreement and rationalise the final decision. This may be escalated to the Prevent Inspector for additional oversight if necessary.

Allocating the referral:

- Once a deconflicted referral is received from FIMU, either a Supervisor or CTCO may enter the referral details onto PCMT, depending on the administrative setup of the region, if the referral is not already recorded.
- The CTCO Supervisor must review the referral and allocate it to a CTCO for management through the PGA stage.

CTCO Reviews FIMU handover:

- At the start of PGA stage, CTCOs must review the FIMU handover. This includes:
  - Reading the referral in its entirety;
  - confirming the RADO outcome and deconfliction date;
  - studying the original referral form and any handover notes from FIMU;
  - checking for attachments;

Starting a new case and completing PGA:

- CTCOs allocated a referral must commence work on the PGA stage as soon as practicable.
- CTCOs must work through each PCMT page methodically, completing as many relevant fields as possible. Relevant tags and drop-down categories must be selected, and all entries must be checked for spelling, accuracy and professionalism.
- Five working days is the recommended time to complete a PGA triage. This is best practice rather than a mandatory requirement and is subordinate to local risk management considerations.
- For granular instructions on creating cases, selecting fields, drop-down menus and tags, refer to the step-by-step guidance available through the PCMT homepage under **PCMT Training Information, Prevent Guidance and Channel Guidance**.

Background checks:

- At PGA, CTCOs should normally rely on the referral, FIMU handover, police checks, open-source checks where appropriate, and clarification from the referral originator.
- Background checks must be conducted by FIMU, with the CTCO filling in any gaps. Details must be recorded as Activities on the PCMT.
- As a minimum, CTCOs must consider checks on:
  - PCMT;
  - T1E
  - T1E
  - T1E
  - local crime systems;
  - intelligence systems;
  - safeguarding systems.
- T1E
- Where relevant to the referral concerns, CTCOs should also consider contextual checks, including:

- T1E
- immigration status;
- T1E

- If reasonable suspicion of a Prevent-relevant concern has already been established at PGA, the contextual checks may be completed during Information Gathering instead.
- CTCOs must record the full results of checks completed, including identifiers used and any limitations to the search. Records must include all details that may be relevant to assessing the referral concerns, e.g.:
  - T1E

Recording biographical and case information:

- If not already complete, CTCOs must establish and record all biographical data requested under the Individual section of the PCMT casefile.
- Where information is not known, CTCOs should endeavour to ascertain it where lawful and proportionate.
- CTCOs must also identify and record as much relevant case information as possible in the correct PCMT sections, including Details, Activities and Notes.
- Where proportionate, and without compelling the referral subject or causing undue distress, CTCOs should endeavour to ascertain and record the protected characteristics of the referral subject. This may support the positive requirements of the Equality Act 2010. It may not be appropriate in every case to ask about these characteristics, and officers must be alert to case-specific sensitivities.

Multiple referrals:

- CTCOs must check for previous or open PCM referrals.
- Multiple referrals will, in most cases, provide reasonable suspicion to progress through PGA into Information Gathering.
- Inspector endorsement is required for closure of multiple-referral cases.
- Refer to the **Multiple Referrals** section in **SPECIAL CONSIDERATIONS IN PCM**.

Uploading documents to PCMT:

- CTCOs must upload relevant documents to supplement the case or subject details throughout the lifetime of the case, e.g.:
  - photos;
  - referral documents;

- relevant correspondence;
- returns from partner agencies;
- minutes from panel meetings;
- documentary evidence relating to the concerns in the referral.

- Refer to **PCMT Guidance Home – Uploading a File** for detailed instructions.

Contacting the Referrer:

- Wherever possible, CTCOs must contact the person referring or the original source of the concern.
- For clarity, on the PCMT:
  - **Person Referring** means the specific named individual who initially identified and reported the Prevent issue, for example a doctor, teacher or safeguarding lead;
  - **Referral Originator Sub-Group** means the specific unit, team or institution within which the person referring works, for example Westshire Psychiatric Unit or Westshire Sixth Form College;
  - **Referral Originator** means the overarching agency or statutory partner within which the sub-group is situated, for example Health or Education.
- CTCOs may contact the referral originator to clarify the concern, source, context, credibility, reliability and any missing information required for the PGA decision. When discussing the referral, CTCOs should:
  - confirm that the details held are what the referrer intended;
  - record any new details, risks, vulnerabilities, protected characteristics and other relevant information, including associates or social media IDs;
  - provide reassurance where appropriate;
  - explore the immediate circumstances of the Prevent concern and the wider situation of the referral subject;
  - identify any permissive environments linked to the subject, including places where the referral subject may be radicalising or being groomed towards terrorism-related offending, online or offline;
  - corroborate relevant referral details where possible, such as diagnoses of illness or mental health conditions.

Credibility and reliability:

- CTCOs must enter all relevant information into the PRS, noting where missing information needs to be sourced.
- CTCOs must consider the credibility and reliability of the information source.
- Where information or sources are deemed non-credible or unreliable, CTCOs must consult with Supervisors to decide next steps and record all relevant details.

- Refer to the **FALSE COMPLIANCE / DISGUISED COMPLIANCE** annex of this document.

Family members / co-residents of concern:

- CTCOs must consider whether people closely connected to the referral subject are themselves current or previous Prevent or Pursue concerns. This includes:
  - checking the referral subject's usual residence address against CTP systems, T1E and PCMT, or confirming that FIMU has completed this;
  - determining whether the referral subject has family members who are, or were, in PCM, or who are or were CT Subjects of Interest (SOIs);
  - considering whether the referral subject lives with non-family PCM subjects or Pursue SOIs – e.g., in a multiple-occupancy house or hostel.
- Such links may be sufficient to progress the referral Subject into Information Gathering, depending on the case-specific context. If these links exist but are not assessed as relevant in the circumstances, the closure rationale must explain why.
- Refer to the PURSUE SUBJECTS OF INTEREST IN PREVENT CASE MANAGEMENT section of this document when deciding whether to make Prevent referrals for family members or co-residents of Pursue SOIs before or after a Pursue-led Executive Action. Family members and co-residents may or may not be relevant for their own Prevent referrals.

Non-CT Safeguarding and Crime:

- Where urgent non-Prevent safeguarding needs relating to the referral subject or family members are identified during PGA, and were not apparent or actioned during FIMU deconfliction, these must be communicated to the most appropriate local unit, team or external partner at the earliest opportunity.
- Details of this signposting must be recorded on the PCMT.
- If safeguarding concerns were included in the FIMU handover but not actioned by FIMU, CTP-Prevent may refer these issues back to FIMU to action.
- Where previously unidentified and unreported crimes are discovered by CTCOs in relation to the referral subject or family members, these must be reported:
  - to FIMU, if terrorism-related; or
  - to the relevant non-CT investigatory team / unit as soon as possible, using the approved local processes.
- Details must be recorded on the PCMT.
- If offending concerns were included in the FIMU handover but not actioned by FIMU, CTP-Prevent may refer these issues back to FIMU to action.

Visiting / Contacting the subject during PGA

- CTCOs should complete all PGA checks and the PRS without visiting the subject.

- Once reasonable suspicion is identified, no further probing is required at PGA.
- Refer to the **VISITS BEFORE FIMU DECONFLICTION** paragraphs of this document..

Contacting partner agencies during PGA:

- Beyond the referral originator or original source, statutory partners must not normally be contacted at PGA.
- PGA is the triage stage and must not become a broad multi-agency information-gathering exercise.
- Contact with another statutory partner at PGA may only take place where:
  - a specific and vital piece of information is required for the PGA decision;
  - the information cannot be obtained by another lawful and proportionate means;
  - the request is necessary to decide whether reasonable suspicion of a Prevent-relevant concern exists;
  - the CTCO has identified that the partner holds specific information vital to the PGA decision;
  - the CTCO has considered whether the information is reasonably likely to change the assessment, bearing in mind the relatively low bar of reasonable suspicion;
  - Supervisor approval is obtained before contact is made;
  - the Supervisor ensures that the decision and justification are recorded in full and are necessary within the circumstances of the case;
  - the rationale and decision are recorded on the PCMT before contact is made.

The PGA Decision:

- Where reasonable suspicion is established, the case should normally progress to Information Gathering.
- Where the PGA threshold is not met, the case must be closed to PCM.
- Any remaining non-CT safeguarding, welfare or criminality concerns must be referred or signposted to the appropriate agency or policing team.
- For guidance on making the PGA decision, and for onward referrals for closed cases, refer to the **CONDUCTING A PRS (PAF)** and **MANAGING PRS ASSESSMENTS FOR SUPERVISORS** PCMT user-guides, and following sections of this document:
  - **THE NDM IN PCM**
  - **PGA AND THE PRS**
  - **PREVENT REFERRAL SCREEN (PRS)**
  - **SIGNPOSTING AND ONWARD REFERRALS**

11.MULTI-AGENCY INFORMATION GATHERING

Overview:

If the PGA stage provides either a reasonable suspicion or reasonable belief of a vulnerability to being drawn into terrorism, the referral is moved into the multi-agency information gathering stage.

Objectives:

Increase PGA information reliability and to deepen intelligence picture to support making a CTSA s.36(3) decision. This involves gathering pertinent information from relevant multi-agency partners to:

- Corroborate single-source or hearsay information;
- Fill-in missing biographical data from the PGA stage;
- Address unanswered PRS questions from the PGA stage;
- Establish any other "complex needs" or "push and pull" factors that may help identify whether the referral-subject vulnerability to being drawn into terrorism;
- Identify other relevant gaps in currently held data and consider where this information can be legitimately sourced.

Subject Visits During Information Gathering:

Visiting a Subject during the Information Gathering phase is not prohibited, but it must be decided on a case-by-case basis. Refer to the **VISITS DURING INFORMATION GATHERING** paragraphs in the **SUBJECT VISITS** section of this document.

Supervisor Actions:

Supervisors must set clear Activities for CTCOs to log in PCMT's Activities function and then complete, e.g.:

- Information sharing request to statutory partners.
- T1E
- Request the school, college, university or employer review the subject's internet filtering and monitoring alerts (where appropriate).
- Further discussions with professionals already involved with subject, wherever required, e.g., social worker, etc.

Recording Standards:

Supervisors must ensure that activities and Information Gathering returns are recorded on the PCMT under 'Activities' - not only within the 'Notes' or the PRS.

Data Sharing Requests:

Providing they are relevant to the case, CTCOs will engage the Partners of Local Panels, i.e., relevant partners listed in Schedule 7 of the CTSA 2015.[1] CTCOs must issue structured requests via agreed local processes and data-sharing agreements (DSA). If a DSA request template is unavailable, refer to the Information Commissioner's Office website, Annex B: Data sharing request form template[2]. Requests should include, as a minimum:

- **Purpose:** To support a Section 36(3) decision under CTSA 2015.
- **Lawful basis for sharing request:** local data-sharing agreements; s.38 CTSA 2015; GDPR Article 6(1)(e) and Article 9(2)(g). For cases that officers know from deconfliction cannot go to Channel: s.115 Crime and Disorder Act 1998; s.31 and s.35 of the Data Protection Act 2018
- **Data Required:** the specific data requested by the CTCO (e.g. attendance records, safeguarding concerns, relevant health concerns, social services activities, etc), plus any concerns the partners may themselves volunteer as potentially relevant in relation to their duty under s.26 CTSA 2025 – *"A specified authority must, in the exercise of its functions, have due regard to the need to prevent people from being drawn into terrorism."*
- **Example form of words:** "This request is made under Section 36 and Section 38 of the Counter-Terrorism and Security Act 2015. The lawful basis for processing under GDPR is Article 6(1)(e) (public task) and Article 9(2)(g) (substantial public interest). Please provide any information relevant to assessing whether [Subject Name, DOB] is vulnerable to being drawn into terrorism, including [safeguarding concerns, mental health indicators, contextual risk factors]." This is simply an example form of words and not at all mandatory.
- **Purpose Limitation:** Data will be used to fulfil the specific and general duties detailed under s.36 CTSA 2015.
- **Partner Information Sharing Request Response Timeframe:** 5 working days – Channel Duty Guidance 2023, para.91.

Protected Characteristics and Special Category Data:

Information gathering may return both the following kinds of sensitive personal data:

- **Protected Characteristics:**
  - **Recording Standards**: Under the Equality Act 2010 Public Sector Equality Duty, policing activity must be capable of demonstrating due regard to eliminating discrimination and advancing equality. Recording protected-characteristic data (beyond what is deemed necessary to manage the CT related risk of a referral within PCM) may support this duty, but such additional data must only be collected where it is lawful, necessary, and proportionate, and where it clearly serves a defined

[1] Counter-Terrorism and Security Act 2016, Schedule 7, Partners of Local Panels
[2] Information Commissioner's Office, Annex B: Data sharing request form template, for use by the organisation making the request for data sharing.

policing purpose in accordance with data-protection legislation and national policing information-management standards.

- **Characteristics:** Age; Disability; Gender Reassignment (as opposed to biological sex); Marriage and Civil Partnership; Pregnancy and Maternity; Race; Religion or Belief; Sex (as opposed to "gender reassignment"); and Sexual Orientation.

- **Special Category Data:**
  - **Recording Standards:** defined under Article 9 of the UK GDPR, there is crossover between this category of data and the protected characteristics, above. Aspects of this data may be relevant to PCM on a case-by-case basis.
  - **Categories:** Racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; health or genetic data –physiological or mental health conditions and provision; biometric data – facial recognition, fingerprints, etc; sex life or sexual orientation.

12.THE CTSA SECTION 36(3) DECISION

Overview:

Alongside the management of - and provision of support to - Prevent referral subjects, one of the core objectives of CTP-Prevent is reasonable decision making under S.36(3) of the CTSA 2015. This section of the Act states that police (on behalf of the 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**."

For CTP-Prevent, the s.36(3) decision is the legal threshold decision for referral to a multi-agency panel for consideration (Channel / PMAP) and made at the culmination of the Multi-Agency Information Gathering Phase after sufficient data sharing and assessment.

Key points:

The CTSA does **not** require officers to suspect terrorism offending of planning, nor does it use "susceptible to radicalisation" as the legal threshold – this is the language used in the Prevent Duty Guidance and Channel/PMAP Duty Guidance. CTCO decisions must be expressed in the language of s.36(3): whether the subject is "vulnerable to being drawn into terrorism" - meaning **any** terrorism related offending described in UK legislation, including the non-violent terrorism offences.

Early Intervention:

The s.36 framework is designed for to enable preventative support. Officers are not expected to find the "points to prove" for terrorism offences before being deciding whether a referral meets the s.36(3) threshold. The legal test is whether the referral subject is "**vulnerable** to being drawn into terrorism", not just referral subjects who are "already being drawn into terrorism".

It is not a criminal threshold, a charging decision, a legal of fact, or a decision that the Subject has committed, planned or intended terrorism-related offending. It is simply a threshold for referral to a statutory Local Authority-led multi-agency panel so that the extent of the person's vulnerability to being drawn into terrorism can be assessed and, where appropriate, support can be considered.

This process is not without boundary: Channel/PMAP Duty Guidance is explicit that support may be provided early, but cases must not be adopted where absolutely no terrorism-connected concerns are believed to be present.

The Decision:

- Where reasonable belief is established, the case should normally progress to Information Gathering.
- Where the threshold is not met, the case must be closed to PCM.

- Any remaining non-CT safeguarding, welfare or criminality concerns must be referred or signposted to the appropriate agency or policing team.
- More serious terrorism-related concerns must be referred back through the FIMU for reassessment
- For guidance on making the s.36 decision, and for onward referrals for cases, refer to the **CONDUCTING A PRS (PAF)** and **MANAGING PRS ASSESSMENTS FOR SUPERVISORS** PCMT user-guides, and following sections of this document:
  - **THE NDM IN PCM**
  - **PREVENT REFERRAL SCREEN (PRS)**
  - **CTSA AND PRS – MAKING THE SECTION 36(3) DECISION**
  - **SIGNPOSTING AND ONWARD REFERRALS**

13.CHANNEL - CTP DUTIES

After a positive s.36(3) decision: prepare the case for Channel

- Once the s.36(3) decision has been made, if the decision was to refer the case to a Channel panel / PMAP, the CTCO must prepare the case for presentation to the panel.
- The CTCO must ensure the case file is complete, auditable and ready for panel. This should include:
  - the s.36(3) rationale;
  - a clear case summary;
  - the completed Susceptibility Assessment (SA);
  - relevant partner information;
  - safeguarding information required for safe panel decision-making;
  - any operational sensitivities or information-sharing restrictions considered;
  - proposed next steps for the panel.
- The **PRS is police-only** and must not be shared with Channel partners. The **SA is the Channel-facing assessment** and should be used to explain the Subject's susceptibilities, protective factors, risk picture and support needs. See para.107-109 of the Channel Duty Guidance 2023.
- Where the case concerns a person under live or overt CT investigation, CTCOs must follow the **PURSUE SUBJECTS OF INTEREST IN PREVENT CASE MANAGEMENT** before presenting the case. In brief: confirm the case meets RTI criteria, T2D T2D agree what can be shared, and ensure the SIO/Prevent position is settled before panel.

Chair pre-brief and panel preparation:

- The CTCO should brief the Channel Chair before the meeting to support agenda-setting, identify required attendees and ensure the right agencies are invited.
- The pre-brief must not become a decision-making forum. Adoption, support planning and closure decisions must be made by the panel.
- The Channel Duty Guidance states that the Chair should be briefed by the Channel case officer before panel to aid agenda-setting and identify attendance, but that the pre-brief must not be treated as a decision-making forum or a filter for Channel referrals. Refer to Channel Duty Guidance**, Section 4: Channel panel roles**.
- Where the case involves a live CT investigation, any pre-brief with the Chair must use the agreed form of words. If there is uncertainty about what can be shared, refer to the **SPECIAL CONSIDERATIONS IN PCM** section before any disclosure is made.

First Channel panel:

- The CTCO must attend the Channel panel and present the case clearly and proportionately.
- The CTCO presentation should cover:
  - reason for referral;
  - s.36(3) rationale;
  - assessed susceptibilities;
  - relevant risk and protective factors;
  - safeguarding and welfare context;
  - known services already involved;
  - any police concerns;
  - whether Channel appears suitable;
  - proposed next steps.
- The CTCO should support the panel to understand the terrorism-related concern, but must not take on the role of the Chair or dictate partner decisions.
- The Channel Duty Guidance confirms that the CTCO should attend every Channel panel and is responsible for escalating terrorism-related risk, transferring cases to PLP or Pursue where appropriate, and ensuring case information and the PAF are kept up to date. Refer to Channel Duty Guidance, **Section 4: The police counter-terrorism case officer and Channel co-ordinator**.
- Where the Subject is under live/overt CT investigation, a Pursue representative may need to attend in line with the **SPECIAL CONSIDERATIONS IN PCM** section. Their role should be limited and clearly understood; the CTCO retains the police position at panel.

Panel Adoption Decision:

- At the first panel, the panel must decide whether to adopt the case. The case must not be left indefinitely for informal monitoring in Information Gathering without adoption.
- The CTCO should support the panel by explaining whether the available information indicates:
  - the referral subject is vulnerable to being drawn into terrorism offending, and the risks around such offending (if any);
  - all identified susceptibilities to radicalisation;
  - whether those concerns may be reduced through Channel support.
- If adopted, the panel should agree who is best placed to seek consent and begin considering support linked to the SA.
- The Channel Duty Guidance states that the panel must decide whether or not to adopt when a referral is first presented, and that decisions must not be deferred or held for

monitoring without adoption. Refer to Channel Duty Guidance, **Section 5: The Channel panel process**.

- Where a case has not been adopted, the CTCO and Supervisor must consider whether sufficient concerns remain for management through PLP escalation to the Pursue space, or onward referral to health, social care or another appropriate agency, or closed and not progressed with. The rationale is recorded
- If a case under live CT investigation is not adopted, or if consent is not secured, CTCOs must refer to the **SPECIAL CONSIDERATIONS IN PCM** section to consider transfer to PLP and continued Prevent/Pursue governance.

Consent for Channel support:

- Consent is required before Channel support is accessed.
- Consent is not required for the police to make a s.36 referral, present the case to panel, or lawfully share information under the statutory framework.
- The panel should decide which agency is best placed to seek consent. This should not default to the CTCO unless the panel agrees that police contact is the most appropriate route.
- For under-18s, consent is normally sought from a parent, guardian or agency with parental responsibility.
- The Channel Duty Guidance states that, where adoption is agreed, the most appropriate agency should be identified to seek consent, and for under-18s the consent of a parent or guardian is required. It also states that if consent is not secured within three months, the case will need to be closed to Channel. Refer to Channel Duty Guidance, **Section 5: The Channel panel process**. The CTCO must then consider whether Prevent or other concerns remain and whether PLP, Pursue, safeguarding or signposting is required.
- For Subjects under investigation, consent must be informed and must not be compromised by the investigation. Refer to the **SPECIAL CONSIDERATIONS IN PCM** section before consent activity is undertaken.

Support Plan:

- Although best practice is to complete a support plan prior to asking the referral subject whether they consent to receive the plan, Channel Duty Guidance prefers consent for the plan to be gained before a plan has been developed.
- Once consent is secured, the panel must develop a support plan linked to the SA.
- The CTCO must assist the Chair and panel to ensure support actions address the identified susceptibilities, risks and protective factors.
- The support plan should identify:
    - the concern being addressed;
    - the intervention or action;

- the responsible agency;
- sequencing and timescales;
- review points;
- risk management arrangements;
- escalation triggers.

- The CTCO must ensure police actions are clearly recorded and achievable, and must not accept ownership of actions that properly sit with the Chair or another partner agency.
- The Channel Duty Guidance explains that the panel is collectively responsible for ensuring delivery of the overall package of support, while support providers are responsible for delivering their own elements. Refer to Channel Duty Guidance, **Section 6: Support plans / Support to address identified susceptibilities**.

Intervention Providers and specialist support:

- Where ideological, theological or fixated-thinking concerns are present, the CTCO and panel must consider whether a Home Office-approved Intervention Provider (IP) is required.
- The CTCO is responsible for arranging IP provision where the panel identifies that the Subject would benefit from an IP.
- The CTCO must complete the required IP commissioning documents, ensure the IP has enough information to work safely and effectively, and record the rationale for commissioning or not commissioning an IP.
- The Channel Duty Guidance states that IPs must be commissioned where there is a need for theological or ideological support, where there are multiple ideologies, or where ideological drivers are unclear. Refer to Channel Duty Guidance**, Section 6: Intervention Providers**.
- Where the Subject is under live/overt CT investigation, CTCOs must refer to the **SPECIAL CONSIDERATIONS IN PCM** section before commissioning an IP. In brief: T2D T2D use agreed red lines, T2D consider disclosure implications, and ensure SIO sign-off where required.
- Where mental health, neurodivergence or complex needs may affect susceptibility or risk, the CTCO should consider relevant specialist consultation, including the **CCS** where the criteria for their involvement appears to be met. Record the decision and its rationale on the PCMT.

Ongoing Channel management:

- The CTCO must attend monthly panels while the case is live, unless otherwise agreed and justified.
- Before each panel, the CTCO should:
  - review new information;

- update the SA/PAF where required;
- review police checks and intelligence;
- liaise with support providers where appropriate;
- identify changes in risk, susceptibility or protective factors;
- prepare a concise update for panel.

- During panel, the CTCO should:
  - provide the police update;
  - explain any change in risk;
  - identify any escalation concerns;
  - support review of the support plan;
  - ensure police actions are clear;
  - ensure decisions and rationales are recorded.
- After panel, the CTCO must:
  - update PCMT;
  - complete police actions;
  - submit intelligence where required;
  - update the SA/PAF;
  - ensure minutes, support plan updates and key documents are uploaded or recorded.
- The Channel Duty Guidance states that panels must be held monthly where there are referrals, live cases or cases for review, and that panel minutes must reflect confidentiality and decision-making. Refer to Channel Duty Guidance**, Section 6: Panel meetings**.
- The Channel Duty Guidance also states that the Channel case officer is responsible for regularly liaising with support providers, updating the PAF and assessing progress. Refer to Channel Duty Guidance, **Section 6: Monitoring Channel support**.

Risk escalation during Channel:

- The CTCO must keep terrorism risk under review throughout Channel.
- If risk increases, the CTCO must discuss the case with a Supervisor and consider whether the case remains suitable for Channel.
- Where terrorism risk can no longer be safely managed by Channel, the CTCO must consider escalation to PLP, Pursue or another appropriate policing mechanism.
- The Channel Duty Guidance states that police keep terrorism risk under review and that cases may be removed from Channel if risk escalates beyond what the panel can safely manage. Refer to Channel Duty Guidance, **Section 6: Risk**.
- Where the case involves a live/overt investigation, any escalation, new intelligence, IP disclosure issue, charging decision, or change in investigative status must be managed

through the **SPECIAL CONSIDERATIONS IN PCM** section and the agreed Prevent/Pursue governance route.

Information sharing, confidentiality and records:

- The CTCO must share information that is necessary, lawful and proportionate for safe and effective Channel decision-making.
- Operationally sensitive material must not simply be withheld where doing so prevents the panel from understanding the risk. The CTCO should prepare an agreed form of words where sensitive detail cannot be disclosed.
- The CTCO must ensure all panel decisions, actions, rationales, assessments and support plan updates are recorded on the PCMT.
- The Channel Duty Guidance states that disclosure requests must specify and record the purpose of disclosure, and that decisions must consider whether disclosure is lawful, necessary and proportionate. It also requires Channel partners to agree a confidentiality declaration at each meeting. Refer to **Channel Duty Guidance, Section 5: Disclosure and confidentiality**.

Transfer of Channel cases:

- Where a Subject relocates, the CTCO must work with the Chair to consider transfer to the new Channel panel.
- Transfer is not a police-only decision. The originating and receiving Chairs must confer, and the case management system must be updated.
- The CTCO must ensure the receiving area has sufficient information to understand the current risk picture, support plan and outstanding concerns.
- Note that when a Subject is in prison, that prison would usually be regarded as the place where the Subject usually resides in relation to transfer decisions.
- The Channel Duty Guidance states that where an adopted case relocates, it should be transferred to the Channel panel of the new local authority, with case management records amended and police notification made to the receiving police force area. Refer to **Channel Duty Guidance, Section 5: Transferring Channel cases**.

Case closure:

- A Channel case should remain open until one of the recognised exit points is reached:
  - terrorism susceptibility has reduced sufficiently to warrant exit;
  - terrorism risk has increased and the case is escalated to police management;
  - consent is not secured or is withdrawn;
  - support options have been exhausted or Channel is no longer appropriate.
- Before closure, the CTCO must ensure:

- the SA/PAF is updated;
- panel rationale is recorded;
- police actions are complete;
- outstanding safeguarding or non-CT needs are signposted;
- intelligence has been submitted where required;
- the correct PCMT closure status is applied.

- The Channel Duty Guidance states that where the panel decides to close a case, the person should receive notification that Channel support is ending and that mainstream support is unaffected. It also says a lead professional should be identified where mainstream support continues, so the person can be brought back to panel quickly if concerns re-emerge. Refer to Channel Duty Guidance, **Section 5: Case closure**.
- Where family has been identified as a protective factor, family communication may be appropriate. For adults, permission to liaise with family must be captured through the consent process. Family communication must not be used where family may be a radicalising influence. Refer to Channel Duty Guidance, **Section 5: Case closure**.
- Where a case under live/overt CT investigation exits Channel, refer to the **SPECIAL CONSIDERATIONS IN PCM** section. In brief, consider transfer to PLP, confirm Pursue risk ownership, record the decision and ensure Prevent/Pursue are aligned before closure from PCM.

Six and twelve-month reviews

- These must take place as per the directives on the PCMT and as described in the Six and Twelve-Month review section of this document.

CTCO Role Limits

- CTCOs are the police/CT risk specialists in Channel, not the Chair and not the owner of every support action.
- CTCOs must:
  - present police assessment and risk;
  - update and maintain the SA/PAF;
  - support lawful information sharing;
  - submit intelligence where required;
  - commission IPs where agreed;
  - keep terrorism risk under review;
  - escalate where Channel is no longer suitable;
  - ensure PCMT is complete and auditable.
- CTCOs must not:

- use Channel to progress a Pursue investigation;
- seek evidence through support activity;
- task IPs or partners to gather intelligence;
- bypass consent requirements for support;
- allow operational sensitivity to prevent the panel from receiving enough information to make safe decisions;
- leave cases drifting without adoption, closure, escalation or review.

- For live/overt investigations, officers must always check the **SPECIAL CONSIDERATIONS IN PCM** section before panel presentation, consent activity, IP commissioning, information sharing, escalation, closure or transfer to PLP.

14.POLICE LED PARTNERSHIP (PLP)

Overview:

The Police Led Partnership (PLP) process is led by CTP-Prevent and works in partnership with other agencies wherever necessary. PLP primarily manages subjects within Prevent who have met the s.36(3) CTSA threshold and require support and/or mitigation but are unsuitable for Channel/PMAP. PLP can also manage cases involving Permissive Environments, previously called Institutions and Ideologies, and will be discussed in more detail.

INDIVIDUALS IN PLP:

Channel/PMAP must always be the preferred route for all individuals within Prevent who have met the s.36 CTSA belief threshold. However, this is not always suitable, and cases can be categorised as such and recorded in the Notes (PCMT system update to follow):

T1E

CAT2 Potential compromise of a CT investigation or National Security.

T2D

CAT2 B –

Any subjects who are also under MAPPA (Level 2 or 3) supervision or any other order which prohibits them from Channel. Refer to the MAPPA section of this document for more details.

CAT 3 - Case exit from Channel/PMAP

CAT3 A –

If a case has not been adopted or where consent for the Channel/PMAP Support plan is not secured (at least within three months). The Supervisor must consider whether sufficient concerns remain for escalation to PLP or for an onward referral to health or social care.

CAT3 B –

- **Live overt CT Investigations - SOI closed by Channel Panel**

  A subject remains under a live CT investigation, but the case exits Channel/PMAP because:

  a. No consent/ consent withdrawn (to all the support plan)

  b. Objectives achieved

  c. Opportunities exhausted

The case must be transferred into PLP for a formal and documented panel meeting with the CT investigation team, including the SIO. The purpose of this panel is to explain the rationale for closure and next steps, which may mean closure from Prevent and responsibility transferred to Pursue.

This is not closure code of 'escalation to Pursue', instead 'Under CT investigation and all intervention options exhausted/considered – transferred back to Pursue' would be most appropriate in these circumstances.

Refer to **PURSUE SUBJECTS OF INTEREST IN PCM** section for details of working with Pursue

---

PLP Case Management:

All cases in CAT1, 2 or 3 must follow the **minimum standards** for case management:

- Opening and closing Susceptibility Assessment (SA), with regular reviews.
- Case Management Plan (CMP) completed and reviewed at each panel.
- Monthly PLP panel chaired by substantive Sergeant or above.
- RPC, or deputy, reviews CMP every 8 weeks and records risk management oversight and rationale for continued management in PLP and not Channel/PMAP.

Susceptibility Assessment

A case entering PLP must have a completed SA as soon as practicable, this remains even if a SA has recently been completed for Channel/PMAP and exited or not adopted.

The SA must be regularly reviewed and especially if new information emerges, where the provision of support has reached a particular milestone, or there have been significant changes to circumstances or levels of risk. It may be relevant to complete an intelligence report for FIMU assessment and update the SA to assess risks and vulnerabilities. Any escalation in risk must be raised to the FIMU as soon as practicable.

The Regional Prevent Coordinator (RPC), or their nominated deputy, must review the CMP every 8 weeks for consideration as to whether PLP continues to be the appropriate management for the subject.

Case Management Plan (CMP)

Once the initial SA is completed and based on the factors that are marked as 'present' a CMP is automatically generated and must be completed on the PCMT. The SA identifies each area of concern and allows an aligned intervention to support or disrupt the subject by CT Police and/or other agencies.

CMPs are **mandatory** for every PLP case and should direct the PLP panel agenda. It is the responsibility of the Prevent supervisor and the PLP Chair to ensure a CMP is completed.

The CMP must be monitored and reviewed at each PLP panel to ensure the plan is being implemented and is effective or needs altering.

The CMP must be updated following every PLP panel.

CMPs can include supportive or disruptive interventions by police and multi-agency partners, and the following may be useful reference and found on CT-Net:

1. Home Office: Prevent Disruptions Legislation Toolkit 2025
2. College of Policing: Menu of tactics

Please refer to the Support and Case Management Plans section of this document for more details.

Transfer from PLP to Channel/PMAP:

If a subject agrees to engage with a PLP intervention, consideration should be given to whether the case should now be presented to a Channel/PMAP Panel for continued management so the Channel/PMAP Support Package is offered (with the "PLP" intervention included) and written consent sought.

Consideration for Channel/PMAP re-presentation should be considered at each PLP panel, RPC (8 week) review and trigger points i.e. Channel Six-and Twelve-Month reviews while open in PLP.

The PLP panel must agree that Channel/PMAP is more appropriate for case management. The case can then exit PLP and be transferred to Channel/PMAP.

PLP case closure:

Refer to the Case Closure section of this document.

Signposting:

It is vital that suitable signposting/referrals to appropriate agencies is completed at case closure. As every case closure at PCM, ensure appropriate signposting occurs and see the Signposting section of this document for further detail.

Six-and Twelve-Month reviews:

Please refer to the Six-and twelve-month reviews section of this document

INSTITUTIONS / PERMISSIVE ENVIRONMENTS CASES IN PLP

Please refer to the Permissive Environments Annex of this document for details.

PLP PANELS FOR INDIVIDUALS AND INSTITUTIONS (PEs)

The following is relevant for the management of both **Individuals** and **Institutions** (Permissive Environments)

Timings and location:

- Should take place every four weeks, or an extraordinary panel if necessary.
- Panels should be scheduled in advance to ensure attendance from partner agencies.
- Can be held after a Channel/PMAP Panel if this is suitable for attendees, but it must be independent from the Channel/PMAP panel with a new chair, introductions and confidentiality agreement.
- Can be held online or in person.

Chair and attendees:

- Must be chaired by a substantive Prevent Sergeant or above. If possible, an Inspector is preferred for new oversight of the case.
- A minute taker must be appointed, where possible, this should not be the CTCO presenting the case.
- Online held PLP Panels should not be recorded by any AI software to protect Personal data under the Data Protection Act.
- **Cat 1 subjects** – attendees will usually only consist of CTP-Prevent, Pursue, T2D Police Professional Standards, other relevant Police teams T2D.
- **Cat 2 subjects** – attendees will be similar as Cat 1, and external attendees will be a case-by-case consideration. It is good practice to invite the Channel Chair.
- **Cat 3 subjects** - the Channel Chair and Prevent Lead must always be invited, and all other internal and external partners must be considered.
- External CTP-Prevent partners could include representatives from education, health, Probation, Police, P1, Charity etc. A more exhaustive list can be found on the CT-Net Police-Led Partnership page.
- Consider inviting Intelligence Partners when appropriate. This can be achieved via a regional SPOC or the CT Investigation team.

Responsibilities:

PLP Chair must ensure prior to a panel:

- A clear agenda and previous panel minutes must be sent to all attendees prior to the forthcoming panel, and,

- The initial SA and subsequent updated SA's are sent only to persons relevant to that subject, and,
- The CMP is current with interventions and activities undertaken and identifies risk which remains mitigating.

PLP Chair must ensure during the panel:

- That all attendees agree to the Confidentiality & Equality Statement
- Previous minutes are agreed
- Review previous actions
- All attendees have the opportunity to provide an update
- The CMP is reviewed with actions and activities decided and agreed.
- Reach a panel consensus on all decisions. If not possible, a panel majority, with the chair holding the casting vote where no majority exists.

PLP Chair must ensure after the panel:

- Appropriate minutes are produced and circulated promptly.
- Calendar invites for the next panel date circulated to appropriate attendees.

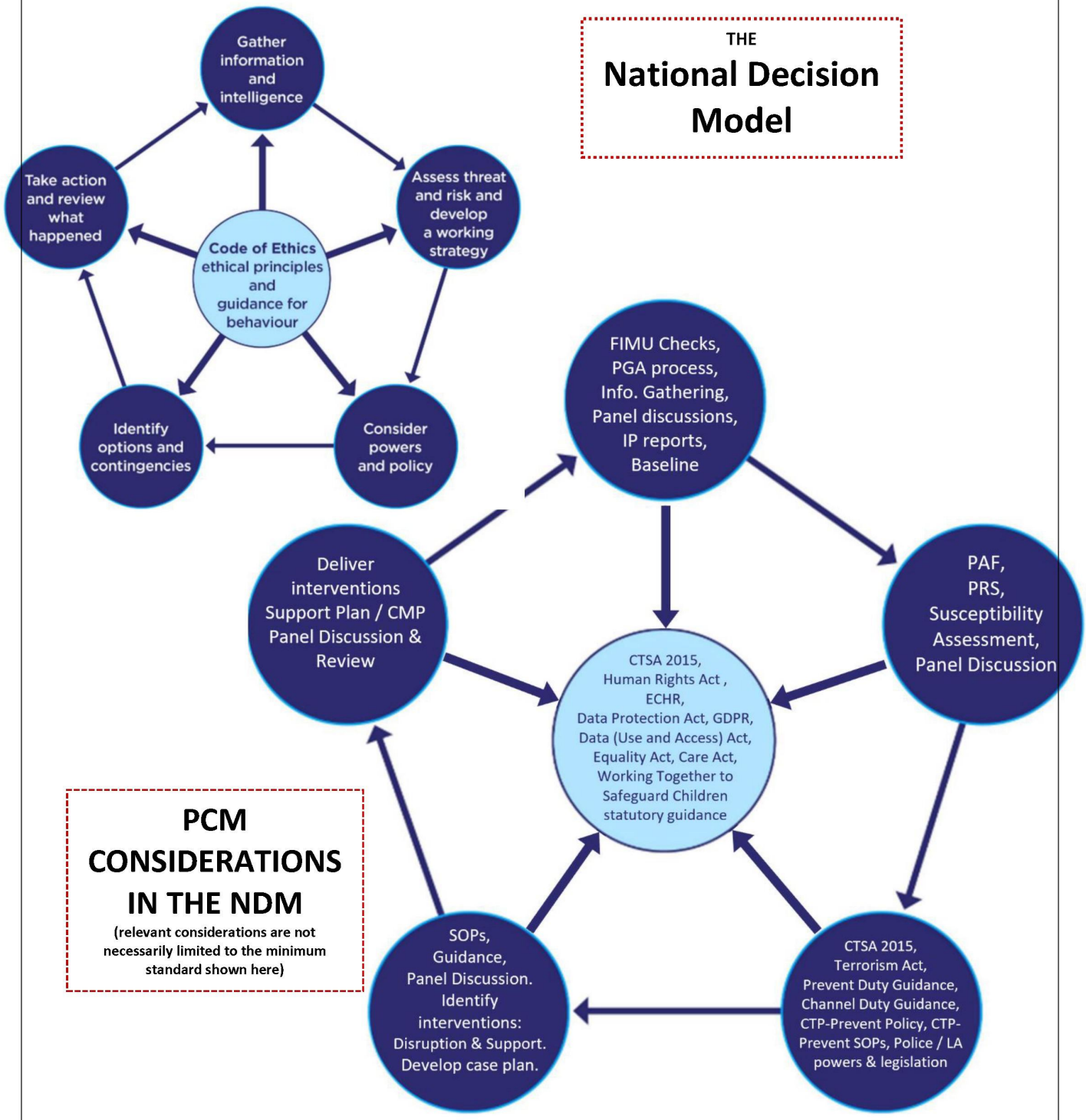
The CTCO is responsible for updating the PCM with

- Panel minutes
- CMP and SA updates
- Any other relevant detail
- Where relevant, completing intelligence reports for FIMU assessment

To help structure efficient practice for PLP panels, standardised templates are available on CT-Net including terms of reference, information-sharing agreements, agendas and confidentiality agreements.

15. THE NATIONAL DECISION MODEL (NDM) IN PCM

All decision making within PCM should use the Police NDM process.



PCM Decision Options:

A CTCO proposes a decision and the CTCO Supervisor must approve and finalise it. In all instances, CTCOs and Supervisors must use all relevant information available to them to clearly articulate what their conclusion is and how it has been reached, describing the risks, vulnerability, susceptibility or mitigations that support their belief, and documenting and using all the relevant information available to them feeding into this process.

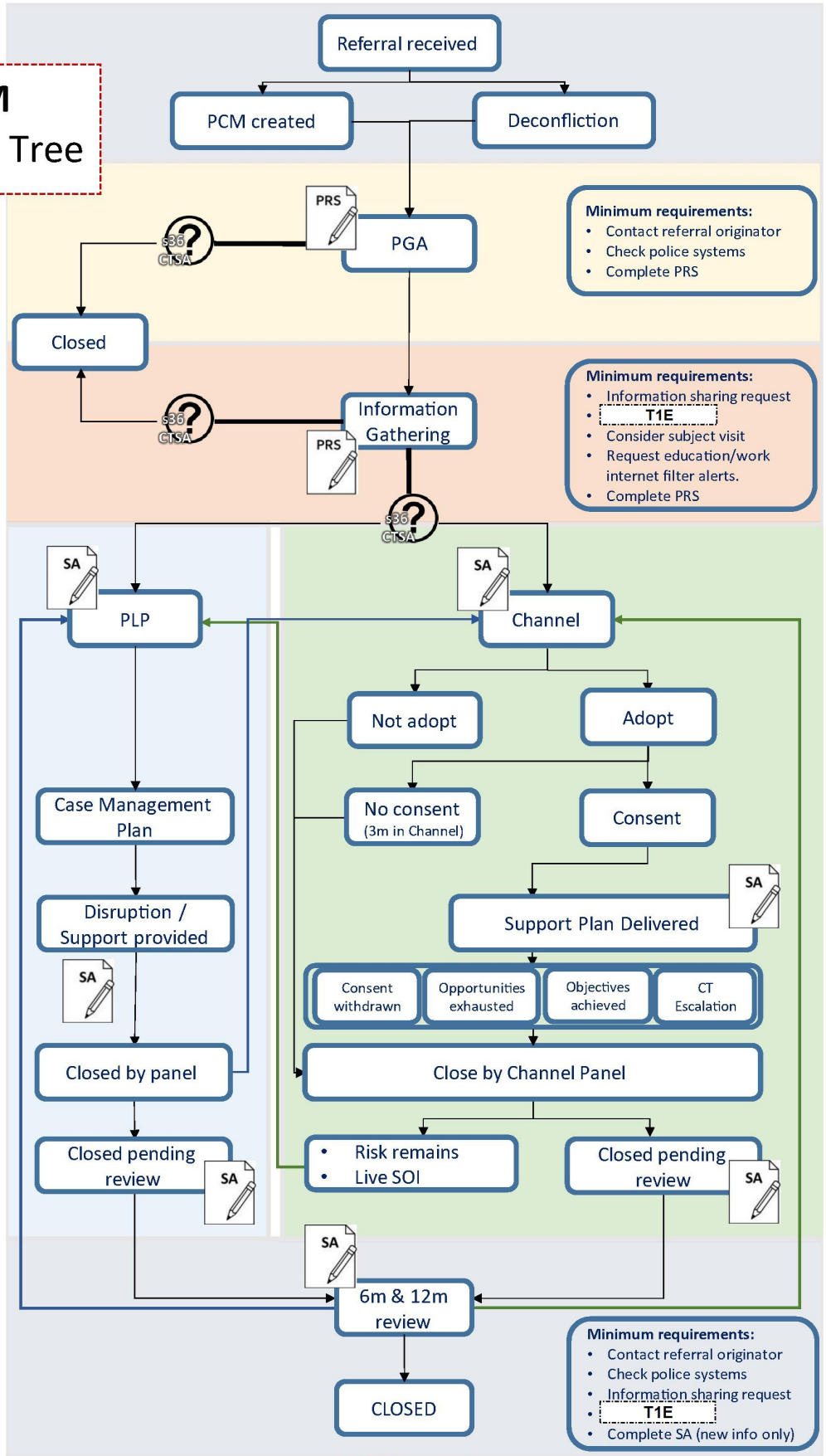
Key PCM Decisions:

At the PGA stage – a reasonable suspicion that the referral subject has "Prevent-relevant" concerns about and should therefore be moved into the Information Gathering stage for a closer examination. If the 'suspicion' standard is not met, the referral may be closed from PCM.

At the CTSA s.36(3) stage –

- **Towards Channel:** a reasonable belief that the referral subject is "vulnerable to being drawn into terrorism", and potentially suitable for management by a local authority led multi-agency panel (Channel / PMAP).
- **Towards PLP:** a reasonable belief that the referral subject is "vulnerable to being drawn into terrorism", but unsuitable for Channel and meeting the criteria for management in PLP.
- **Towards Pursue Escalation:** the referral subject appears to be **more** than simply "vulnerable to being drawn into terrorism", and the terrorism-related concerns are of a type that is inappropriate for management in PCM, and needs to be escalated out altogether, back through the FIMU for Pursue re-assessment and possibly management.
- **Towards Closure:** It is **not** reasonable to believe the referral subject is "vulnerable to being drawn into terrorism", and so the case may be closed from PCM altogether, e.g.:
    - Not Progressed With (**NPW**) at all,
    - Closed with a minor issue resolved with the Subject, or
    - Forwarded out of PCM altogether for other safeguarding or law enforcement management by another unit or agency.

PCM Decision Tree



16.PREVENT REFERRAL SCREEN (PRS)

Overview:

The PRS is built 'into' the PCMT and it is used during the **PGA** to support triaging and decision-making. It is designed to help CTCOs identify at the PGA stage whether there are genuine **Prevent-relevant concerns** attached to the referral subject and help CTCOs at s.36(3) stage identify whether it is reasonable to believe that the referral subject is vulnerable to being drawn into terrorism.

For details of how to navigate the PRS on the PCMT, CTCOs and Supervisors should refer to the **Conducting a PRS (PAF)** PCMT guidance document and Supervisors should refer to the **Managing PRS Assessments for Supervisors** PCMT guidance document. Both are available on CT-Net and through the PCMT's homepage.

Indicators and Professional Judgement:

The PRS contains **ten structured indicators** covering potential signs of engagement with extremism or terrorism, alongside contextual factors that may affect susceptibility to radicalisation, vulnerability to being drawn into terrorism offending, exploitation, capability and escalation.

Structured Professional Judgement:

The indicators must be used to structure, not replace, professional judgement. CTCOs must record supporting information against relevant indicators and provide a clear rationale for the recommended outcome. Non-starred indicators do not usually establish Prevent-relevance on their own. Factors such as isolation, mental health concerns, trauma, weapons access or criminality may become relevant where they help explain susceptibility, vulnerability, exploitation, capability, escalation or a pathway towards terrorism-related activity.

Starred Indicators:

These carry particular weight because they are most directly linked to Prevent/CT concerns. Where a starred indicator is supported by specific, credible information, this will normally generate the "reasonable suspicion" at PGA unless clearly negated by context, reliability, credibility or alternative explanation. Starred indicators also carry weight at the S.36(3) stage, but they do not necessarily provide the "reasonable belief" of a vulnerability to being drawn into terrorism – this assessment still requires the judgement and discretion of CTCOs and their Supervisors.

Mental ill health and neurodiversity:

Refer to the **CCS REFERRALS** section of this document.

Safeguarding:

The PRS also supports early identification of serious non-CT safeguarding or welfare concerns, including self-harm or suicide risk. Where Prevent is not the appropriate pathway, these concerns must be signposted or referred to the appropriate service and recorded.

Missing information:

"Known unknowns" must be recorded. Where relevant information is unavailable, the CTCO should record what is missing in the correct PCMT box, along with what steps have been taken to obtain it, and whether the absence of that information weakens, strengthens, or does not affect the PGA decision.

17.PGA AND PRS – MAKING THE GATEWAY DECISION

Overview:

At PGA stage, CTCOs must decide whether there are reasonable grounds to suspect that a Prevent-relevant concern is present. If so, the referral may be moved into the Information Gathering stage. If the standard of "reasonable suspicion" is not met, the referral may be closed from PCM.

The rationale should explain why the information interpreted through the PRS is plausibly Prevent-relevant. This may any combination of factors from the PRS, starred indicators, and the CTCO's professional judgement of a suspicion, which, providing it is 'reasonable', is enough by itself to put a referral subject through to the Information Gathering stage.

Reasonable suspicion:

This is a low but real and 'tested' threshold. It is not a standard of proof, and it is lower than both the civil standard of the "balance of probabilities" and the criminal standard of "beyond reasonable doubt".

Suspicion — subjective: the decision-maker must genuinely suspect that the relevant concern may be present. Suspicion means a state of conjecture or surmise where final proof is lacking. In practical terms, "I suspect but cannot prove".

Reasonableness — objective: the suspicion must be reasonable, meaning it must be justifiable and based on identifiable facts, information, intelligence, behaviour, referral material, or other relevant information available at the time. To be reasonable and objective, the rationale for the suspicion must:

- Explain the suspicion in plain terms, e.g. what is the specific concern; what makes the concern Prevent-relevant; and why does the information justify continued PCM assessment. Is it a specific behaviour or group of behaviours? A specific event or context? A concerning associate, contact or relationship? A concerning object or item?
- Explain the source of the suspicion and why it is source credible or reliable. It can include the referral(s), tangible evidence, professional briefings, intelligence reports, partner information and hearsay, but the CTCO/Supervisor must form their own suspicion and be able to explain the basis for it.
- Be judged by reference to the information available at the time, when the decision was made, not with hindsight. Information later turning out to be wrong does not automatically make the original suspicion unreasonable, provided the suspicion was rational and justifiable at the time.
- Be rational, justifiable, and properly recorded based on the information available at the time – but an objectively reasonable suspicion it does not mean the decision is necessarily "correct." Although we must endeavour to make 'correct' decisions, the standard is for a reasonable decision, and that is not the same as a decision that later proves to be correct.
- Be aware that it is possible that the CTCO may already have enough evidence to form a reasonable **belief** at PGA stage that the referral subject is already vulnerable to being drawn into terrorism. Even so, the PRS, information gathering, and s.36(3) processes remains the same, although may be expedited if the context seems urgent enough. Multi-agency partner information can be brought to the first Channel panel meeting, if the case is adopted.

18.CTSA AND PRS – MAKING THE SECTION 36(3) DECISION:

Overview:

When making the s.36(3) decision, CTCOs and Supervisors must decide whether there are reasonable grounds to believe that the referral subject is "vulnerable to being drawn into terrorism."

"Prevent-relevance", "susceptible to radicalisation" and similar terms may assist in the PGA triage and in professional discussion, but they are not the legal threshold for s.36(3). Where a case reaches the s.36(3) decision, the decision must be framed around whether the Subject is **vulnerable to being drawn into terrorism**.

Reasonable belief:

This is a firmer and more developed threshold than reasonable suspicion, but it is **not** a criminal charging decision, nor a legal 'finding of fact', nor a court standard of proof such as the "balance of probabilities" or "beyond reasonable doubt". In the s.36(3) CTSA context, the decision-maker must decide whether there are **reasonable grounds to believe** that the Subject is **vulnerable to being drawn into terrorism**.

Belief — subjective: the CTCO and Supervisor must genuinely believe that the statutory threshold is met. This is more than a state of conjecture or surmise. In practical terms, it is not "I suspect but cannot prove"; it is closer to "the available information now supports the conclusion that the Subject is vulnerable to being drawn into terrorism, although this is not proved to a court standard."

Reasonable grounds — objective: the belief must be reasonable, meaning it must be rational, justifiable and based on identifiable facts, information, intelligence, behaviour, referral material, partner information, professional assessment, or other relevant information available at the time. The rationale must explain, in plain terms, what information is being relied upon; why that information is credible or sufficiently reliable; how it demonstrates vulnerability; what makes the concern terrorism-linked; and what credible pathway exists by which the Subject may be drawn into terrorism. To be reasonable and objective, the rationale for the belief must:

- **Be the CTCO's and Supervisor's own formed belief.** They may rely on information from others, including referrals, partner returns, intelligence, briefings and hearsay, but they must understand and record the basis for relying on it.
- **Be explainable in plain terms,** e.g. what is the specific concern; what makes the concern terrorism-linked; how does the information demonstrate relevant 'push and pull' factors; and why it supports the conclusion that the Subject is vulnerable to being drawn into terrorism. Is it a specific behaviour or group of behaviours? A specific event or context? A concerning associate, contact or relationship? A concerning object or item? A pattern of escalation, influence, exploitation, capability or movement towards terrorism-related offending?
- **Be able to explain the source** of the belief and why it is credible or sufficiently reliable in the context. This can include the referral(s), tangible evidence, professional briefings, intelligence reports, partner information, open-source material and hearsay, but the CTCO and Supervisor must form their own belief and be able to explain the basis for it.

Where material information is missing, contested or capable of an innocent explanation, the rationale must explain why the statutory threshold is still met, or why it is not met.

- **Be judged by reference to the information available at the time** the decision was made, not with hindsight. Information later turning out to be incomplete, wrong or overtaken by events does not automatically make the original belief unreasonable, provided the belief was rational, justifiable and based on the information available to the CTCO and Supervisor at the time.
- **Be rational, justifiable, and properly recorded**. An objectively reasonable belief does not mean the decision is necessarily "correct". Although officers must endeavour to make correct decisions, the standard is for a lawful, reasonable and defensible decision, not one that later proves to be correct.

Minimum decision standard:

For the s.36(3) threshold to be met, the rationale must explain all three elements below.

1. Vulnerability

The rationale must explain how the Subject's current circumstances, characteristics, behaviour, relationships, experiences or context reduce their ability to protect themselves from being drawn into terrorism-related offending.

This may include permanent, long-term, situational or time-limited vulnerability. It may arise through grooming, coercion, exploitation, duress, influence, grievance, fixation, dependency, isolation, capability, online exposure, or other relevant factors.

Vulnerability to being drawn into terrorism does not require the Subject to be willingly, knowingly or ideologically committed to terrorism. The policy draft expressly recognises that coercive vulnerability may arise through coercion, duress or exploitation, as well as through grooming or personal adoption of extremist belief.

2. Terrorism link

The rationale must explain why the concern is terrorism-linked, rather than only a general safeguarding, welfare, criminality, public order, mental health or social-care concern.

The link may be direct or indirect, but it must be present and capable of explanation. It may include terrorist ideology, terrorist-supporting activity, terrorist material, extremist ideology reasonably linked to terrorism, coercive influence by a terrorism-linked person or network, or a plausible pathway into violent or non-violent terrorism-related offending.

Prevent is grounded in early intervention and safeguarding, and includes stopping people becoming terrorists or supporting terrorism. The Channel Duty Guidance also recognises that Prevent may involve challenging extremist and non-violent ideas where they are part of a terrorist ideology.

3. Credible pathway:

The rationale must explain how the available information indicates a credible pathway by which the Subject may be drawn into terrorism-related offending.

This does not require evidence that the Subject is already planning an offence. The pathway may relate to influence, grooming, exploitation, online radicalisation, contact with extremist

or terrorist material, increasing ideological fixation, movement towards support for terrorism, exposure to terrorist narratives, capability, escalation, attack-planning indicators, or non-violent terrorism-related offending.

The Channel Duty Guidance is clear that there is no single pathway to terrorism and no simple profile of those who become involved. Assessment must therefore be based on the available information in the individual case, not on assumptions or profile-based reasoning.

What is not enough by itself:

The following do not, by themselves, establish the s.36(3) threshold:

- mental ill-health, neurodivergence, trauma or substance misuse;
- general vulnerability, isolation, low mood, grievance or social difficulty;
- criminality without a terrorism-linked pathway;
- hateful, offensive or extremist views without a reasonable link to terrorism;
- possession of concerning material where the terrorism relevance is not explained;
- association, identity, religion, politics, ethnicity, protected characteristics or lifestyle;
- vague concern that "something is not right".

These factors may become relevant where they help explain vulnerability, exploitation, susceptibility, capability, escalation or a pathway towards terrorism-related offending. They must not be used as substitutes for the statutory threshold. The SOP and policy draft both make clear that mental ill-health, neurodivergence and other contextual factors may be relevant, but do not prove or disprove suitability for Channel or PMAP by themselves.

Relationship with the PRS and PAF:

The PRS and PAF support structured professional judgement. They do not replace the s.36(3) decision.

Starred PRS indicators may carry significant weight because they are more directly linked to Prevent or CT concerns. However, even where starred indicators are present, CTCOs and Supervisors must still explain why the full statutory threshold is met. The SOP recognises that starred indicators may generate reasonable suspicion at PGA and may carry weight at s.36(3), but they do not automatically create reasonable belief.

Recording the decision:

The s.36(3) rationale must be clear, concise and auditable. It must explain:

- what information has been relied upon;
- why that information is credible, reliable or sufficiently capable of being relied upon;
- how the information demonstrates vulnerability;
- what makes the concern terrorism-linked;

- what the credible pathway towards terrorism-related offending is;
- why the threshold is met or not met;
- any significant "known unknowns" and whether they affect the decision;
- any alternative explanation and why it does or does not change the assessment.

The decision must be made on the information available at the time. A decision is not automatically unreasonable because later information changes the risk picture, provided the original rationale was lawful, rational, proportionate, based on available information and properly recorded.

Where the threshold is not met, suggested safer wording may be:

> **"The available information does not provide reasonable grounds to believe that the Subject is vulnerable to being drawn into terrorism."**

This avoids implying that officers have proved the person is not vulnerable. It records that the statutory threshold is not met on the available information.

19.CASE CLOSURE

Overview:

- CTP-Prevent closes a case from Prevent Case Management (PCM) when ongoing Prevent management is no longer appropriate.
- Case closure must be lawful, justified, supervised and fully recorded on the PCMT.
- Closure must not be used where the case still requires active Prevent management, Channel/PMAP consideration, PLP management, Pursue escalation, or further lawful and proportionate assessment.
- CTCOs and Supervisors must choose the closure outcome that best reflects the case circumstances and record the rationale clearly on the PCMT.

General closure criteria:

- A case may be closed from PCM where one or more of the following applies:
  - the available information does not provide reasonable grounds to believe that the Subject is vulnerable to being drawn into terrorism;
  - no Prevent-relevant concern is identified;
  - the Prevent-relevant concern has been mitigated;
  - the case has been escalated to Pursue;
  - the case has been redirected to another safeguarding, welfare, public protection or law enforcement route;
  - all PCM options have been exhausted;
  - the Subject cannot be located;
  - the Subject is abroad or has left the UK;
  - the Subject is deceased;
  - another case-specific reason has been identified, justified and approved.
- Closure must be based on the available information at the time of decision. The rationale must explain why continued PCM is no longer required.

Closure roles and responsibilities:

CTCOs:

- The CTCO must lead the closure process, complete the relevant assessment updates, finalise PCMT Activities and Notes, record the closure rationale and select the correct closure outcome.
- The CTCO must ensure any required signposting, onward referral, intelligence submission, subject notification or referrer update has been completed or clearly accounted for. Refer to the **Signposting and Onward Referrals** section of this SOP for detailed requirements.

Supervisors:

- The Supervisor must quality assure and approve the closure decision.
- The Supervisor must check that PCMT is complete and accurate, the closure rationale is defensible, outstanding actions are resolved or cancelled with rationale, and any required **SPECIAL CONSIDERATIONS IN PCM** approval has been obtained.

Channel or PLP Chair:

- For panel-managed cases, the Channel/PMAP or PLP Chair must agree the closure decision through the relevant panel process.
- Where concerns remain or re-emerge, the Chair must be informed and the case must be considered under the appropriate review, re-referral or re-presentation process. Refer to the **Six-and Twelve-Month Reviews** and **Transfers / Pathway Changes** sections of this SOP for details.

Pending Closure and post-closure status:

- The correct post-closure status must be applied on the PCMT so that required review triggers are generated.
- Pre-adoption closures, including PGA and Information Gathering closures, do not require 6 or 12 month reviews and should not be placed into Pending Closure for review purposes.
- Channel-adopted cases must remain in Pending Closure, effectively dormant, until the required 12 month review process is complete. If no Prevent-related concerns are identified during the review period, the case may then be fully closed.
- PLP cases should be closed under the correct PCMT status but remain subject to required Six-and Twelve-Month reviews where applicable. Refer to the **Six-and Twelve-Month Reviews** section of this SOP.
- Where Channel closes but PLP opens, the case remains live in Prevent. It must not be placed into Pending Closure while PLP management is active. The Channel review duty still applies, but the detail should be managed under the **Six-and Twelve-Month Reviews** section.
- Where new Prevent-related concerns emerge during the review period, the case may be reopened and re-presented to the last panel, or to a more appropriate pathway. Refer to the **Six-and Twelve-Month Reviews** and **Transfers** section of this SOP.

Closure at PGA

- A case may be closed at PGA where, after completing the required PGA checks and PRS, the CTCO and Supervisor do not identify reasonable grounds to suspect that a current Prevent-relevant concern is present.

- A case must not be closed at PGA where reasonable suspicion of a Prevent-relevant concern has been identified. In those circumstances, the case should normally progress to Information Gathering, unless escalation to another route is required.
- Before closing at PGA, the CTCO must demonstrate that lawful and proportionate enquiries have been completed or considered, including referral review, relevant police checks, referrer contact where appropriate, assessment of source credibility and reliability, and completion of the PRS.
- All lines of enquiry must be documented on the PCMT. Outstanding or cancelled Activities must be closed with rationale.
- Pre-adoption closures at PGA do not trigger 6 or 12 month reviews and should not be placed into Pending Closure solely for review purposes.
- Refer to the Closure section of this document for more detail.

Subject cannot be located at PGA

- Where a referral contains insufficient contact details and the Subject cannot be located through FIMU information, police systems or lawful and proportionate PGA enquiries, the CTCO may recommend closure as **Subject Could Not Be Located**.
- The CTCO must record all enquiries completed and why further enquiries are not available, lawful or proportionate.
- The Supervisor must approve the closure rationale before the case is closed.

Closure during Information Gathering

- A case may be closed during or after Information Gathering where the available information does not provide reasonable grounds to believe that the Subject is vulnerable to being drawn into terrorism.
- Before closure, the CTCO must ensure that Information Gathering Activities have been completed, reviewed and recorded, or that any outstanding Activities have been cancelled with clear rationale.
- The PRS and relevant assessment fields must be updated to reflect the information gathered and the reason the case is not progressing to s.36(3), Channel/PMAP or PLP.
- Any remaining non-CT concerns must be addressed through the **Signposting and Onward Referrals** section of this SOP.
- Pre-adoption closures at Information Gathering do not trigger 6 or 12 month reviews and should not be placed into Pending Closure solely for review purposes.

Closure following the s.36(3) decision

- Where the s.36(3) threshold is not met, the case may be closed or redirected from PCM.

- The rationale must avoid suggesting that officers have formed a formal "negative belief". The correct formulation is that the available information does not provide reasonable grounds to believe that the Subject is vulnerable to being drawn into terrorism.
- Where the s.36(3) threshold is met, the case should not be closed simply because Channel/PMAP is difficult, consent may be uncertain, or partner engagement may be complex. The CTCO and Supervisor must consider the correct route: Channel/PMAP, PLP, Pursue escalation or another lawful pathway.

Escalation to Pursue before closure

- If, at any stage, the CTCO and Supervisor reasonably suspect that the latest information may meet the threshold for a Pursue lead or investigation, the information must be escalated through FIMU for assessment.
- If there is an immediate or serious ongoing terrorism risk, FIMU must still be informed, but urgent contact must also be made with the relevant response, intelligence or investigation team.
- Where the case is closed because it has been escalated out of PCM, the closure rationale must explain why PCM is no longer the appropriate route and what escalation action has been taken.
- The intelligence loop must be maintained throughout the PCM lifecycle. Relevant new information, T1E T1E or other intelligence, must be submitted through the appropriate intelligence route and recorded on the PCMT.

Closure from Channel or PMAP

- A Channel or PMAP case may close where:
  - the identified concerns have been addressed;
  - the panel agrees that terrorism susceptibility has reduced sufficiently;
  - adequate mainstream support is in place and Channel oversight is no longer required;
  - consent is not secured or is withdrawn;
  - support options have been exhausted;
  - Channel is no longer appropriate;
  - terrorism risk has increased beyond Channel suitability and requires police management;
  - a custodial sentence prevents Channel delivery.
- Where consent is not secured within three months, the case must close to Channel. Police must then consider whether sufficient concerns remain for PLP, Pursue escalation or onward referral to health or social care.
- Before Channel or PMAP closure, the CTCO must ensure:

- the closing SA is completed or updated;
- the panel rationale is recorded in minutes;
- police actions are complete;
- PCMT Activities and Notes are finalised;
- required signposting or onward referral is complete or accounted for;
- required intelligence submissions have been made;
- the correct PCMT closure outcome and post-closure status are applied.

- Where the panel decides to close a case, the person receiving support should be notified that Channel support is ending and that mainstream support is unaffected. Where mainstream services continue, the panel should identify a lead professional so concerns can be returned to panel quickly if they re-emerge.
- Where family has been identified as a protective factor, family communication may be appropriate. For adults, permission to liaise with family must have been captured through the consent process. Family communication must not be used where there are concerns that family may be a radicalising influence.
- Where a Channel or PMAP case involves a Subject under live or overt CT investigation, CTCOs must refer to the **SPECIAL CONSIDERATIONS IN PCM** section of this SOP before closure. Where appropriate, consider PLP or return to Pursue governance; do not treat this as automatic closure from all Prevent activity.

Closure from PLP:

- Closure from PLP means closure from Prevent and PCM. It is not the same as transfer to Channel/PMAP.
- A PLP case may close where the PLP Chair and panel agree that ongoing Prevent case management is no longer required.
- Before closure from PLP, the CTCO must ensure:
  - the CMP is updated;
  - a closing SA is completed;
  - all Activities are finalised;
  - PLP minutes record the joint decision and rationale;
  - any required signposting, intelligence submission or onward referral is complete or accounted for;
  - RPC approval is obtained where required.
- PLP may close where risk has reduced, where the SA and CMP evidence diversion, deterrence or desistance, or where the Subject is demonstrably disengaging from concerning influences.

- Where the PLP Chair and panel agree that the case should close but Prevent-related risk remains, the remaining risk must be clearly recorded and escalated for RPC approval where required by policy.
- Where a PLP case involving a live CT investigation is being handed back to Pursue, this should not automatically be recorded as **Risk Remains – CT Escalation** if it is not an escalation. Use the correct closure code and refer to the **SPECIAL CONSIDERATIONS IN PCM** section for the specific process.

Special Considerations in PCM before closure

- Some cases require enhanced approval before closure. CTCOs and Supervisors must refer to the **SPECIAL CONSIDERATIONS IN PCM** section of this document before closure where the case involves:
  - multiple referrals for the same Subject;
  - fascination with committing extreme violence or mass-casualty attacks;
  - T1E
  - live or overt Pursue investigation;
  - MAPPA or other offender management arrangements;
  - suicide risk, mental health or other complexity requiring enhanced oversight.
- Multiple referral cases and cases involving fascination with committing extreme violence or mass-casualty attacks require Prevent Inspector oversight at closure from any stage of PCM outside Channel/PMAP. All such cases must be clearly identified on the PCMT.

Contact with the Subject, Legal Guardians and Referral Originator:

- **Contacting the referral originator:** Where appropriate, CTCOs (or other suitable staff) should contact the referral originator with the case outcome.
- CTCOs should prioritise contact with the referral originator where the originator is an education establishment.
- CTCOs should advise the referral originator to re-refer if concerns continue, re-emerge, or escalate.
- Contact may be withheld where information-sharing restrictions apply, including (but not limited to):
  - T1E
  - live Pursue investigations; or
  - restrictions imposed by FIMU, T1E SIO, an operational Gold Group, or another relevant command structure.
- Where contact is withheld, CTCOs **must** record the decision and rationale on PCMT.

- **Contacting the Subject or legal guardian(s):** Where possible and appropriate, the Subject should be informed that the case is closing from PCM and told about any onward referrals or signposting, where lawful and proportionate. Where the Subject is a child or lacks capacity, legal guardians (or those with appropriate responsibility) should be informed where lawful and appropriate.
- **When NOT to contact:** The Subject or legal guardian **must not** be informed where doing so would:
  - interfere with national security;
  - compromise escalation to Pursue;
  - place any person at increased risk;
  - disrupt any other legitimate operational process; or
  - interfere with urgent child protection or safeguarding action.
- **Recording:** Any decision not to inform the Subject or legal guardian **must** be recorded on PCMT with a clear rationale.
- **Other contact considerations:** CTCOs should consider the most appropriate person or agency to conduct contact, recognising that direct contact by CTP may not assist the Subject in every case. Where CTP contact is assessed as unhelpful or counterproductive, CTCOs may request that another agency makes contact where lawful and appropriate. A contact visit may be considered where appropriate.
- **Minimum information provided:**
  - **Referral originator:** CTCOs should communicate the case outcome at an appropriate level and the instruction to re-refer if concerns continue, re-emerge, or escalate.
  - **Subject or legal guardian:** CTCOs **should** communicate:
    - that the case is closing from PCM (where appropriate);
    - any onward referrals or signposting (where lawful and proportionate); and
    - any relevant next steps that the Subject or legal guardian needs to understand.
- **Signposting:** Contacting the referral originator with the case outcome is **not**, by itself, signposting:
  - Contacting the referral originator becomes signposting **only** where the referral originator is also being asked to take responsibility for outstanding support, safeguarding, or risk-management actions.
  - Where signposting/onward referrals are required, CTCOs must follow the Signposting and Onward Referrals section of this SOP.
  - CTCOs must not treat outcome notification as a substitute for signposting/onward referrals where safeguarding, support, or risk-management actions remain outstanding.
  - Where onward action is required, CTCOs must follow the **Signposting and Onward Referrals** section of this SOP.

PCMT recording standards:

- Before closure, CTCOs must ensure:
  - the correct closure outcome is selected;
  - Activities are complete or cancelled with rationale;
  - Notes are contemporaneous and complete;
  - relevant assessments are updated;
  - the closure rationale is clear and defensible;
  - Supervisor sign-off is recorded;
  - Inspector, RPC or other enhanced approval is recorded where required;
  - required signposting or onward referral is recorded;
  - significant intelligence or enforcement matters are recorded in the relevant police systems as well as PCMT.
- The closure rationale must explain:
  - what decision has been made;
  - why continued PCM is not required;
  - what information supports the decision;
  - what risk or vulnerability remains, if any;
  - what has been done with any residual non-CT concern;
  - why the selected closure outcome is the correct one.

PCMT CLOSURE OUTCOMES:

Channel Panel Meeting Outcomes (Consideration at First Panel)

- **Open code (remain in channel)**
  - Panel accepted: sufficient concerns regarding the individual's vulnerability to being drawn into terrorism for the panel to consider support (this is 'adopted')
- **Closure code (closed from panel)**
  - Panel rejected: no concerns. Insufficient Vulnerability to be drawn into terrorism – no other non-CT concerns identified
  - Panel rejected: non-CT concerns identified. Before Support Offered. Insufficient Vulnerability to be drawn into terrorism – non-CT concerns identified and referred to relevant agency
  - Panel rejected: support services already in place. Insufficient vulnerability to be drawn into terrorism AND appropriate support provided through other service

- CT Escalation: Police have intelligence to suggest individual now comes under investigation
- Subject Deceased: Subject has passed away.

Channel Panel Meeting Outcomes (Ongoing (subsequent) Channel Panels)

- **At Panel open codes (remain in channel)**
  - Panel accepted but no support offered: sufficient concerns regarding the individual's vulnerability to being drawn into terrorism for the panel to consider support but support not accepted at this time.
  - Receiving Support: Support offered and accepted: currently receiving intervention through Channel
- **Panel Closure codes (closed from Panel)**
  - *No support offered, insufficient CT concerns – closed to panel: no concerns. Insufficient Vulnerability to be drawn into terrorism – no other non-CT concerns identified
  - *No support offered, non-CT concerns identified – closed to panel: non-CT concerns identified. Before Support Offered. Insufficient Vulnerability to be drawn into terrorism – non-CT concerns identified and referred to relevant agency
  - *No support offered, other support in place – closed to panel: support services already in place. Insufficient vulnerability to be drawn into terrorism AND appropriate support provided through other service
  - Support rejected, no consent: individual (or parent/guardian if under 18) does not consent to support offered – case referred back to police
  - Consent withdrawn during support: after support accepted individual (or parent/guardian if under 18) withdrew consent – case referred back to police
  - Objectives Sufficiently Addressed: panel closed following completion of support and individual enters review process
  - *CT Escalation: Police have intelligence to suggest individual now comes under investigation
  - *Subject Deceased: Subject has passed away
  - Supported offered - consent pending: Individual deemed suitable for support from Channel but consent to receive support has not yet been received

PLP Panel Meeting Outcomes

- **Panel Open codes (remain in PLP)**
  - Monitoring: sufficient Prevent-relevant concerns for PLP panel to manage but support cannot be offered yet due to information sharing restrictions (from

Pursue or Professional Standards Units for Police Subjects in Prevent) and no approach made to Subject or partners.

- Receiving Support: Support offered and accepted. Currently receiving supportive / safeguarding interventions through PLP voluntarily. No police disruptions required.
- Safeguarding: Support offered and rejected. IPs rejected. Wrap-around tactics employed. No police disruptions required.
- T1E

- **Panel Closure codes (closed from Panel)**
  - No support / disruption necessary - closed at panel: initial Prevent concerns resolved. Insufficient Vulnerability to be drawn into terrorism related activity – no other non-CT concerns identified.
  - *No support / disruption necessary: non-Prevent concerns identified - closed at panel: No Prevent-relevant concerns. Non-Prevent concerns identified. No Support or Disruption Offered or Necessary. Insufficient Vulnerability to be drawn into terrorism – non-Prevent concerns referred to relevant agency
  - *Subject Suitable for Channel: the case Subject has become suitable for Channel and will agree to Channel support if case adopted by Channel Panel.
  - Objectives Sufficiently Addressed: panel closed following completion of support and/or disruption, and individual enters review process.
  - CT Escalation: intelligence suggests individual may now be a Pursue lead.
  - Subject within HMPS: Subject has been sent to prison but Prevent-relevant concerns still present.
  - Subject within HMPS: Subject has been sent to prison but Prevent-relevant concerns still present.
  - Subject Abroad: Subject has gone abroad.
  - Subject could not be located: Subject could not be located.
  - *Subject Deceased: Subject has passed away.

Channel Review Panel Meeting Outcomes — Review Channel Panel Meeting - Case in Closed Pending Review Status

- **6 Month / Ad Hoc Review**
  - Remain Closed to Channel Support – awaiting next review - the subject remains not vulnerable to being drawn into terrorism
  - Remain Closed To Channel Support but evidence of other vulnerability – referred to other support process - the subject remains not vulnerable to

being drawn into terrorism but other vulnerabilities have been identified and referred to an appropriate agency

- Appropriate to reoffer support plan – re-open case into Channel - re-offering support to the individual
- Move to PLP - relates to further de-confliction checks have resulted in the police withdrawing the Subject from the process and moving the case to PLP
- Subject Deceased

- **12 Month Review**
  - Final Closure - case closed following 12 month review
  - Appropriate to reoffer support plan – re-open case into Channel - re-offering support to the individual
  - Move to PLP - relates to further de-confliction checks have resulted in the police withdrawing the Subject from the process and moving the case to PLP
  - Subject Deceased

Channel Review Panel Meeting Outcomes — Review Channel Panel Meeting - Case in PLP Status

- **6 Month / Ad Hoc Review**
  - Remain Closed to Channel Support – awaiting next review - the subject remains not vulnerable to being drawn into terrorism
  - Remain Closed To Channel Support but evidence of other vulnerability – referred to other support process - the subject remains not vulnerable to being drawn into terrorism but other vulnerabilities have been identified and referred to an appropriate agency
  - Appropriate to reoffer support plan – re-open case into Channel - re-offering support to the individual
  - Subject Deceased
- **12 Month Review**
  - Appropriate to reoffer support plan – re-open case into Channel - re-offering support to the individual
  - Final Closure – case closed following 12 month review [Only available for 12 month review]
  - Subject Deceased

PLP Review Panel Meeting Outcomes — Individual (subject) Outcomes

- **6 Month / Ad Hoc**
  - Remains Closed – awaiting next review

  - Re-open Case in to PLP
  - Refer Case into Channel (sec 36 required first)
  - Subject Deceased
- **12 Month Review**
  - Final Closure
  - Re-open Case in to PLP
  - Refer Case into Channel (sec 36 required first)
  - Subject Deceased

PLP Review Panel Meeting Outcomes — Institution and Ideology (subject) Outcomes

- **6 Month / Ad Hoc**
  - Remains Closed – awaiting next review
  - Re-open Case in to PLP
- **12 Month Review**
  - Final Closure
  - Re-open Case in to PLP

20.SPECIAL CONSIDERATIONS IN PCM

Overview:

Some Prevent referrals require enhanced attention or processes that are divergent from usual procedures. Staff must follow the relevant CTP-Prevent SOP in every such case.

Key special considerations include:

- Multiple referrals for the same Subject
- Fascination with committing extreme violence or mass-casualty attacks
- Pursue Subjects of Interest (SOIs) referred to Prevent whilst under investigation
- People in Channel becoming subject to an overt Pursue investigation
- Subjects under overt Pursue investigation entering PLP
- T2D
- Suicidal Ideation, Risk and Safeguarding
- Multi-Agency Public Protection Arrangements (MAPPA)
- T2D
- Other special considerations

21.MULTIPLE REFERRAL CASES

Overview:

Multiple Referral cases are defined as:

- Two or more Prevent referrals for the same Subject, describing different incidents or two different concerns.
- Relevant previous referrals include closed Prevent cases and new referrals while a Subject is “live” in PCMT.
- A previous referral may predate PCMT and still count as a previous referral.
- The length of time between the current and historical referral is not relevant.
- The case closure status for the previous referral does not matter.

Heightened Risk:

Multiple referrals indicate a cumulative risk factor and require enhanced scrutiny, particularly if previous referrals did not progress to Channel or PLP.

Identifying Multiple Referral Cases:

CTCOs must check the Subject’s:

- name, including variations and misspellings;
- date of birth;

- address;
- previous addresses, where known;
- enhanced PCMT search results;
- relevant police systems.

All Previous Referrals:

Any historical referral found during this process will activate the multiple-referral process. No matter how old a referral, it must be reviewed alongside the latest information. CTCOs must flag new referrals immediately when a Subject has an open or previous case. All Prevent teams must clearly record and identify multiple-referral cases on the PCMT.

Duplicate Referrals:

These are out of scope, even if they come from different sources. They are referrals for the same Subject and the exact same incident or concern as a live referral.

Duplicate referrals do not activate the multiple-referral process but must still be recorded using the Referral tab on the PCMT.

With every referral, "information source credibility and reliability" must be considered and noted on the PRS, including where missing information needs to be sourced. Discretion is permitted for cases that are deemed non-credible and unreliable, and a defensible rationale must be applied.

All other types of information received about the Subject of a live case on the PCMT are treated as intelligence, not as new referrals. CTCOs must record new intelligence on the PCMT within the relevant case file, ensure all relevant intelligence still goes to the FIMU on an intelligence report, and record the FIMU's assessment results on the PCMT using the correct drop-down categorisation.

22.FASCINATION WITH COMMITTING AN EXTREME VIOLENCE OR MASS-CASUALTY ATTACK

Overview:

Henceforth "Fascination Cases" are defined as cases where an individual does not have an identifiable terrorist/extremist ideology but evidence of a fascination in committing an extreme violence or mass casualty attack, the consequences of which may have no specific racial, religious, or political motivation.

Extremist / Terrorist Ideology:

If there is an identified link to a terrorist or extremist ideology, cause, movement, individual or group, the referral must be recorded as the identified ideology with Primary Radical Influence and/or Primary Activity selected. The Fascination element must still be recorded, although it should be treated as an aggravating factor to the ideology.

Other Ideologies:

If there is identifiable but apparently non-extremist or non-terrorist political, religious, racial or other ideological group, cause or movement that appears to be motivating the fascination with committing an extreme violence or mass casualty attack, the referral must be primarily recorded as that identified ideology with Primary Radical Influence and/or Primary Activity selected it. If there is no drop-down option for the relevant ideology, describe it in the case notes.

Themes:

These cases involve individuals, often young people, who show a strong interest in conducting extreme violence or mass-casualty attacks, without a clear ideological motive. The absence of ideology does not lower the risk. Behaviour may indicate planning, copycat intent, or violence driven by hate, online notoriety, nihilism or despair. Individuals showing this fascination, even without explicit extremist ideology, may still be suitable for PCM, including Channel, PMAP or PLP.

Relevant Fascination includes:

- school massacres;
- IEDs and bombings;
- deliberate mass-public poisonings;
- marauding shooter or knifer attacks;
- use of vehicles as mass-casualty weapons.

The risk profile increases where this fascination is present alongside an existing terrorist, extremist or hateful ideology, or appears alongside signs of attack planning.

Unpacking the Definition:

for the purposes of this SOP, the definition breaks down as follows:

- **Fascination** is the state of feeling and intense interest in something.
- **Intense interest** takes a topic to an "extreme degree", exhibiting strong feelings or seriousness. It is expressed by great enthusiasm, energy, determination or concentration. It describes captivation – an attraction that completely holds attention, whether driven by curiosity, awe, excitement or even a sense of danger. "Leakage" about any of these issues can be accidental or deliberate.
- **Extreme violence or mass-casualty attack** has no legislative definition, but for the purpose of CTP-Prevent relevance it includes the following:

In-Scope Attacks

- "School massacre" attacks.
- Random or pre-planned "spree-killer" attacks.
- Marauding Terrorist Attacks (MTAs) of any kind.
- Rampaging mass-shooter or mass-knifing attacks.
- Public bombings or other deliberately life-endangering explosions.
- Deliberate mass-poisonings, such as intentionally poisoning public drinking water or poison-gas attacks.
- Deliberate vehicle-as-weapon "ramming" attacks, whether random or targeted against a specific demographic of society.

Out-of-Scope Attacks:

For CTP-Prevent, a referral subject who appear fascinated with committing any of the following cases is unlikely to include the following:

- Murder of an individual for entirely personal reasons, e.g., personal grievance based hatred for a specific individual, domestic violence, or targeting specific bullies, where there are no political, religious, racial or other ideological motivations.
- Acquisitional murder or violence, e.g., grievous bodily harm or murder solely to enable robbery, or where the motivation is to acquire money, jewellery or other valuable items.
- Criminal inter-gang murder or violence, where the gangs concerned are not also hate-groups or identifiably extremist in nature.
- Spontaneous reactionary violence, for example people with a propensity for violence reacting violently to an incident, such as pub fights or football hooliganism, where there are no religious, political, racial or other ideological reasons.

Potentially Relevant Indicators – may include:

- Researching and collecting detailed information about terrorist attacks or other notorious mass-casualty attacks, consider:
  - detailed knowledge or persistent sharing knowledge of such attacks;
  - defending or glorifying such attacks;
  - expressing or "leaking" desires to emulate such attacks, irrespective of the reason given;
  - drawings, plans or preparatory acts for such attacks.
- Attack planning;
- Escalating violent behaviour;
- Attempting to obtain illegal weapons;
- Suicidality, particularly in relation to "death by police," "going out in a blaze of glory", or suicide bombing;
- Producing a terrorist or extremist manifesto, or a hate-manifesto calling for unlawful mass violence against any protected group.

Aggravating Fascinations:

- If an individual who seems fascinated with committing a mass-casualty attack also shows a contextually concerning interest in other forms of extreme and graphic violence, such as murder footage, beheadings, torture or gore, this further aggravates the risk and must be treated as a higher priority case.
- CTCOs must consider the person's environment, capability, access to means to offend, the period in which violence could occur, and any indicators of attack planning or escalation.

Multiple Referral and "Fascination" Enhanced Oversight Considerations

CTCO: as the officer managing the case day-to-day, the CTCO is responsible for:

- searching PCMT for previous referrals;
- reviewing previous referrals;
- identifying previous risks and vulnerabilities, resolved or otherwise;
- selecting the "Multiple Referral" tag on the PCMT case file, where relevant;
- ensuring "fascination" cases are correctly recorded on the PCMT.

For "Fascination" cases, the Primary Radical Influence may be recorded as:

- Fascination with Extreme Violence;
- Fascination with Mass-Casualty Attacks.

Where there is evidence of a Primary Activity, the following may be recorded on the PCMT:

- viewing or sharing extreme violent content;
- viewing, sharing, researching or planning mass-casualty attacks.

Supervisors are responsible for:

- reviewing referral information and confirming or changing the classification of the case before allocation to a CTCO;
- ensuring the "Multiple Referral" tag has been selected on the PCMT, where relevant;
- reviewing the CTCO's findings;
- reviewing the current referral and previous referrals;
- creating a bespoke action plan for the CTCO at PGA and Information Gathering stages;
- remaining involved in case progression through set actions, activities and decision-making.

Inspectors:

- Multiple-referral cases and Fascination cases require oversight by a Prevent Inspector at case closure from any stage of PCM outside Channel or PMAP. All cases with multiple referrals must be authorised and recorded on the PCMT for closure using the "Inspector Review" drop-down on Notes.

Multiple Referral and "Fascination" Case Considerations at PGA

- CTCOs must consider progressing Multiple Referral Cases and "fascination" cases through the PGA stage so that further enquiries can be made in the Information Gathering stage to support the s.36 CTSA decision.
- This is the recommended approach to exhaust all proportionate lines of enquiry, particularly if previous referrals did not progress past the PGA stage.
- The originator of every new referral must be contacted to discuss its detail and context, which may establish new risk, vulnerabilities and information such as social media IDs or handles.
- Comprehensive checks of police systems must be conducted and recorded using Activities on the PCMT. CTCOs must create a full picture of the referral Subject, including any family members or associates, especially any who have been previously referred to Prevent or are under Pursue investigation.
- Multiple Referral and "fascination" cases may be closed at PGA only where:
  - the referral is clearly non-credible and unreliable; or
  - CTCOs and their Supervisors can explain a high degree of confidence that the referral Subject is not vulnerable to being drawn into any terrorism-related offending.
- This must be clearly detailed in a closing rationale. Refer to the Case Closure section of this SOP.

Multiple Referral and "Fascination" Case Considerations at Information Gathering:

- The purpose of the Information Gathering stage remains the same as for any other case.
- Supervisors must set clear actions on the PCMT for the CTCO to complete, and the results must be recorded fully on the PCMT under Activities, not only within Notes or the PAF assessment pages.
- The following Activities must be considered for every case:
  - T1E
  - request that the school, college, university or employer review the Subject's internet filtering and monitoring alerts, if appropriate;
  - information sharing request to statutory partners, and further discussion with professionals already involved with the Subject wherever required, for example social workers;
  - subject visits, if at the conclusion of all gathered information it is still not possible to form a reasonable belief that the Subject is vulnerable to being drawn into terrorism.

Refer to the Subject Visits section of this SOP.

Multiple Referral and "Fascination" Case Considerations at S.36 CTSA Decision

- When assessing the risks and making a s.36 CTSA decision, CTCOs must detail all previous referrals and draw out any relevant detail.
- This decision itself remains the same. CTCOs 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".
- Where the s.36(3) threshold is not met, the rationale for that decision must be clearly recorded.
- Refer to the Decision Making sections of this document.

Multiple Referral and "Fascination" Case Considerations at Case Closure

Although all Multiple Referral and Fascination Cases must be authorised by an Inspector if closed prior to adoption by a Channel panel / PMAP, Inspector oversight is not required after closure from these local-authority led multi-agency panels – unless the case is subsequently drawn into PLP.

Regardless of whether the case closed from Channel / PMAP or PLP, the Support Plan or Case Management Plan must still demonstrate how the susceptibility factors – how the vulnerability to being drawn into terrorism – has been mitigated or, if they could not be mitigated in the context, why.

PLP cases closed as "Risk Remains" require RPC authorisation unless the case is closed because the referral Subject has been sent to prison.

Refer to the Case Closure, Signposting and Onward Referrals, and Six-and Twelve-Month Reviews sections of this SOP.

T1E

24.SUICIDE RISK AND MENTAL HEALTH

Safeguarding the individual's wellbeing is as important as preventing harm to others.

Where there is risk of self-harm or suicide, CTCOs must adopt a welfare-first approach and involve relevant healthcare professionals as soon as possible, using established multi-agency processes.

Channel and PLP panels should, wherever possible, include mental health professionals so that support plans:

- focus on stabilisation;
- provide ongoing care;
- address both safeguarding and offending risk.

In some cases, suicidal ideation can also indicate increased risk of suicide-related attacks, for example martyrdom-style attacks. Threat assessments must consider this carefully.

Duty of care is paramount. All signs of suicidal ideation must be taken seriously and followed by prompt safeguarding action, recorded on the PCMT.

Please refer to the Suicidal Ideation section of the CTP-Prevent SOP for more details.

25.MULTI-AGENCY PUBLIC PROTECTION ARRANGEMENTS (MAPPA)

MAPPA is the statutory multi-agency framework used to assess and manage the risk posed by eligible sexual, violent and terrorism or terrorism-risk offenders. It is a set of arrangements, not a standalone body, through which agencies coordinate risk management using MAPPA categories, including Category 4: terrorism or terrorism risk, and management levels: Level 1 single agency; Level 2 multi-agency; Level 3 enhanced multi-agency.

For detailed criteria, governance and thresholds, refer to the MAPPA section of the CTP-Prevent SOP.

In CTP-Prevent, a discretionary referral to Category 4 MAPPA may be appropriate where:

a) terrorism-related risk is exceptional or escalating;

b) effective multi-agency controls are required and non-statutory pathways, for example PLP, are insufficient; or

c) the Subject is already managed under MAPPA for another matter, or has committed serious offending in the UK or abroad that would meet MAPPA criteria but is not currently MAPPA managed.

This should only be considered after the CTCO has assessed the person as "vulnerable to being drawn into terrorism" under s.36(3) CTSA and CTP-Prevent judges that Category 4 is the most appropriate forum to manage both radicalisation risk and wider public protection concerns. The decision must be set out in writing, with a clear rationale.

Where a Category 4 referral is made, CTCOs should consult local CTNM, submit the required MAPPA referral paperwork, and ensure all actions and rationale are recorded on the PCMT.

If a Subject is accepted into Category 4, CTCOs must record decisions on the PCMT, open or update ViSOR, and close the Prevent record in line with local process, including the relevant PCMT closure outcome code.

If a Subject is not accepted and CT concerns remain, management continues via Channel, where consent and eligibility allow, or PLP, where Channel is not appropriate or consent is absent.

Where a Subject is managed at MAPPA Level 2 or 3, Channel should not run in parallel to avoid duplication. CTCOs should liaise with CTNM and MAPPA leads, attend where appropriate, and summarise MAPPA developments within PCMT.

Pathfinder/HMPPS related scenarios, including custody and post-release, must be managed in accordance with the MAPPA section of the CTP-Prevent SOP, including required notifications when custody or probation management is identified.

T2D

27.OTHER SPECIAL CONSIDERATIONS

The above list is not exhaustive, e.g., consider CCS where the criteria for their involvement appear to be met. Refer to the Clinical Consultancy Service section of this SOP for details.

Other specialist scenarios, for example complex cases involving very young children or returnees from conflict zones, are covered in national guidance and the CTP-Prevent SOP.

Prevent officers must consult Supervisors and national policy leads where cases have unusual features to ensure that they adopt the correct approach.

28.SIGNPOSTING AND ONWARD REFERRALS

Overview:

- Signposting and onward referral must be completed where a case is exiting PCM and there are outstanding non-CT safeguarding, welfare, criminality, public protection or support needs.
- Signposting is not the same as contacting the referral originator with the case outcome.
- Signposting is not the same as exiting a case from PCM as a Pursue escalation through the FIMU.
- Signposting concerns further support, safeguarding, investigation or risk management outside of Prevent's processes.
- CTCOs and Supervisors must ensure that any outstanding needs are directed to the appropriate agency, unit or policing team before the case is closed on the PCMT.

When signposting is required:

- Signposting must be considered in every case exiting PCM, particularly at PGA and Information Gathering stages, i.e. if the case has not been managed.
- Signposting is required where:
    - Prevent is not the appropriate pathway, but other safeguarding or welfare needs remain;
    - non-CT criminality or public protection concerns have been identified;
    - self-harm or suicide concerns are present;
    - the Subject or family requires support from another agency;
    - another unit, team or agency is better placed to manage the remaining concern.
- Urgent safeguarding concerns identified at any point in the case must be referred at the earliest opportunity and must not wait until closure.

Safeguarding and welfare concerns:

- Where safeguarding, welfare or vulnerability concerns remain, CTCOs must refer or signpost the matter to the relevant agency or team outside Prevent.
- This may include, but is not limited to:
    - adult social care;
    - housing services;
    - children's services;
    - other policing teams;
    - mental health services;
    - education safeguarding leads;

- Child and Adolescent Mental Health Services (CAMHS);
- other relevant statutory or support services.

- Where possible, signposting should be made to a named professional or clearly identified team, although a team 'inbox' is sufficient where there is no named individuals.
- If urgent non-Prevent safeguarding concerns were included in the FIMU handover but do not appear to have been actioned, CTCOs should raise this with FIMU or refer the matter to the appropriate safeguarding route directly, depending on urgency and local process.

Suicidality and self-harm:

- Concerns relating to suicidality or self-harm must be treated as a priority. Refer to the SUICIDAL IDEATION, RISK AND SAFEGUARDING section of this document.
- CTCOs must consider signposting to the appropriate service, which may include:
  - CAMHS;
  - local frontline policing;
  - adult mental health services;
  - mental health crisis services;
  - ambulance or emergency services – if immediate risk is present.
- The action taken, receiving agency and rationale must be recorded on the PCMT.

Non-CT criminality and harm:

- Where non-CT criminality or risk of harm is identified, CTCOs must ensure the information is shared with the appropriate police / law enforcement unit, statutory service or local referral route.
- This includes information indicating that the Subject or another person has:
  - planned, threatened or committed any offence;
  - planned, threatened or committed unlawful violence;
  - planned, threatened or committed hate-based offences;
  - committed, disclosed or presented risk of sexual offending;
  - unlawfully possessed, downloaded or distributed illegal images or films;
  - possessed, downloaded or shared material involving extreme violence or animal cruelty.
- Where appropriate, information must be submitted through intelligence reporting routes or referred to a named policing team or public service.
- The referral must include a clear indication of the concern, risk and any suggested areas requiring attention.

Information to include in signposting:

- Signposting or onward referral must include enough information for the receiving agency to understand and act on the concern.
- The referral should include:
  - the nature of the concern;
  - the identified risk or vulnerability;
  - any urgency;
  - relevant context;
  - suggested actions or areas requiring attention;
  - the agency, team or named professional receiving the referral;
  - any limitations on information sharing.
- CTCOs must not share excessive or irrelevant information. Information sharing must remain lawful, necessary and proportionate.

Consent and non-state third parties:

- Consent may be required before sharing personal data with a non-State third party, such as a charity, voluntary organisation or community support provider.
- Where consent is required, CTCOs must obtain and record it before sharing personal data.
- Where information is shared without consent, the legal gateway and rationale must be recorded on the PCMT. Refer to the INFORMATION AND DATA SHARING IN PCM section of this document.

Recording requirements:

- All signposting and onward referrals must be recorded on the PCMT as a Signposting Activity.
- The record must include:
  - the reason for signposting;
  - the concern or risk identified;
  - the agency, unit, team or named professional contacted;
  - the information shared;
  - any consent obtained or legal gateway relied upon;
  - the date and method of referral;
  - any response or agreed action;
  - any decision not to signpost and the rationale.

- Cases must not be closed from PCM until required signposting, onward referral, intelligence submission or safeguarding escalation has been completed or clearly accounted for.

T2D -

International travel data can be provided, that can support policing in relation to national security, serious crime, safeguarding and other policing purposes. Relevant factors may include:

- expressed intent or plans to travel for extremist or terrorism-related purposes;
- travel to or through a country, region or route relevant to the Prevent concern;
- travel to areas where unlawful contact with terrorists or proscribed organisations is a realistic concern;
- in juvenile cases, indications that family members or associates may be planning to take the child abroad;
- any other factor suggesting a propensity to travel for extremist or terrorism-related purposes. Where the information suggests the Subject may already be involved in terrorism-related offending, the case must be escalated through FIMU for Pursue assessment rather than treated solely as a Prevent travel-risk matter.

T2D

T2D

T2D -

International travel data can be provided, that can support policing in relation to national security, serious crime, safeguarding and other policing purposes. Relevant factors may include:

- expressed intent or plans to travel for extremist or terrorism-related purposes;
- travel to or through a country, region or route relevant to the Prevent concern;
- travel to areas where unlawful contact with terrorists or proscribed organisations is a realistic concern;
- in juvenile cases, indications that family members or associates may be planning to take the child abroad;
- any other factor suggesting a propensity to travel for extremist or terrorism-related purposes. Where the information suggests the Subject may already be involved in terrorism-related offending, the case must be escalated through FIMU for Pursue assessment rather than treated solely as a Prevent travel-risk matter.

T2D

T2D

T2D

31.ASYLUM, IMMIGRATION, AND TRAVEL CHECKS

Overview:

- For foreign nationals, recent immigrants, asylum seekers, UK citizens returning after long or suspicious periods abroad, consider international checks to identify risks and relevant intelligence, that may result in a new Prevent referral or for a previous case to be reopened. All actions undertaken must be recorded on the PCMT.

Initial Considerations:

- For foreign nationals or recent immigrants to the UK, the CTCO and Prevent Supervisor must consider contacting the Foreign, Commonwealth & Development Office (FCDO), the Criminal Records Office (CRO), and Immigration Services to establish whether the subject:
  - is under investigation or wanted for any offences abroad;
  - has potentially Prevent-relevant overseas convictions T2D;
  - is known in any intelligence relating to Prevent concerning activities abroad;
  - has any immigration history and what their current immigration status is T2D T2D.

T2D

PCMT Requirements: Activities must be used in the PCMT to document immigration checks.

- Activity type: Police Checks , Activity: immigration'.
- Log actions taken in Activity description box.
- Document the outcomes in the Activity Outcome box.
- The PCMT step-by-step user guide for Activities is available at Creating and Managing Activities

---

Closure at PGA Stage with Outstanding ACRO Checks:

- Keep the case open whilst awaiting ACRO results, although complete a local risk assessment if the wait stretches on too long.
- If the case has been closed, you may reopen it if there is a positive ACRO return. Whatever the scenario, the case history must be clearly documented on the PCMT.

32.SUICIDAL IDEATION, RISK AND SAFEGUARDING

Overview:

- On identification of suicide, self-harm or broader suicidality risk, practitioners must act immediately and proportionately, recording all risks, decisions and interventions contemporaneously in PCMT.

  Suicidality should be understood both as an individual safeguarding issue and as a potential indicator of increased vulnerability to extremist influence or escalation in terrorism risk. All actions including supervisory notifications, clinical referrals, welfare considerations, and ongoing reassessment must be logged with clear rationale.

  Further guidance can be found on the **Suicide Prevention Guidance for Counter Terrorism Prevent staff** document on CT-Net.

Immediate Risk Actions:

- Where there is imminent concern for the subject's safety, practitioners must:
  - Follow local mental health crisis procedures - ambulance or emergency services, where immediate risk is present.
  - Ensure the subject is urgently assessed by a medical professional.
  - If necessary, consider use of police powers:
    - Section 136 Mental Health Act 1983
    - Section 46 Children Act 1989

Required CTCO Actions:

When suicide or high-risk self-harm concerns are identified, practitioners must:

- Concerns relating to suicidality or self-harm must be treated as a priority. Notify a Prevent Supervisor immediately.
- Contact any relevant key workers or medical professionals involved in the subject's care.
- Consider urgent referral or signposting to the appropriate service, such as CAMHS;
- Consider the **CCS** where the criteria for their involvement appears to be met.
- Consider any changes to risks the terrorism offending risk that may be linked to the subject's suicidal ideation.
- Submit an intelligence report to inform other relevant policing units of safeguarding risks, should there be any incidents reported about the referral subject, be they missing person reports or any other safety concerns.
- Ensure clear agency responsibility is agreed and documented on the PCMT.

Further Considerations:

- Providing support resources/toolkits to the subject and family.
- T1E

Other Considerations:

- Placing a high-priority response marker on the call-handling/dispatch system.
- Appointing a lead officer for follow-up welfare checks.
- Convening an urgent Channel Panel or PLP (post S36 cases).

Lower-Risk Self-Harm and Historical Suicidal Ideation:

- Record historic or "very low-risk" suicidal ideation to inform cumulative risk assessment, support defensibility, and guide multi-agency safeguarding in Prevent case management. For lower-risk presentations:
- Use professional judgement to determine which (if any) of the actions listed for 'Suicide or High-Risk Self-Harm' should be applied.
- Record and assess all historical suicidal ideation in context with the subject's current presentation.
- Determine actions that are proportionate and justified based on current risk, not solely history.

Recording Suicidal Ideation and risk in PCMT:

- Using the PCMT's suicidality tools keeps information organised, visible, and consistent, preventing key details from being lost in free-text notes. These structured fields make risks and actions clearer for anyone managing or reviewing the case. All decisions, including decisions not to act, must be recorded in PCMT with a clear rationale.

How to Create a Suicide Management Activity:

- Create a new Activity.
- Select **Suicide Management** for both *Activity Type* and *Activity*.
- In the Activity Description, record:
- How the risk was identified
- Actions taken
- Rationale for decisions
- Any changes in presentation
- Interventions, referrals, and signposting

- Relevant contextual factors (e.g., family concerns, mental health involvement)
- Set the Start Date to the date the suicide risk was first identified.
- Use the **Notes** section for all ongoing updates; entries must be clear and searchable.
- Keep the Activity open for the duration of the Prevent case and close only at case conclusion.

Record Suicide Risk in Mental Health Needs:

- Go to **Subject Details**.
- Add **Suicide Risk** under Mental Health Needs.
- Enter a concise outline of the concern.
- Refer to the Suicide Management Activity for full details.
- Example: *"Subject disclosed intent to end life. See Suicide Management Activity for all updates."*

Add a Suicide Tag:

- Open the **Tag** section in Subject Details.
- Select **Add Tag**.
- Choose **Suicide**.
- Confirm the tag appears in the left-hand column.

Additional Recording Requirements:

- Record all signposting undertaken.
- Document interventions within a **Support Plan** or **Case Management Plan (PLP)**.
- Update the SA with significant change at any time during case management.

Review Requirements:

- Suicide risk in Prevent is dynamic and must be reconsidered during the lifetime of a case. Practitioners must complete proportionate risk reviews at defined triggers:
  - IP sessions,
  - arrest or charge,
  - after a subject visit,
  - and any significant behavioural or circumstantial change.
  - Each review must update the risk judgement and rationale, record decisions and any actions in PCMT, set a next review date, and escalate via safeguarding

pathways if risk increases. Do not delay reassessment pending meetings or case milestones, act on new information immediately.

T2D

T2D

T2D

T2D

ANNEX 1 - PERMISSIVE ENVIRONMENTS / INSTITUTIONS

Overview:

"Institutions" cases are now described in the Prevent Duty Guidance 2023 and CTP recognises Permissive Environments. These are is in scope for CTP-Prevent, as we are expected under the Prevent Duty Guidance to help reduce permissive environments. The Duty Guidance (paras.81-81) connects permissive environments directly with radicalisation:

- "Radicalisers create and take advantage of permissive environments to promote or condone violence and to spread poisonous ideologies that undermine our values and society."

The Home Office characterises "permissive environments" as being:

- "[…] tolerant of behaviour or practices strongly disapproved of by others, such as an environment where radicalising ideologies are permitted to flourish. Radicalisers create and take advantage of permissive environments to promote or condone violence and to spread harmful ideologies that undermine our values and society. Permissive environments can exist both online and offline. Permissive online environments can contribute to online radicalisation."

For the purposes of the CTP-Prevent SOP "permissive environments" are:

- Environments that perpetuate extremist ideologies linked to terrorism, radicalise, or draw people into participating in or supporting terrorism.

Referral receipt:

Intelligence about a Permissive Environment requires FIMU deconfliction before a PCM case is created and before enquiries begin.

CTCOs must not begin Prevent enquiries until deconfliction is complete, unless authorised through the relevant deconfliction process.

PGA for Permissive Environments:

At PGA, CTCOs must complete initial enquiries. These should include:

- contact with the original referrer;
- review and assessment of all relevant police systems;
- informing the Local Authority Prevent Lead of the information received;
- completion of the PRS, using the most appropriate boxes available to outline the key information.

The threshold for Information Gathering is suspicion that the environment could perpetuate extremist ideologies linked to terrorism, radicalise, or draw people into participating in or supporting terrorism.

If the case does not meet this threshold, CTCOs must inform the Local Authority Prevent Lead and close the case, considering whether any agency may benefit from receiving the information.

If the CTCO suspects that the Permissive Environment does meet this threshold, the case should progress to Information Gathering before a decision is made on whether it should be retained in PLP.

Information Gathering for Permissive Environments:

The purpose of Information Gathering is to conduct further enquiries to understand the Permissive Environment and assess whether CTP is the most appropriate lead agency, or whether the Local Authority Prevent Lead should maintain responsibility.

Suggested enquiries include:

- research on police systems for any individuals involved or associated with the Permissive Environment;
- T1E
- assessment of whether an individual Prevent referral would be appropriate;
- attendance at a Local Authority Prevent Lead panel or meeting with relevant agencies, if convened;
- contact with relevant agencies, T1E where appropriate.

New information must be assessed through the intelligence cycle.

Any enquiries must be for the purpose of identifying criminal offences, Prevent risk, safeguarding concerns, disruption opportunities, or relevant associated individuals.

T2D

Local Authority management:

Where CTP is not the appropriate lead agency, responsibility for managing the Permissive Environment remains with the Local Authority Prevent Lead.

The Local Authority Prevent Lead is responsible for arranging a panel or meeting with relevant agencies and partners to assess and mitigate the risk posed.

CTP should continue to attend relevant meetings and comply with its statutory duty to reduce the threat posed by Permissive Environments, in coordination with local policing.

Refer to the Prevent Duty Guidance and Prevent Duty Toolkit for Local Authorities for further detail.

T2D

CTP-Prevent Case Management of Permissive Environments / Institutions:

If a Permissive Environment case is suitable for PLP management, the minimum standards are the same as for an individual PLP case:

- opening and closing Susceptibility Assessment, with regular reviews depending on case circumstances;
- Case Management Plan completed and reviewed at each panel;
- monthly PLP panel chaired by a substantive Sergeant or above;
- Local Authority Prevent Lead invited to every panel;
- RPC, or nominated deputy, review of the Case Management Plan every eight weeks;
- recorded risk management oversight and rationale for not transferring the case to Local Authority lead.

Case Management:

It is noted by CTPHQ that the PCMT and PAF are not designed to assess and manage PEs and that CTP-Prevent need to make best use of the principles and framework of PCM. As always, consider the College of Policing Rick Principles and NDM model and refer to the Case Management Plans section of this document.

PGA:

Complete initial enquiries:

- Contact original referrer
- Review and assess all police systems
- Inform LA Prevent lead of information received
- Complete the PRS to outline the key information in the most appropriate boxes available.[3]

The threshold for Information Gathering is your suspicion that the environment could *perpetuate extremist ideologies linked to terrorism; or radicalise; or draw people into participating in, or supporting, terrorism.*

If the case does not pass this threshold, then inform the LA Prevent Lead and close with consideration for any agencies who may benefit from sharing this information.

If you suspect that the PE does meet this threshold, aligned with current PCMT processes a further stage of information gathering should be completed before a decision is made to retain in PLP.

---

[3] CTPHQ acknowledge this is not an assessment tool suitable for PE, and this is under review for improvement. Until then, the PRS will be completed with the indicators applied with discretion and consideration to the case being managed.

Information Gathering:

The purpose of this stage is to conduct further enquiries to fully understand the PE and assess if CTP are the most appropriate lead agency, or if the LA Prevent Lead should maintain responsibility.

Suggested enquiries to be completed:

- Research on police systems any 'individuals' involved or associated with PE.
  - New information must be assessed through the intelligence cycle
  - Consider if a Prevent referral would be appropriate
- T1E
- Attend a LA Prevent Lead panel/meeting with relevant agencies (if convened)
- Complete the PRS to outline the key information in the most appropriate boxes available.[4]

There may be other enquiries to assist with information gathering T1E T1E - from relevant agencies, but it must always be for the purpose of identifying criminal offences and disruption opportunities T1E.

PLP threshold:

There is no legal threshold for PE as there are for Individuals (s36(3) CTSA). For a PE case to be managed in PLP, it must be assessed that the prominent tactic utilised will be criminal disruptions and CTP must lead to preserve the integrity of the investigation.

If criminal investigation or disruption is not the main tactic but could be utilised in a minor way alongside other disruption activities, this case should be closed and referred to the Local Authority.

Local Authority management:

The responsibility for the PE remains with the LA Prevent Lead to arrange a panel/meeting with relevant agencies and partners to assess and mitigate the risk posed. CTP will continue to attend meetings and adhere to our statutory duty to reduce PE, this will also be conducted in coordination with local policing.

For more information see the Prevent duty guidance: Local authority toolkit s.7.

Disruption options:

Activities to disrupt a PE is likely to conflict with Art 8, Art 10 and Art 1 (which protect privacy and freedom of speech and association). Therefore, reducing the PE should be necessary, proportionate and lawful. Any intervention should be appropriate for the setting. CTP

[4] CTPHQ acknowledge this is not an assessment tool suitable for PE, and this is under review for improvement. Until then, the PRS will be completed with the indicators applied with discretion and consideration to the case being managed.

Prevent should consider the below documents which, are not exhaustive, are useful guides to review when considering tactical options:

- Home Office: Prevent Disruptions Legislation Toolkit 2025
- College of Policing: Menu of Tactics

Home Office Prevent Disruptions Team:

Use existing mechanisms to analyse, prevent and disrupt the spread of high-harm radicalising ideologies that can lead to community division and to radicalisation into terrorism, particularly those who perpetuate radicalising ideologies linked to terrorism but who operate, often intentionally, below terrorism thresholds.

If advice or support is required in relation to a PE, CTP or the Local Authority can contact the team T1E

ANNEX 2 - CLINICAL CONSULTANCY SERVICE (CCS)

The CCS provides specialist advice, guidance and options to help manage mental ill-health and neurodivergence needs where these are relevant to Prevent Case Management.

A referral to CCS **must be considered** where there is relevant CT risk and indicators of mental ill-health or neurodivergence, evidenced through one or more of the following:

- formal diagnosis;
- behaviour observed by the CTCO;
- information gathered from partners;
- admission by the subject or a family member.

CCS referrals will usually be made after a positive s.36(3) decision has been recorded and the case is being progressed to Channel, PMAP or PLP.

Cases at PGA or Information Gathering may still be referred to CCS where additional CT risk is evidenced and a s.36(3) decision for presentation to Channel, PMAP or PLP is expected.

CTCOs should submit referrals using the **CCS link** on CT-Net and record the referral, rationale and any advice received on the PCMT.

Mental ill-health, neurodivergence, trauma and substance misuse in PCM:

These must not be treated as Prevent-relevant concerns by themselves. They are contextual factors that may or may not be relevant to a person's vulnerability to being drawn into terrorism.

They may become relevant where they exacerbate relevant susceptibility, risk of exploitation, grievance, fixation, judgement, capability, engagement with extremist material, or risk of harm, or where they aggravate an existing Prevent-relevant concern. The presence of mental ill-health or neurodivergence does not prove or disprove suitability for Channel or PMAP, and decisions must be based on the s.36(3) CTSA threshold rather than diagnosis alone. Also, where Prevent-relevant concerns **are** present, they must not be dismissed solely because they appear connected to mental ill-health or neurodivergence.

Where vulnerability to being drawn into terrorism is identified alongside mental ill-health, neurodevelopmental complexity, trauma or substance misuse, CTCOs should consider whether closer multi-agency review, clinical consultation, safeguarding action or health referral is required.

ANNEX 3 - SUBJECT VISITS

Purpose and general principles:

- Subject visits may take place at different points of PCM, but must always be lawful, necessary, proportionate, risk assessed, supervised and clearly recorded on the PCMT.
- CTCOs must consider the potential impact of direct CTP contact before any visit. Early contact may affect engagement, increase anxiety or paranoia, create a flight risk, damage public confidence where a referral is later found to be unfounded or malicious, or interfere with Pursue activity if the matter has not been deconflicted.
- Visits must not be used as routine information-gathering activity where the same information can be obtained by less intrusive, lawful and proportionate means.
- Where early information is essential, CTCOs should consider whether a partner agency with an existing relationship or rapport with the Subject can obtain the information more appropriately.
- CTCOs must not seek consent for a Channel Support Plan before a case has been adopted by a panel and a support plan / case management plan has been developed. Consent relates to the support plan if the case is adopted by Channel / PMAP; it is not required to make the s.36(3) referral decision.

Visits before FIMU deconfliction

- CTCOs must not contact or visit the Subject before FIMU has confirmed that deconfliction is complete.
- CTCOs must avoid all direct and indirect contact with the Subject during this stage to avoid jeopardising any Pursue activity or other operational requirement.
- CTCOs should respond to FIMU clarification requests using available information only, without engaging the Subject.
- Urgent safeguarding or non-CT criminal risks, including child protection concerns or suicide risk, must be escalated immediately to the appropriate agency or policing team.
- Any urgent welfare visit or non-CT safeguarding visit required before deconfliction must be carried out by the appropriate safeguarding partner or policing team, not by CTP-Prevent as a Prevent visit.
- Any visit carried out before deconfliction must not be treated or recorded as a Prevent visit, as the Prevent/Pursue pathway has not yet been determined.

Visits during PGA

- CTCOs should normally complete PGA checks and the PRS without visiting the Subject.
- Once reasonable suspicion of a Prevent-relevant concern has been identified, further probing is not required at the PGA stage, unless there is a clear and exceptional operational necessity.

- A visit during PGA may only be considered where essential information cannot be obtained by any other lawful and proportionate means.
- Channel must not be discussed with the Subject at PGA. Premature discussion of Channel or consent may complicate later s.36(3) decision-making, undermine panel engagement, or lead to refusal before the case has been properly assessed.
- Where the Subject is a child and their legal guardians are already aware of the referral and supportive of engagement, a visit during PGA may be more appropriate and justifiable. The same approval and recording requirements still apply.
- Any proposed PGA visit must be discussed with a CTCO Supervisor before contact is made.
- The Supervisor must ensure that the rationale, operational necessity, intended outcome and proportionality of the visit are recorded in full on the PCMT before endorsing the visit.
- The visit must not proceed until the decision and visit details are confirmed on the PCMT.

Visits during Information Gathering

- Visiting the Subject during the Information Gathering phase is not prohibited but must be decided on a case-by-case basis.
- A Subject visit should be considered prior to making a s.36(3) decision where, **after** all other gathered information has been reviewed and assessed, it remains unclear whether there are reasonable grounds to believe that the Subject is vulnerable to being drawn into terrorism.
- Any visit during Information Gathering must have a clear purpose, such as clarifying key risk, vulnerability, safeguarding, capability, access, influence, exploitation or pathway concerns that cannot be resolved otherwise.
- CTCOs must consider asking the Subject or their legal guardian for access to review relevant devices, including phones or computers, where this is necessary and proportionate to assess relevant risk.
- Consent for a Channel Support Plan must not be sought during Information Gathering.
- Where a visit is undertaken in relation to a child, it is not sufficient to meet only with a legal guardian. The Subject must also be seen in person unless there is a clear, recorded reason why this is not possible or appropriate. Subjects should be visited at their homes wherever it is safe and possible to do so.
- A pre-visit risk assessment must be completed and recorded before any visit. CTCOs are recommended to use the Prevent Subject Engagement Risk Assessment, available on CT-Net.

Visits after a s.36(3) decision and before the first Channel, PMAP or PLP panel

- Where contact with the Subject is being considered after a s.36(3) decision but before the first Channel, PMAP or PLP panel, CTCOs must discuss the matter with a Supervisor.
- The Supervisor may consult the Channel or PMAP Chair where appropriate.
- Any discussion with the Channel or PMAP Chair must be recorded on the PCMT. For Channel or PMAP cases, this should be recorded as an Extraordinary Channel Panel meeting where required.
- Direct contact with the Subject before the first panel must be limited to obtaining vital information that cannot reasonably be acquired by other means.
- At the first Channel or PMAP panel meeting, the Chair will determine the most appropriate agency to approach the Subject for consent to Channel engagement. This should not be assumed to be the CTCO by default.
- Ownership of the case remains with CTP-Prevent until the case is formally adopted by Channel or PMAP.

Visits during Channel, PMAP or PLP

- Visits during ongoing case management must be linked to the aims and objectives of the agreed Channel Support Plan, PMAP plan or PLP Case Management Plan.
- CTCO involvement in visits should be proportionate and should support risk assessment, safeguarding, support planning, risk mitigation, case review, escalation or closure.
- CTCOs should agree roles with any accompanying staff or partner agencies before the visit. The lead agency, purpose of the visit, speaking roles and intended outcomes should be clear.
- CTCOs must record all relevant observations, disclosures, risks, safeguarding concerns and agreed actions on the PCMT.
- Where a visit identifies escalated risk, the CTCO must discuss this with a Supervisor and consider whether the case requires urgent review, escalation to PLP, escalation to Pursue, or other safeguarding or policing action.

Visits linked to case closure or resolved concerns

- Where a matter has been resolved and the case is being closed, the relevant s.36(3), Channel, PMAP or PLP closure decision should be made and recorded before any closure visit takes place, unless there is a clear operational reason to do otherwise.
- CTCOs must record the rationale for any closure visit, including why contact is required and what the intended outcome is.
- Any visit or contact with the Subject must be recorded on the PCMT, including the outcome, any remaining concerns, signposting, onward referrals and responsibility for future support.

- If a closure visit identifies new or escalated Prevent, safeguarding or criminal risk, the case must not be closed until the risk has been reviewed and an appropriate case management decision has been made.

Risk Assessment and Safety

- CTCOs deployed for Subject visits must be operationally deployable and not restricted from carrying out the activity required.
- The CTCO Supervisor must review the rationale, necessity, proportionality and intended outcomes before the visit takes place.
- A pre-visit risk assessment of the Subject, venue and circumstances must be completed before deployment and recorded or uploaded to PCMT as an Activity.
- CTCOs may use a local force visit risk assessment or the Prevent Subject Engagement Risk Assessment form available on CT-Net. Set the risk assessment as an Activity in the PCMT casefile, and upload any copies of the risk assessment used.
- Each CTCO must conduct an ongoing dynamic risk assessment throughout the visit.
- PPE, Body Worn Video and radio use should be considered in advance and decided on a case-by-case basis following the pre-deployment risk assessment.
- A record should be raised with the relevant force control room so local police are aware of the CTCOs' presence at the location and can provide assistance if required.
- CTCOs must not provide personal phone numbers to Subjects or family members. Work phone numbers and work email addresses may be provided where appropriate and in line with local force practice.
- CTCOs must record relevant observations from the visit on the PCMT, including risk indicators, safeguarding concerns, engagement issues, protective factors, signposting and agreed actions.

ANNEX 4 – PURSUE SUBJECTS OF INTEREST IN PCM

Overview:

- This section replaces the **CTCO Responsibilities in Support of Pursue Actions** and summarises the **Pursue Investigations in Prevent Case Management** policy (which can still be accessed, along with all its resources, on CT-Net).
- **Core Principle:** Prevent and Pursue processes may run in parallel but must remain properly separated. CTCOs are not evidence gatherers for Pursue investigations.
- T2D
- **Pursue Referrals to Prevent:** This annex also applies where an individual is, or becomes, subject to a live Pursue investigation while being considered for, or managed within, PCM.

  Core PCM processes remain unchanged: referral, FIMU deconfliction, PGA, Information Gathering, s.36(3), Channel/PMAP, PLP and closure. Additional safeguards apply because the referral subject is also under investigation.

  The overall aim remains to provide support to a person who is susceptible to radicalisation or otherwise vulnerable to being drawn into terrorism, through reasonable and measurable objectives, without impeding the investigation or compromising the integrity of consent.

  Minors under investigation must be actively considered for Channel support. Adults are not excluded, but consideration must be given to likely consent, investigation sensitivity and the feasibility of intervention opportunities.

  Channel is not a Pursue tactic. It must not be used to progress an investigation, gather evidence, obtain intelligence, or bypass criminal justice safeguards. A Prevent referral is subject to CTSA 2015, Prevent policy, Channel Duty Guidance and the full PCM process. Where an SOI is referred into Prevent, case management and decision-making remain with the CTCO and Supervisor.

T2D

T2D

T2D

Risk ownership

- The CTP-Pursue investigation team owns the CT investigation and, in general terms, the risk of terrorism-related offending by the referred SOI.
- Prevent officers own the police elements of the Subject's journey through PCM.
- The Channel panel owns the safeguarding risk in relation to Channel support once the case is adopted.
- CTCOs remain the CTP decision-making representative at Channel panels. CTP has one vote at panel meetings, usually represented by the CTCO or Supervisor.
- CTCOs must continue to facilitate the intelligence cycle by passing new and relevant information from PCM activity to FIMU in a timely and detailed manner.
- If a CTCO fails to pass on information that policy requires to be passed to FIMU, and that information is relevant to the investigation, that risk rests with the CTCO.

T2D - Pre referral/pre meeting

T2D - Pre referral/pre meeting

T2D

Referral package and PCMT creation

- If CTP-Prevent and Pursue agree that a referral should be made, Pursue officers should normally submit National Referral Form. Where this is not practicable for operational reasons, another auditable method may be used, provided it contains at least the same level of information.
- The referral package must be sufficient to allow Prevent to create the case, complete assessment activity, and prepare for Channel, PMAP or PLP if required.
- A "form of words" alone is not sufficient for presentation to an external multi-agency panel. The case summary must contain enough information for the Channel Chair and panel to understand what they are being asked to adopt.
- Where the original summary cannot be shared with partners, a redacted version must be agreed. It must still contain enough detail to allow the Channel panel to assess the case lawfully and safely.

- The referral package should include, as a minimum:
  - case summary;
  - Subject profile;
  - confirmation of awareness of the investigation and Prevent referral, where appropriate;
  - mental health or neurodiversity needs;
  - immigration status;
  - serious criminality or international links;
  - risk assessment of the Subject, risk to others and risk to professionals;
  - internet or social media research report;
  - investigation safeguarding strategy;
  - CCS referral, if appropriate;
  - concerns about family members, household members or known associates;
  - any other case-specific information identified at the T2D joint meeting.
- A new PCM case must be created in the normal way where the Subject is not already open to Prevent:
  - Date: the date Prevent were made aware by Pursue;
  - Referral Originator: Policing (CT);
  - Referral Originator Sub Group: Case Under CT Investigation.
- Where a live Prevent case already exists and a CT investigation is opened and overt, CTCOs must:
  - open the live Prevent case on the PCMT;
  - open the Referral tab;
  - add a referral;
  - record the date Prevent were made aware by Pursue;
  - record Referral Originator as Policing (CT);
  - record Referral Originator Sub Group as CT Investigation Opened Whilst in Prevent.

Referrals arising from Executive Action:

- T2D
- CTCOs and Supervisors must consider whether there is identifiable Prevent-relevant information relating to each person.
- Where a Prevent referral is appropriate, it must be submitted to FIMU for deconfliction and assessment through the normal process.

- Where no Prevent referral is made, the rationale should be recorded locally or on the PCMT where there is an existing case or relevant case record.
- T2D
- Where the information is insufficient to support a Prevent referral but there are safeguarding or welfare concerns, these must be routed through the appropriate safeguarding or support pathway.

SOI Referrals at PGA:

- For Referred SOIs, the PGA stage will usually be passed automatically because the T2D T2D meeting should already have established reasonable suspicion that the Subject may be vulnerable to being drawn into terrorism.
- This does not remove the requirement to complete all relevant checks, information gathering and assessment activity.
- The referral originator does not need to be contacted at PGA if the CTCO assesses this as unnecessary, because the Pursue referral should already have been discussed at the T2D meeting. It remains good practice for CTCOs to keep the Pursue investigation team informed about the progress of the case.
- If the information provided is insufficient, the CTCO must raise this with their Supervisor. The Supervisor should liaise with the Pursue investigation team to establish whether further information can be shared.

Information Gathering:

- If no additional information-sharing restrictions prevent Channel consideration, the case may move from PGA into Information Gathering.
- The Information Gathering phase operates as normal, with the added requirement that any activity must not compromise the Pursue investigation T2D T2D. CTCOs should discuss relevant actions with the investigation team to ensure oversight.
- Investigation, intelligence-gathering and enforcement activity must be administered and controlled by Pursue.

---

s.36(3) decision:

- The s.36(3) decision remains a legal step and cannot be bypassed.
- The fact that the Subject is under a Pursue CT investigation does not, by itself, satisfy the s.36(3) threshold.
- CTCOs and Supervisors must record a full s.36(3) rationale explaining whether there are reasonable grounds to believe that the Subject is vulnerable to being drawn into terrorism.

- The rationale must identify the push-and-pull factors, susceptibilities, risks and support needs that may be reduced through Channel, PMAP or PLP.
- If information-sharing constraints mean Channel cannot operate safely or lawfully, the case must be considered for PLP or closure from PCM, depending on the risk and available Prevent options.

Channel suitability for Subjects under investigation

- A person subject to a CTP Pursue investigation may be presented to Channel only where all three criteria are met:
  - **Overt case:** the person has been formally notified by Pursue investigators that they are under investigation and for which alleged offence or offences;
  - T2D **post-arrest:** Channel support can only be offered after T2D such as a warrant, arrest, search or interview;
  - **Assessment / management of risk:** the Channel panel, with inclusion of the SIO or SIO representative, agrees that the case holds a level of risk that can be managed within Channel, and that risk assessments will continue to be kept under review by CTP.
- If the Subject is aware of the investigation only through unofficial means, this does not count as an overt investigation for PCM or Channel.
- T2D
- T2D

First Channel panel:

- At first panel, the CTCO presents the case and asks the panel to decide whether the case is suitable for adoption.
- It is strongly recommended that a member of the investigation team attends the first and subsequent monthly Channel panels where appropriate. This must be discussed and agreed with the Channel Chair.
- The investigation representative attends so that the panel has the clearest information and the investigation team can hear from partners and ask questions. They do not direct the panel on what intervention should be applied.
- CTP has one vote at panel, usually represented by the CTCO or Supervisor. The police vote should reflect the agreed Prevent and Pursue position.
- A Channel panel is not required to adopt a case simply because the Subject is under investigation. The CTCO's s.36(3) rationale and panel presentation must identify the relevant susceptibilities, risks and support needs that may be reduced through Channel support.

- If the Channel Chair or panel refuses the case because insufficient information can be shared for safe and lawful adoption, the case should be considered for PLP.

Consent:

- Written consent is still required for a referral subject to Channel support.
- Consent is not required for Prevent referral, police assessment, lawful information sharing or presentation to panel.
- The consent form must make clear that information shared for the purpose of assessing and informing a support plan is disclosable where it is legal, necessary and proportionate to do so.
- The Subject must be informed that personal information will be shared between agencies involved in the case via the designated local authority. This may include police and other law enforcement agencies, health and social care, education, Channel panel members, the Home Office and Home Office-approved IPs.
- Where legal advice leads the Subject not to consent, it may be appropriate for the Channel Chair or another suitable professional to speak with the legal advisor to explain Prevent and provide assurance. If consent is still not secured and Prevent concerns remain, the case should be considered for PLP.
- Refusal of one element of a support plan, for example a specific IP, does not necessarily prevent continued Channel support if the Subject consents to other relevant support.
- CTCOs and the panel must be clear whether the Subject is refusing a particular element of the support plan or all Channel support.

Subject already in Channel becomes subject to an overt Pursue investigation:

- Where a person already adopted as a Channel case is subsequently made aware that they are subject to an overt CTP Pursue investigation, they may remain in Channel if the SIO is in agreement and the panel believes appropriate support can still be provided.
- The same three criteria must be met:
    - the case is overt;
    - the case is T2D post-arrest;
    - the Channel panel and Pursue investigation team agree that the risk can be managed within Channel and will remain under review by CTP.
- The panel must be assured that the Subject is aware they are under investigation. The context of notification, for example arrest or verbal notification by the SIO, must be recorded in panel minutes.
- It is good practice to verbally confirm that the Subject's existing consent remains valid and to record this on the PCMT.

- If the Channel Chair requires written consent again, the CTCO should assist where CTP-Prevent is the best agency to ask the Subject. Another panel member or agency may be more appropriate.
- Any renewed consent request must explain that information shared for the purpose of assessing and informing a support plan is disclosable where legal, necessary and proportionate.
- Details of the renewed consent must be recorded in the relevant PCMT consent field and in Channel panel minutes.

Channel Subject becomes a lead:

- A lead is not an investigation. A Subject in Channel who becomes a lead may remain in Channel.
- CTCOs must maintain the confidentiality of the lead process as they would in any other circumstance.
- If the lead develops into T2D an investigation, this policy applies from that point.

Support plan and IP commissioning:

- Support plans are developed and recorded in the same way as other Channel cases, drawing on completed assessments and partner information.
- The delivery of Channel support must operate separately from the Pursue investigation.
- All communications from IPs, statutory partners and any other agencies tasked with a role in the Channel Support Plan must be with the CTCO, not with the Pursue investigation team.
- An IP may be commissioned only after the Channel/PMAP panel has reached majority agreement to engage a specific IP and at the panel's request.
- CTCOs are responsible for commissioning IPs in the usual way, but must use the updated IP Commissioning Form for Referred SOIs, including objectives, priorities and Red Lines.
- The SIO must have final sign-off for the IP commission and risk assessment.
- Before sessions begin, CTCOs must ensure:
    - clear objectives are set;
    - a suitable summary of the radicalisation concerns and investigation is provided;
    - the IP is told what can and cannot be discussed;
    - Red Lines are clear;
    - the IP understands that they must not compromise the investigation or future prosecution;

  - the IP understands that they must not gather intelligence or seek specific information related to the investigation;
  - the IP reads out the DPIN at the first session;
  - the IP records significant or unsolicited statements in reports;
  - all IP reports and communications are recorded and handled with potential CPIA disclosure in mind.
- CTCOs must never ask an IP to obtain specific information related to the investigation.
- IPs are under no obligation to accept commissioning.
- If an IP is unclear about what they should or should not do, they should seek clarification from the CTCO or Home Office Interventions Team before proceeding.

Disclosure and information sharing:

- Information sharing must be necessary, proportionate and linked to the legitimate aim of preventing the Subject from being drawn into terrorism.
- It may be appropriate to disclose that the Subject is under CT investigation, but this must be justified by necessity and proportionality. In many cases, it will be sufficient to state that the request is made under CTSA because the Subject has been referred to Prevent.
- Operationally sensitive information must not simply be withheld if this prevents Channel or PLP from functioning lawfully and safely. An agreed form of words or redacted case summary must be prepared where required.
- IP reports and Channel documentation may be disclosable where there is a legal requirement to do so. CTCOs must ensure records are accurate, clear and capable of disclosure if required.

Record-keeping:

- CTCOs and Supervisors must follow regional Prevent recording processes.
- PCMT must be used for any case accepted into Prevent.
- Where CTCOs are involved before a Prevent referral is created, records must be kept minimal, factual and in accordance with local decision-log processes.
- CTCOs must anticipate disclosure requirements. BWV, notes and records must be retained in accordance with local evidential and information-management standards.
- Any significant statement, safeguarding disclosure, volunteered offence-relevant information, referral decision, risk decision or rationale must be recorded clearly and passed to the appropriate owner.

Disagreements and escalation:

- Where Prevent and Pursue cannot agree on referral, information sharing, Channel suitability, PLP suitability, IP commissioning, T2D or risk management, the matter should be escalated through the agreed local governance route.
- T2D
- If a case cannot be safely managed in Channel due to risk, disclosure restrictions, consent issues or investigation sensitivity, CTCOs must consider PLP or closure from PCM with suitable rationale.

Subjects under overt Pursue investigation entering PLP:

- The case must be considered for PLP through a formal and documented panel meeting with the CT investigation team where a Subject remains under a live CT investigation but exits or cannot enter Channel/PMAP because:
  - the panel refuses to adopt the case;
  - intervention opportunities are exhausted;
  - objectives have been achieved;
  - information cannot be shared sufficiently for Channel to operate;
  - the SIO decides that the Subject is no longer suitable for Channel depending on the type and level of terrorism risk.
- In these circumstances, the Subject may be moved from Channel into PLP as a Category 3 case. Refer to the PLP section of this SOP.
- This is not automatically a closure outcome of "Risk Remains – CT Escalation". Where appropriate, the more accurate rationale will be that all intervention options have been exhausted or considered, and responsibility has transferred back to Pursue.
- CTCOs or Supervisors must seek direction from the SIO to ensure that any IP tasking, support activity or partner engagement does not conflict with the investigative strategy.

Withdrawal, closure and return to Pursue:

- Pursue may withdraw an SOI from Prevent if operationally necessary.
- If a live-investigation SOI exits Channel while the investigation continues, the case should be considered for PLP so that Prevent and Pursue can agree next steps.
- A case may be handed back to Pursue without this being recorded as an escalation to Pursue, where all relevant parties have agreed that PCM is no longer required and the investigation remains the appropriate route.

- CTP-Pursue cannot require a case to remain open in PCM where the CTCO and Supervisor assess that continued PCM is unnecessary. Any closure rationale must be clearly recorded and defensible.
- Where Channel or PLP closes, refer to the Case Closure and 6/12-month review sections of this SOP.
- If Channel support becomes suitable again later, a new joint meeting T2D should be held. If the case is still within the 6/12-month review period, it may be reopened following an ad-hoc review. If outside the review period, a new Prevent referral may be considered.

Investigation ends:

- If the Subject is no longer subject to a live Pursue investigation, CTCOs should revert to usual Channel, PMAP, PLP, case management and closure processes.
- The CTCO and Supervisor must update PCMT and ensure the panel, where relevant, understands the change in status and its impact on risk, information sharing and support planning.

ANNEX 5 - INFORMATION AND DATA SHARING IN PCM

Overview:

- This section applies to information and data sharing with external agencies, statutory partners, local authorities, health partners, education providers, safeguarding services, charities, Channel or PMAP partners, PLP partners, and other relevant non-police bodies.
- This section does not cover internal police intelligence submissions, police system checks, or internal police-to-police requests, except where they affect whether external information sharing is permitted.
- CTCOs may request, receive or share information only where it is lawful, necessary, proportionate, relevant and recorded.
- Information sharing must be considered case by case. CTCOs must be clear about:
  - what information is required;
  - why it is required;
  - who holds it;
  - the lawful basis or legal gateway relied upon;
  - how it supports the PCM decision being made;
  - what outcome is expected.
- Requests must be targeted. CTCOs must not make broad or speculative requests unless there is a clear and recorded operational necessity.
- Safeguarding information that is not specific to Prevent must be shared with the relevant local safeguarding system or agency, where it is not already held there.

Information-sharing tools and templates:

- CTCOs must use local Data Sharing Agreements, Information Sharing Agreements, Channel or PMAP protocols, PLP agreements, or agreed local request processes where available.
- Refer to the **Data Sharing Agreements (DSA Toolkit)** on CT-Net, which is comprised of the following resources, accessible through the hyperlinks below:
  - **Data Sharing Agreement Process Map (Powerpoint)**
  - **Presentation on DSA (comprehensive) (Powerpoint)**
  - **DSA Definitions (Word)**
  - **ICO Guide to Police DSA (PDF)**
  - **ICO Guide to Police DPIA (PDF)**
  - **ICO DPIA Sample Template (Word)**
  - **CTPHQ Tasking Template (Word)**
- The above DSAs have been agreed and signed by respective Assurance and Compliance Leads, Legal departments and Senior Leaders.

- The agreements are purpose specific and only cover PCMT data sharing arrangements between CTPHQ and DfE/HO respectively.
- The **National Referral Form,** the **Notice, Check, Share** process and the **Act Early Hotline** are the main national referral routes into Prevent.

Legal gateways and lawful bases:

- The appropriate legal gateway for data sharing will depend on the case stage, purpose, recipient and type of data. Consent is not required for lawful police referral, statutory assessment, or information sharing.
- Data protection legislation is not a barrier to lawful information sharing. It provides the framework for sharing personal data lawfully, securely and appropriately. Common gateways and lawful bases may include:
    - **Channel:** CTSA 2015, ss.36 and 38, which requires partners of a panel to co-operate with the panel and police in carrying out Channel functions. This includes providing relevant information so far as appropriate and reasonably practicable.

      S.38 does not override data protection law, legal privilege, confidentiality duties or other statutory restrictions. The Channel Duty Guidance is clear that the duty to co-operate does not require or authorise disclosure that would contravene data protection legislation.
    - **PLP:** the CTSA does not apply to information sharing for PLP panels. In the absence of a PLP Data Sharing Agreement (DSA), common information sharing gateways can include:
        - UK GDPR Article 6(1)(e), public task;
        - UK GDPR Article 9(2)(g), substantial public interest, and relevant Data Protection Act 2018 Schedule 1 conditions for special category data;
        - Data Protection Act 2018, Part 3, including sections 31 and 35, where processing is for law enforcement purposes;
        - Crime and Disorder Act 1998, section 115, where disclosure is necessary or expedient for crime and disorder purposes;
        - Relevant safeguarding powers and duties under the Children Act, Care Act or other statutory frameworks;
        - Common law policing powers to protect life, preserve order, prevent crime, protect the public and uphold national security.

External disclosure requests outside ordinary PCM:

- FOI requests relating to Prevent must be referred to local information management teams and, where relevant, CTPHQ-Interventions. Aggregate, anonymised data may sometimes be disclosed, but sensitive case information or operational detail is usually withheld under exemptions for national security, law enforcement or personal data.

- Subject Access Requests must balance the rights of the individual with security needs. Personal information may be shared where safe and lawful, but confidential sources, third-party data and operational tactics are usually redacted.
- Inquests, inquiries and court cases may request Prevent data. CTP-Prevent must co-operate lawfully, while protecting sensitive sources and sensitive operational methods. RPCs or designated officers must inform CTPHQ of significant proceedings to support consistent national handling.
- Use of PCMT data for research or external communication is permitted only with CTPHQ approval and robust controls. Where research involves CTP data or interviews with CTP staff, advice must be sought from the CTPHQ Interventions Research and Development Team.

Enhanced DBS disclosure requests:

- Prevent referrals and PCM information do not automatically appear on an Enhanced DBS certificate.
- Where a Force Disclosure Unit is considering disclosure of police information relating to extremism, radicalisation or Prevent, it must contact the intelligence owner before disclosure.
- The intelligence owner must confirm:
    - accuracy of the information;
    - relevance and proportionality;
    - whether any sensitivities exist, including operational impact, covert tactics or live enquiries.
- A clear and proportionate form of words must be agreed with the intelligence owner to ensure that disclosure is limited to what is strictly necessary, sensitive operational activity is not compromised, wording is factual and neutral, and the content complies with statutory tests and human rights considerations.
- Prevent and CT teams may advise and provide specialist context, but they do not decide whether information is disclosed on an Enhanced DBS certificate.

ANNEX 6 - PREVENT INTELLIGENCE HANDLING ON LOCAL POLICE SYSTEMS

Overview:

This section sets out the principles and procedures for recording Prevent-related intelligence on local police systems. It ensures compliance with Data Protection Act (DPA) 2018, GDPR, and safeguarding obligations, while maintaining proportionality and consistency across all regions.

Scope:

Applies to all Prevent practitioners and senior leaders within UK policing who manage or access local force intelligence systems.

Position Statement:

Prevent is a supportive safeguarding programme, not a punitive measure. Intelligence handling must protect individuals' privacy rights, avoid unintended negative consequences (e.g., employment, education), and align with public messaging (e.g., Act Early campaign).

Principles

When recording, retaining and otherwise using Prevent-related intelligence on local police systems, practitioners and senior leaders must comply with Article 8 European Convention on Human Rights (the right to privacy):

a) Legitimate Aim – the recording of personal data must be for one or more of the following objectives: the interests of national security, public safety or the economic wellbeing 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.

b) Lawfulness – there must be a lawful basis in statute or common law to record and otherwise use the data. Practitioners and senior leaders must be satisfied that it is necessary to process the data for one or more of the law enforcement purposes and fulfill a policing purpose.[5,]

c) Necessity & Proportionality – practitioners and senior leaders must be satisfied that:

- **i.** The objective of the (legitimate aim) fulfilled by recording intelligence is sufficiently important to warrant intrusion into the subjects' rights to privacy.
- **ii.** The intrusion is rationally connected to the objective.
- **iii.** The intrusion goes no further than is necessary.

[5] The "law enforcement purposes" are 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 (s.31 Data Protection Act 2018). The "policing purposes" include but are not limited to: protecting life and property, preserving order, preventing the commission of offences, bringing offenders to justice, any other police duty or responsibility arising from common or statute law (Police information and records management Code of Practice).

iv. Standing back, by recording the information, a fair balance is struck between the rights of the individual and the interests of the community.

Principles:

Practitioners and senior leaders must, insofar as the information comprises personal data, ensure that they comply with the six data protection principles:

Principle 1: processing of the personal data is lawful and fair (s.35(1) DPA) - see Article 8 Principes above, and public messaging must reflect operational practice.

Principle 2: the purposes of processing be specified, explicit and legitimate (s.36(1) DPA).

Principle 3: The requirement that personal data be adequate, relevant, and not excessive (s.37 DPA).

Principle 4: requirement that personal data be accurate and kept up to date (s.38(1) DPA) - Information must be current and reviewed regularly.

Principle 5: The requirement that personal data be kept for no longer than is necessary (s.39(1) DPA).

Principle 6: The requirement that personal data be processed in a secure manner (s.40 DPA).

To comply with the above principles, practitioners and senior leaders must record and handle intelligence in accordance with the College of Policing's Intelligence Management Authorised Professional Practice (APP), the Information management APP and the Police information and records management Code of Practice.

When to Record Prevent Intelligence

Prevent related information may be recorded on local police systems only when:

- It relates to safeguarding concerns necessary for local risk management.
- It supports officer safety or public protection.
- It meets the CTSA Section 36 threshold (reasonable grounds to believe the individual is vulnerable to being drawn into terrorism).
- It meets intelligence recording standards for the said local force.

Do NOT record:

- Blanket uploads of all Prevent referrals or risk assessments.
- Information that does not meet necessity and proportionality tests.

Access Control:

Systems must signpost to PCMT as the authoritative source. You should only share information from PCM which is deemed relevant and necessary for local police to be aware of. No uncontrolled sharing or 'intel dumping'. FOW example " Full information is stored on the PCMT please contact the owner PC/DC...Contact details ... "

Governance

CTPHQ Prevent will issue national guidance and monitor compliance. Data Protection Impact Assessment (DPIA) must be updated to reflect this policy. T1E

T1E

Review and Audit

Annual review by Prevent HQ. Regional audits to ensure compliance and consistency.

Breach Management

Any breach of this policy must be reported to CTPHQ Prevent and information Governance Unit and handled under police force data breach procedures.

RRD Obligations

All Prevent-related data recorded on local systems must comply with Review, Retain, Delete (RRD) principles; more information can be found in the RRD Policy relating to the local force and PCMT:

- Review: Data must be reviewed at regular intervals to ensure relevance.
- Retain: Retain only data that is necessary for safeguarding or operational purposes.
- Delete: Remove data promptly when it is no longer required for the purpose it was collected.

Position on Local Intelligence Systems

CTPHQ Prevent recognises that forces may use local intelligence systems for operational risk management; however, strict controls must apply:

- PCMT remains the single authoritative source for Prevent information.
- Local systems may only reference PCMT using markers that signpost back to PCMT.
- Prevent-related intelligence must be minimal, proportionate, and separated from other intelligence to avoid unintended disclosure.
- Blanket uploads or 'intel dumping' of Prevent referrals or assessments are strictly prohibited.
- Operational practicality and desirability of this approach will be monitored by Prevent HQ to ensure compliance and consistency.

ANNEX 7 - GUIDANCE FOR FORCE DBS TEAMS AND PREVENT POLICE

Joint Working on the Disclosure of Police Intelligence Relating to Extremism

Overview:

This guidance sets out how Prevent policing, Force Disclosure Units, and the Disclosure and Barring Service (DBS) should work together when considering whether police intelligence relating to Prevent about an individual should be disclosed on an Enhanced DBS Certificate. It is particularly relevant where intelligence relates to extremism, radicalisation or behaviour that may pose a safeguarding risk.

The objectives of this guidance are to ensure that:

- information is shared lawfully, accurately and only where necessary
- safeguarding decisions remain consistent, proportionate, and owned by the correct authority
- Prevent police teams, Disclosure Units and DBS practitioners understand their distinct but complementary roles
- all disclosures relating to extremism are handled with appropriate scrutiny, care and oversight

Prevent is a supportive safeguarding programme, not a punitive measure. A Prevent referral does not constitute a criminal disposal, caution or conviction, and DBS does not routinely access Prevent case data. Any disclosure must therefore be lawful, necessary, proportionate and be for a legitimate safeguarding purpose.

The NPCC leads for CT policing, and the DBS portfolio have been in discussion with the DBS and ultimately the intention is for the national counter terrorism policing unit (hosted by the Metropolitan Police) to operate its own DBS disclosure unit which will assess any intelligence information it and regional CTUs hold relating to an enhanced disclosure certificate applicant and ultimately determine the content of any appropriate disclosure in accordance with s113B(4) of the Police Act 1997.

This note is intended to provide guidance to force disclosure units in the interim around the potential disclosure of CT (including PREVENT) related information.

Key Principles

Safeguarding First:

Prevent, policing and the DBS all share a statutory responsibility to protect:

- children
- vulnerable adults
- the wider public

Where intelligence suggests a **risk of extremism, radicalisation or harm**, this may be relevant to recruitment and safeguarding decisions.

Clear Decision-Making Accountability

Section 113B Police Act 1997 describes the requirements for enhanced criminal record certificates, which include that:

[...]

(2) The application must—

(a) be countersigned by a registered person, and

(b) be accompanied by a statement by the registered person that the certificate is required [for the purposes of an exempted question asked]22 for a prescribed purpose. [...]

(4) Before issuing an enhanced criminal record certificate [DBS] must request [any relevant chief officer] force to provide any information which [...] —

(a) [the chief officer reasonably believes to] be relevant for the purpose described in the statement under subsection (2), and

(b) [in the chief officer's opinion,] ought to be included in the certificate.

[...]

Thus, the responsibility for providing local police information on an Enhanced DBS Certificate rests with the **Chief Officer of Police**.

In practice, this is delegated to:

- the **Force Disclosure Unit Manager**, or
- the **force lead for Safeguarding/Public Protection or**
- **other senior roles within force**

Counter Terrorism Units (CTUs) and Prevent teams **support** the process by providing expert intelligence context, but **do not** make disclosure decisions.

Proportionate, Necessary and Relevant Disclosure

Force Disclosure Units assess information in accordance with national guidance, including the Statutory Guidance and Quality Assurance Frameworks. In summary, information should only be disclosed if it is:

- **accurate**
- **up to date**
- **directly relevant** to the workforce (Child, Adult, Child & Adult) the applicant is seeking to work with, except for 'Other' workforce applications where the risk considerations are to anyone the applicant comes into contact with within their role
- **necessary** to safeguard

Not all intelligence with an extremism link meets these thresholds. Decisions must weigh **seriousness**, **recency**, **credibility**, and **relevance**.

Contact with the Intelligence Owner

Before any local intelligence is disclosed, the **Force Disclosure Unit must contact the intelligence owner**.
The intelligence owner must confirm:

- accuracy of the information
- relevance and proportionality
- whether any sensitivities exist (e.g., operational impact, covert tactics, live enquiries)

Form of Words

A clear and proportionate **Form of Words** must be agreed with the intelligence owner to ensure:

- disclosure is limited to what is **strictly necessary**
- sensitive operational activity is **not compromised**
- the wording is factual, neutral and free from unnecessary detail
- the content complies with all **statutory tests and human rights considerations**

Although they do not authorise disclosure, Prevent and CT teams must ensure wording is contextualised and appropriate.

Ownership of Information

Chief Constables are the data controllers for all information held on local policing systems and jointly control data on national police information systems such as the Prevent Case Management Tracker (enhanced) (PCMTe).

Prevent teams:

- may advise
- may provide intelligence context
- **cannot mandate disclosure**

How Police and DBS Should Work Together

When Disclosure Units Should Engage CTU/Prevent

Engagement with CTU or Prevent is required when there is a CT footprint on police systems, which may indicate that:

- intelligence relates to extremist activity, radicalisation or ideological motivation
- further specialist context is needed to interpret severity, meaning or risk
- there is doubt about whether behaviour meets the threshold for disclosure
- the intelligence may indicate escalating or persistent risk

CTU/Prevent can provide context on:

- nature and type of extremist behaviour
- level of risk, vulnerability, intent or capability
- known networks or previous engagement
- changes in behaviour or risk indicators

CTU/Prevent do not decide whether information is disclosed.

How DBS Uses Disclosed Information

Once disclosed by police, DBS may:

- insert disclosed information into an enhanced DBS certificate
- consider the information as part of suitability and barring decisions
- apply **automatic barring** where the individual has relevant extremism-related convictions or civil orders
- notify employers if new extremism related information later becomes available (pending legislative changes)
- extend eligibility criteria to ensure more roles involving vulnerable people are appropriately vetted

---

Practical Process for Force Disclosure Unit Practitioners

Step 1 — Identify intelligence that may require disclosure

Review all relevant records for including those relating to extremism, radicalisation or behaviour that may pose a safeguarding risk and consider/assess the information against the Statutory Guidance and Quality Assurance Frameworks.

Step 2 — Contact the intelligence owner

Discuss:

- relevance to the workforce (Child, Adult, Child & Adult) role the applicant is seeking to work with, except for 'Other' workforce applications where the risk considerations are to anyone the applicant comes into contact with within their role
- proportionality
- sensitivities (operational, safeguarding, legal)
- credibility and seriousness

Step 3 — Agree the Form of Words

Work with the intelligence owner to ensure wording is:

- factual and proportionate
- compliant with the Statutory Guidance and Quality Assurance Frameworks
- does not compromise ongoing operations

- suitable for inclusion on an Enhanced DBS Certificate

Step 4 — Record the rationale

A full decision record must include:

- why information was (or was not) relevant
- the proportionality assessment
- advice received from Prevent/CTU
- evidence informing the decision
- details of discussions with the intelligence owner

Step 5 — Seek further advice if required

Where uncertainty remains:

- consult Prevent
- consult CTU
- seek legal advice from Force Legal Services

Summary of Statutory Disclosure Guidance (Plain English)

The Statutory Disclosure Guidance (Home Office) and Quality Assurance Frameworks set out how police must decide whether to disclose local intelligence. Before disclosing police must assess and consider the information against all of the Statutory & Quality Assurance Frameworks requirements/tests (i.e. the Chief Officer has deemed the information to be relevant for the prescribed purpose and ought to be disclosed

Decisions must:

- be made by the Chief Officer or authorised delegate
- be well recorded and justified
- comply with the Statutory Guidance and Quality Assurance Frameworks
- comply with data protection and human rights law
- be capable of scrutiny by the Independent Monitor

Statutory Guidance Link:

(Statutory disclosure guidance - GOV.UK) and the Quality Assurance Framework

N.B. Applicants have the right in legislation to seek a review by the IM of any information disclosed on their certificate, and the IM will decide whether in (currently) his opinion it fulfils both thresholds imposed by s113B(4). The IM has the power to require the chief officer to delete any information which he feels does not satisfy the disclosure threshold. Clearly the IM needs to be able to review all the information considered by the chief officer when undertaking such a review, and the chief officer is therefore obliged to provide that to the IM – that would include any CTU related information that has been considered in making the original disclosure.

ANNEX 8 - FALSE COMPLIANCE / DISGUISED COMPLIANCE / INSINCERITY OF CHANGE

Overview:

- This section sets the minimum practice standard for CTCOs to identify, manage, mitigate and audit concerns that a subject's engagement may be performed (i.e., designed to reassure professionals) rather than representing sustained, evidenced change.

Core practice principles (apply throughout PCM)

- T1E

Definitions (for recording language)

- **Disguised / false compliance:** engagement that appears cooperative but is primarily aimed at reducing scrutiny or accelerating closure, without corresponding evidence of meaningful, sustained change.
- **Insincerity of change:** claimed change that is not corroborated by independent sources, durable behavioural shifts, or outcomes across contexts/time.
- **Recording rule:** Use factual language: *"Evidence is / is not present that…"* rather than *"The subject is being insincere."*

ANNEX 9 - REVIEW, RETAIN & DELETE (RRD)

Overview:

- This section provides the practical, operational considerations for completing mandatory RRD on the PCMT.
- For the step-by-step process and technical instructions on completing RRD Approval in PCMT, CTCOs and Supervisors must refer to the **PCMT** Managing RRD Approval Requests user guide.

Understanding Review Types:

- **Initial Review** – Created automatically at final case closure; retention initially set to 6 years.
- **Scheduled Review** – Conducted 6 years after final closure (and then at 6-year intervals where retained).
- **Triggered Review** – Can occur at any time between scheduled reviews (e.g., errors, ROAR/SAR, complaints, court directions, internal decisions).

When to Start a Triggered Review:

- A case has been created in error, but not duplicate casefiles. If a subject already has one PCMT casefile created for them, deleting a duplicate would also permanently delete all other casefiles too, even ones that CTCOs may need to keep.
- No policing purpose apparent (no interventions; malicious/misguided referral; no outstanding legal/process matters).
- Subject Access Request (ROAR/SAR), complaint, court direction, independent/serious review.
- Deceased subject (retain only if still connected to CTP activity).

RRD Principles and Considerations:

- The PCMT user guide linked at the start of this section takes users through the steps and checks required to complete RRD. In this SOP we will look at the principles reviewers need to consider whilst deciding whether to retain or delete a record.

Consider Continuity of Cases:

- Alongside completing the specific system checks that the PCMT will guide you through, play close attention to any previous Retention summary, if present, and also the original closure rationale and outcome of the PCMT case.
- If there is a suggestion that the case was closed with risk remaining, it is recommended that unless something can be identified in the interim that negates that risk, the

previous 'risk remaining' outcome would likely provide a legitimate policing purpose to retain the case further.

- Ensure that checks on any of the relevant databases (PCMT, T1E etc) cover the **entire** timeframe from the last RRD process until the time and date of the current RRD process.

Retention Considerations: Considering the casefile's closing rationale, any previous RRD outcomes and your own checks:

- **Is there evidence of a capacity or propensity to inflict serious harm of any kind?**
  - Consider offences specified in Schedule 18 of the Sentencing Act 2020;
  - Offences of causing or permitting mutilation or unnecessary suffering to a protected animal under S.2 of the Animal Welfare Act 2006.
  - Consider any predatory offences, aggravated offences, domestic or sexual violence, intentional serious harm arson, war crimes, and "insider threat" concerns, if noted.
- **Are there any other issues that in your CTP professional judgement causes you concern in terms of the risk the individual presents?**
  - Consider hate offences and antisocial behaviour.
  - Consider ongoing asylum processes.
  - Consider whether a firearms licence has been revoked or a firearm application refused.
- **Are there any concerns in relation to behaviours towards children or vulnerable adults?**
- **Are there any concerning behaviours involving a breach of trust? Was dishonesty, grooming or fraud involved?**
- **Is there evidence of established links or associations that might increase the risk of harm?**
  - T2D - Provides various factors of risk by association
  - Hate-groups; online extreme / sadistic violence groups or groomers; criminal gangs; human trafficking; proscribed groups or other extremists.
- **Could the PCMT record be of interest to a specific inquiry or court matter, upcoming or ongoing?**
  - Consider known disciplinary proceedings, court cases, internal / independent / public inquiries, etc.
- **Are there ongoing concerns in relation to substance misuse?**
  - Consider anything present at the close of the original PCM case and since and its relevance in context (if any).

- **Are there concerns that an individual's mental state might demonstrate relevant risk, particularly involving violence?**
    - Use the NDM, your professional judgement and the standard of reasonableness to decide whether the details stored on the PCMT are still necessary, proportionate and retained with a legitimate policing purpose?

ANNEX 10 - SIX- AND TWELVE-MONTH REVIEWS

Overview:

- This procedure applies to:
  - all cases **closed from Channel/PMAP**, and
  - all cases **closed from PLP**, and
  - cases that have **previously been in Channel/PMAP** and later become **live in PLP**, where a Channel/PMAP six- or twelve-month review trigger is generated.
- **Channel/PMAP:**
  - CTCOs must complete a six-month review and a twelve-month review for all cases adopted by Channel/PMAP following closure.
  - CTCOs must ensure that, at the point of Channel/PMAP closure, PCMT is updated accurately so that review triggers are generated.
- **PLP:**
  - CTCOs must complete a six-month review and a twelve-month review for all closed PLP cases.
- **Channel/PMAP review triggers generated while the case is live in PLP**
  - If a case has previously been in Channel/PMAP, it may generate a Channel/PMAP six- and twelve-month review trigger even if the case is currently live in PLP.
  - Where this occurs, the review must be used as an opportunity to consider whether the case should be presented again to Channel/PMAP.

CTCO duties – minimum expectations:

- CTCOs should complete proportionate checks and information requests before each six- and twelve-month review. As a minimum, CTCOs should consider and record:
  - police database checks;
  - information sharing requests to statutory partners (and other partners where lawful and appropriate to the case context);
  - referrer contact where appropriate;
  - review of any new safeguarding, police, or Prevent-relevant information since closure;
  - open-source checks (including i3/iii), where proportionate and appropriate.
- CTCOs should ensure that actions taken, and the outcomes of those actions, are recorded on the PCMT in a manner that supports audit and supervision.

Contact with the subject, family, and lead professionals:

- CTCOs should consider speaking with the subject and, where appropriate, the family or a lead professional, as part of review activity on a case-by-case basis, recognising that contact by CTP might sometimes not assist the Subject.
- CTCOs may determine that another agency is more appropriate to make contact.
- CTCOs may consider a contact visit or telephone call where appropriate.
- Refer to the **Contacting the Referral Originator or Subject** section of this SOP for details.

Channel/PMAP: review actions and outcomes:

- **Review actions:** For Channel/PMAP six- and twelve-month reviews, CTCOs should:
  - complete the proportionate checks and information requests set out above;
  - complete an SA at both the six-month and the twelve-month review stages to assess any new information since case closure.
- Where partner information is requested for a Channel/PMAP review, returns from those partners should be expected within five working days.
- **Outcomes:**
  - If no Prevent concerns have re-emerged, the CTCO must record the review outcome.
  - If new Prevent-related information emerges, the CTCO must notify the panel Chair and the case must be reassessed by police,
  - A case re-opened to PLP panel should consider whether the case should be re-presented to Channel/PMAP instead, especially where the case was previously categorised as CAT3 A or CAT3 B.

Handling new referrals during the twelve-month review period

- If a new referral is received during the twelve-month post-closure review period, it must be deconflicted and then must be recorded within the original case on the "Referral" tab.
- The case must be reopened as soon as practicable.
- If a referral is received after the twelve-month period, the normal case creation process must be followed.

Channel/PMAP six- and twelve-month reviews while the case is live in PLP

- Where a Channel/PMAP six- or twelve-month review trigger occurs but the case is currently open in PLP, CTCOs must apply the following:
  - The review must be used as a structured opportunity to consider whether the case would be better managed in Channel/PMAP and should be presented again.

- If the panel decides that re-presentation to Channel/PMAP is not appropriate, and the PLP SA has been updated within the preceding month, the Channel/PMAP review should consist of a concise update confirming the case remains open in PLP for case management.

- Suggested wording for the review SA entry (example):
  - "Case remains open in PLP. SA completed on DD/MM/YYYY. Channel/PMAP panel updated on DD/MM/YYYY."

ANNEX 11 - SUPPORT AND CASE MANAGEMENT PLANS

Overview:

- This section does not tell CTCOs how to use the mandatory Case Management Plan or Support Plan functions of the PCMT. Step-by-step user guides for how to do this are available here - Create and Manage Support Plans – and here Create and Management Case Management Plans on the NHOP Collaboration Spaces.
- This section will instead present **considerations** and **themes** that make for successful support and case management plans – henceforth just "support plans".

First Principles:

A good support plan does five things:

1. **Defines the issues that need addressing** – what are the problems? List them so everyone is clear about what needs to be changed or controlled in relation to the case.
2. **Selects interventions that target those problems** – what will you do about those problems? Supportive first, with safeguarding and management, and disruption wherever necessary.
3. **Tests effectiveness (or not) of the interventions** – how do you know whether your interventions are working? So you can evidence success, change tactics when they are not successful, and avoid "assuming" protective factors are working.
4. **Draws on multi-agency partners –** who at the panel has what expertise? We are not expected to know everything, so we draw upon the skills and experiences of colleagues.
5. **Use the National Decision Model (NDM) –** to keep the plan effective and justifiable. Gather Information → Assessment → Consider Powers / Policy → Consider Options → Take Action and Review – all revolving around our ethical and legal standards).

Define the issues you need to address in a way you can later test:

- Write out the problem statements in observable terms (behaviours, what is happening, how often, where, and with whom).
- Avoid labels without indicators (e.g., "radicalised", "fixated"). Labels do not guide action; specific, described problems do.

Establish a baseline before you "treat"

- For each problem, capture frequency, intensity, recency and context (offline, online, associations, safeguarding) – whatever is relevant to that specific issue.
- Without a baseline you cannot credibly measure improvement or deterioration.

Analyse what is driving and maintaining the problems

- Use the PRS, the SA and professional discussion at panels to identify the specific **push-and-pull factors,** including but not limited to –
  - the needs, grievances, trauma, emotional dysregulation, isolation, instability, coping deficits, substance misuse, crisis stressors, etc.;
  - grooming, echo chambers, influencers, reinforcement loops, normalisation of harm;
  - family, peers, professionals, online spaces.

Identify key priorities.

- Prioritise what is most risk-relevant, most urgent, and most likely to reduce multiple problems.

Set objectives that can be marked "met / partly met / not met":

- Record objectives as: reduce/improve X from baseline to target by date.
- Targets should be practical (reduced exposure, improved stability, reduced frequency/intensity, reduced risky contact).

Build a layered intervention package (supportive first; safeguards always; management/disruption if needed):

- **Supportive actions:** target drivers and build protective/promotive factors; choose the best-placed agency to deliver, not automatically police.
- **Safeguarding actions:** set out immediate protective steps, what "stabilised" might look like, and escalation thresholds.
- **Management/disruption:** explore **triggers → actions** (e.g., non-engagement, escalation, continued harmful behaviour). Keep it proportionate and time-bound.
- **Indirect actions ("by proxy"):** where appropriate, consider whether the Subject's environment be changed? Consider family boundaries, school/workplace plan, health support.

Plan engagement, not just interventions:

- Identify the best-placed engager and the approach style (supportive, clear boundaries, trauma-aware).
- Use family/carers as protective factors only if you specify what they will do differently, what support they need, and how you will evidence impact.
- Keep communication audience-specific (subject, family, school/work, partners) and purposeful.

Sequence interventions to avoid unintended harm:

- Phase the plan: stabilise first, then target drivers and exposures, then consolidate and step down.
- Check for unintended consequences (increased grievance, secrecy, urgency, shame, isolation) and state how you will detect and mitigate them.

Measure outcomes, not just activity:

- For each objective, use three measures:
  - **Process:** did the intervention happen (attendance, sessions delivered, referrals accepted)?
  - **Problem change:** has the baseline shifted (frequency/intensity/recency/context)?
  - **Meaning:** one sentence on why that change reduces vulnerability.

Review discipline:

- Review at every panel cycle and at planned checkpoints (e.g., 4/8/12 weeks).
- Set trigger reviews in advance, e.g., missed sessions, new information, safeguarding events, major life changes, escalation indicators.
- At review, consider: did the response happen, did the problem decline, could there be another explanation, did the problem move elsewhere, is there false compliance?

Keep records simple, consistent and audit-ready

- Every priority must have an action; every action must have an owner, timescale and minimum "dose".
- Record decisions, outcomes and reasons for continuing, adapting, escalating or closing.

Common pitfalls to avoid

- Too many priorities ("laundry list planning").
- No baseline, so "progress" becomes opinion.
- Actions without owners/dates/dose, so delivery drifts.
- Assuming protective factors are working without evidence.
- Disruption used as a substitute for addressing drivers, rather than as part of a layered plan.

This document is **OFFICIAL-SENSITIVE.**

By taking responsibility for this document, I acknowledge that I will handle the document in accordance with its protective marking and the handling instructions detailed below.

STORAGE	Stored in a CPNI approved Class 2 cabinet within a standard Police operating environment.
MOVEMENT WITHIN BUILDING	In an unsealed envelope by trusted hand.
MOVEMENT OUTSIDE OF BUILDING	By trusted hand in a single cover, or; Using a signed for postal service under a single cover. No protective markings should be displayed, and a return address must be on the reverse of the envelope.
REVIEW	In no more than 6 years' time from the originating dates of the document.
DESTRUCTION	To be shredded.

Counter Terrorism Policing is an alliance of UK police forces working with security and intelligence agencies to protect the public from terrorism.