COUNTER TERRORISM POLICING

HEADQUARTERS

# CTPHQ

# CTP-PREVENT Policy 2020

## Prevent Case Management by CTCOs & CTCO Supervisors

**V 3.5 August 2020**

| | |
|---|---|
| **Protective Marking** | OFFICIAL – SENSITIVE |
| **Title** | CTP-Prevent Policy 2020 |
| **Summary / Purpose** | Policy for Police PREVENT Practitioners |
| **Owner** | CTPHQ PREVENT – National Co-ordinator's Office |
| **Organisation** | Counter Terrorism Policing HQ |
| **Unit** | CTPHQ-PREVENT |
| **Contact Details** | NationalPolicePrevent@met.Police.uk |
| **Version** | 3.5 |
| **Publish Date** | 25 / 08 / 2020 |
| **Review Date** | Yearly from above date & after each official CTP-Prevent Policy update. |
| **Author** | Marek HUBERT |
| **Approval** | CTPHQ PREVENT – National Co-ordinator's Office |

| Version | Date | Distribution |
|---|---|---|
| 0.9 | 9th January 2018 | CTPHQ Prevent Team |
| 1.0 | 15th January 2018 | All CTP-Prevent staff via RPCs |
| 1.2 | 7th March 2018 | Author only |
| 1.3 | 18th March 2017 | CTPHQ Prevent Team |
| 1.4 | 22nd March 2018 | OSCT, Apollo, & L.A. Partners |
| 1.5 | 7th April 2018 | CTPHQ SLT |
| 2.0 | 9th May 2018 | CT Network Publication |
| 3.0 | 9th June 2020 | Policy Update 1st Draft |
| 3.1 | 22nd June 2020 | SLT feedback, profiles & DPIA |
| 3.2 | 10th July 2020 | Further SLT feedback. |
| 3.3 | 30th July 2020 | Final checks before RPCs |
| 3.4 | 13th August 2020 | RPC feedback |
| 3.5 | 25th August 2020 | Foreword & hyperlinks inserted |

Return to Contents

## CONTENTS

# Section 1 – Foreword

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

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

With the amount of time we spend online increasing every year, much of which adds enormous value, people are also exposed to a potential "pick 'n' mix" of online risks. These are especially relevant for the most vulnerable and isolated and those aged 11-25. Whilst terrorist tactics change to remain relevant and effective, their aims stay the same: to divide us, stoke hatred, increase influence and inspire supporters to murder innocent people. By working will other CT pillars and building strong and trusted external partnerships that work as a single Prevent system, we will continue to pre-empt threats and reduce risk and vulnerability by carefully intervening early using experience, skill and innovation.

The Prevent Policy serves as a framework that allows regions to identify, promote and build upon existing good practice across the network. It is intended to be a living document that is flexible and adaptive to future changes in the terrorism threat, and it underpins the delivery of the national Prevent strategic plan. The policy sets out overarching principles and should be read in conjunction with the detailed guidance contained within the CTCO Guide. This unpacks all the themes and processes within the Prevent Policy in much greater detail.

The Prevent Policy has been updated to reflect changes since 2018. Feedback and learning from the Prevent network over the past 2 years has been integrated where possible, and language has been sharpened to match the Channel Guidance update (no "multi-agency led", only Local Authority led and Police led (Channel and Police-led Partnership - PLP). Processes within PLP have been clarified, terms of reference for "Panels" within PLP have been defined, and the policy sets out how these interact with the Local Authority and other partners.

These excellent documents have been produced with the sole aim of helping front-line specialists to tackle radicalisers and protect those who are vulnerable to radicalisation. I am thankful to both the CTPHQ team who have developed this product and to all those working in vital front-line Prevent roles who have contributed.

**Nik Adams**

National Co-ordinator for Prevent
Counter Terrorism Policing Headquarters

# Section 2 – How to use this Document

## How to use this Document

- This document contains the foundational elements of the CTCO and CTCO Supervisor roles, however it should be read in conjunction with the CTCO Guide and Channel Guidance documents, both of which provide further direction and detail on all matters contained herein. These are available on the CTnet.
- Section can be navigated to from the Contents page by means of the blue, underlined hyperlinks. The Contents can be returned to by clicking on the "Return to Contents" hyperlink in the top right-hand corner of every page.
- Bullet points contain the policy itself. These points consist mainly of activities that **must** be undertaken at certain stages of the management process.
- On some occasions these points will also detail activities which must **not** be undertaken.
- A small number of points will contain **considerations** rather than directives. Whilst these **must** be considered, they may or may not be implemented within the specific context of any given case. A rationale concerning why the consideration was deemed appropriate or inappropriate within the specific context would always have to be uploaded into the relevant case on the PCMT.

**Text boxes contain further detail where policy points are felt to need further explanation. They may also include examples of the activities being discussed or good practice.**

## Section 3 – CTP-Prevent Strategic Objectives

This policy is a key part of delivering the strategic objectives for Prevent policing: to safeguard and support those vulnerable to radicalisation and to stop them from becoming terrorism offenders or supporting terrorism offenders. This is achieved by:

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

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

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

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

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

# Section 4 – PCM Overview

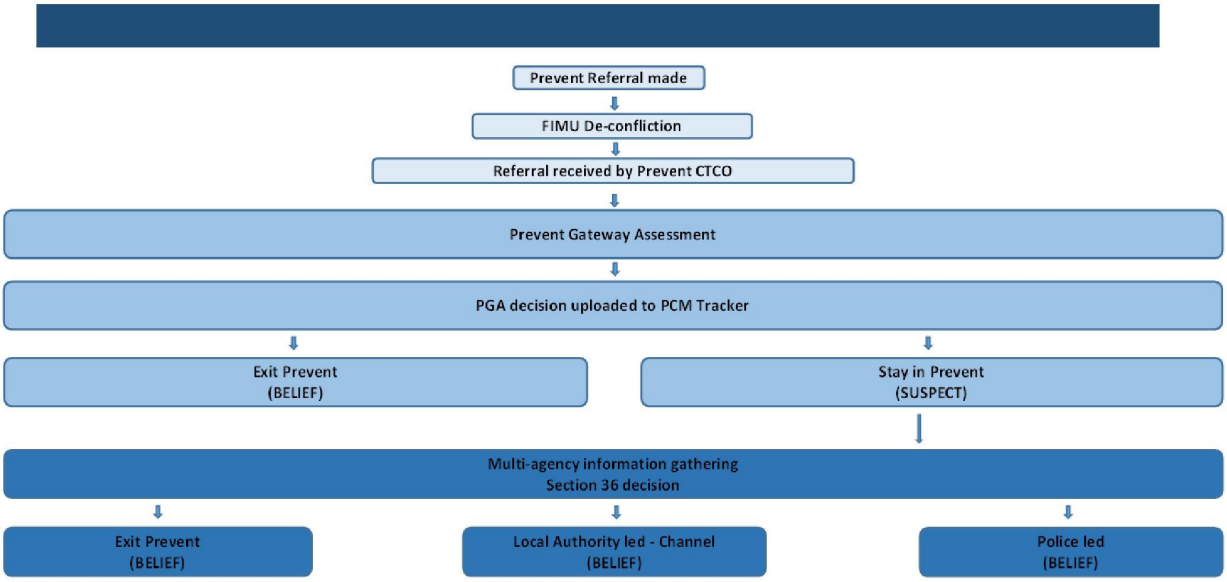


*Figure 1: The basic process map of the **non-Dovetail** PCM process*

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

### 1. Prevent Referrals

This is the initial receipt of a referral potentially suitable for Prevent Case Management. It may arrive with CTP-Prevent directly or via a Local Authority or an Intelligence Management Unit (IMU). This section of the policy outlines clearly the requirement to record referrals on the PCM Tracker at the earliest possible opportunity as well as the necessity for de-confliction and assessment of cases by IMUs before any activity is undertaken locally by CTCOs. This also addresses issues such as case responsibility where a Subject is active across multiple CTUs or CTIUs.

### 2. Prevent Gateway Assessment

The Prevent Gateway Assessment (PGA)[1] is the term given to the initial screening & triage phase that CTCOs must complete on all FIMU de-conflicted Prevent referrals. At the time of writing, the PGA is still referred to within the PCMT as the "Initial Assessment". The PGA / Initial Assessment is **mandatory** for **all** cases arriving with CTP-Prevent **after** IMU de-confliction. Drawing upon Policing databases and contact with the initial referrer, the PGA is the first use of CTP-Prevent's dedicated threat, risk and vulnerability assessment tool: the **Dynamic Investigation Framework** (**DIF**).

### 3. The Intelligence Cycle

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

[1] Formerly the "Police Gateway Assessment", and sometimes referred to simply as the gateway assessment.

### 4. Channel Cases

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

### 5. Police-led Partnership Cases

Led by Police but working in partnership with other police units and non-policing agencies, the Police-led Partnership (PLP) process concerns the management of individuals, groups, institutions or ideological expressions that, although not suitable for Channel, still have identified relevance to Prevent that requires support and/or mitigation. PLP was formerly known as "Police Led" or simply "PCM".

### 6. Outcomes, Case Closure and Case Transfer

Decisions around case closures should be made solely upon the basis of the presence of risks around terrorism related offending, not simply whether interventions have been made or attempted. Very generally speaking, whilst extremist behaviours and a risk of any terrorism related offending remains, cases should be regarded as still requiring Prevent management and mitigation. The circumstances in which case closure is appropriate and how closures can be made are detailed here.

### 7. Supervision

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

## PCM Tracker (PCMT)

The PCMT is a Prevent-specific web based case management application, accessible to all CTIUs and CTUs via their normal IT platform. Everything CTCOs do within the PGA, Information Gathering and PLP phases, including PLP Panels and any interventions and final outcomes from Channel, must be recorded within the PCMT. Although CMIS is the system used for the management and recording of case information within Channel, escalating risk and Channel outcomes must still be recorded on the PCMT as well.

The security marking for the system is **Official-Sensitive**, which means it is accessible via the PNN/PSN network and also works on work laptops and tablets, providing they are operating within PNN/PSN.

As the platform is Official-Sensitive any intelligence obtained which is Secret or above must not be recorded on PNN and instead recorded on the appropriate system as per local force guidance.

CTP-Prevent's use of the PCM Tracker has been mandatory since July 2018. Plans are underway to combine CMIS with the PCMT, making the proposed new system the only system upon which PCM activities will be recorded and from which CTP-Prevent performance data will be collated.

The Prevent network and this Policy document will be updated as progress is made on the proposed combined system.

# Section 5 – CTCO: The Role

## What are CTCOs?

Refer to the CTCO Guidance document for a more detailed breakdown of the following areas.

A Counter Terrorism Case Officer (CTCO) is a Police member of staff or warranted officer designated to enact the Police Prevent statutory duty under the CTSA 2015.

Police staff and officers performing the CTCO role will have comparable roles, with the key difference being the ability of an officer to utilise warranted powers where necessary. They are distinct from CTCO Supervisors and 2nd Line Managers.

### Basic Requirements

- **CTCOs will:**
  - Be vetted to at least Security Clearance (Enhanced) (SC(e)).
  - Have current force led safety and first aid training (or equivalent) for staff and officers.
  - Have current access to the PCMT, CMIS & all required local force intelligence & crime systems.
  - Complete the National Prevent Foundation Course (NPFC) as soon as practicable from starting role or complete online course, and attend any required refresher courses if already in post.

**PCM Basics**

- **CTCOs will:**
  - Record all received referrals and details of any case management action or decisions taken on PCM Tracker (PCMT). At the conclusion of the case, provide a closing assessment of the risk for supervision and apply all appropriate closure codes and drop-down boxes.
  - Apply the Dynamic Investigation Framework (DIF) to complete PGAs on all de-conflicted referrals and conduct background checks (including online footprint) to de-conflicted referrals and determine the PCM route.
  - Utilise and liaise with the Vulnerability Support Hubs (VSH) to assess vulnerability of referral Subject.
  - Submit all referrals to FIMU for de-confliction and "Pursue Assessment" before any dedicated "Prevent Assessment" by CTCOs.
  - Find out whether the case subject is under investigation for any non-CT offences.
  - Continually feed all relevant intelligence to FIMU, throughout the PCM process.
  - Monitor local Police systems for potential CT related incidents or intelligence, including missing person or crime reports.
  - Flag Subjects when necessary (PIW, PNC, NCIA, local systems) and remove as appropriate.

**Channel**

- **CTCOs will:**
  - Assess if cases are suitable for Local Authority led management and refer such cases to Channel Coordinators (or non-Dovetail equivalents).

- Attend all Channel Panels and fulfil the Police role as statutory partner as CT Subject Matter Expert (SME), disclosing Police held intelligence necessary to make effective risk management decisions. Note that other, non-Prevent, Police may also be invited to attend as necessary and requested by the Channel Chair.
- Risk assess deployment of Intervention Providers (IPs) to a Subject.
- Identify risk escalation in Channel cases with potential IHM lead or Priority Operation. Refer to FIMU for urgent assessment.
- **Non-Dovetail:**
  - Create CMIS record, record S.36 CTSA 2015 decision, complete updates and closure on CMIS
  - Gather information to complete Vulnerability Assessment Framework (VAF).
- **Dovetail:**
  - Provide relevant intelligence to LA Channel Coordinator (LACC) for their ongoing management of the case.

**Police-led Partnership:**

- **CTCOs will:**
  - Regularly apply the DIF to:
    - Assess Prevent relevant risks & vulnerabilities,
    - Decide the priority banding for the case,
    - Inform & build Case Management Plans (CMPs).
  - Attend, administer and document all PLP Panels where their cases are being discussed, or at the direction of the PLP chair.
  - Provide attendees with findings and recommendations arising from DIFs and the Vulnerability Support Hubs.
  - Identify, engage and risk assess deployment of approved Intervention Providers.
  - Undertake the activities/interventions detailed within the CMP to safeguard the Subject and public by reducing the Subject's Prevent-relevant risk and vulnerability.
  - Reassess DIFs and CMPs as frequently as required, based upon risk and on receipt of information which represents a relevant change to the circumstances of the case.

**Disruptive Activity:**

- **CTCOs will:**
  - Throughout the PCM process, disrupt extremist behaviour using problem solving approaches and activities to investigate and prosecute any ASB and offences by Prevent Subjects, not just terrorism offending. Wherever necessary, this should be done in conjunction with safeguarding activities.
  - Divert, deter, desist & where possible prosecute extremist "groomers", extremism-related offending & all other extremist activity by Individuals within the PLP process. To achieve this, officers should consider the full range of lawful & proportionate investigation, disruption & prosecution options available to them, paying due regard to the operational guidance on "extremism" provided in this CTCO Guide document.
  - Work with Partners to utilise their unique powers to divert, deter or desist extremists and other persons involved in extremist activities, including events which support or promote extremism.

- Compile evidence and build files to support the Local Authority to take safeguarding action, up to and including Wards of Court procedures.
- Provide disruptive capacity to CT investigations and other Pursue operations by completing tasks as directed as an overt response option.
- Officers should consider the full range of investigative and prosecution options when it comes to disrupting extremist material and activities. Please refer to the CTCO Guide and further guidance documents provided on the CTnet.

**Outcomes and Closures**

- **CTCOs will:**
  - Ensure the correct closure code is recorded on the PCMT / CMIS.
  - Ensure that if any flagging has been used during management (PIW, PNC, NCIA, and local systems), it is removed expeditiously.
  - Ensure all policing activity has been accurately recorded on the PCMT / CMIS including the use of activity flags to show specific interventions.
  - Ensure closure of cases only occurs when the identified case priorities around risk and vulnerabilities have been addressed and any risk has been appropriately mitigated, or at least evidence and justification that all management options have been exhausted.

**Partnership Working Outside of the Police**

- **CTCOs will:**
  - Support existing Intervention Providers & help identify potential new ones.
  - Provide to Local Authority Partners, where appropriate, details of the Police Counter Terrorism Local Profile (CTLP).
  - Work with Partners to develop a common understanding of roles & responsibilities, thus empowering specified agencies & other Partners to fulfil their Prevent Duty.
  - Support Prevent co-ordinators, regional further & higher education co-ordinators, regional health Prevent leads & regional NOMS Prevent co-ordinators in carrying out their work.
  - Wherever possible, support Partners with targeted engagement in order to help improve their processes and increase the quantity and quality of referrals into Prevent.
  - Work with Partners within multi-agency boards driving the Prevent program, (e.g. Contest boards, Prevent boards, Prevent steering groups).

**Partnership Working Within the Police Family**

- **CTCOs will:**
  - Work with Police Partners to assess and monitor community tensions particularly after executive actions and CT consequence management processes.
  - Support CTP Partners outside of Prevent in the management of their cases where they intersect with Prevent policing.
  - Provide support in the production of Counter-Terrorism Local Profiles (CTLP) and assist Partners with action plan development and the delivery of objectives and activities outlined.
  - Promote, encourage and support the delivery of Prevent with police staff and officers across the force or region (Prevent Champion / SPOC network, training etc.) to fulfil its obligations under the CTSA 2015.

- Support Pursue Operations, acting as a Prevent subject matter expert and tactical advisor around wider Prevent safeguarding issues for families and RSOIs.
- Deploy as a Prevent Contact Officer at the time of executive action (where relevant training has been completed).

**Community Engagement**

- **CTCOs should:**
  - Identify, engage and maintain relationships with key individuals, institutions and groups within the community wherever necessary to:
    - Promote and support the delivery of Prevent at a local and national level.
    - Support community resilience building, to challenge extremist and terrorist ideologies.
    - Invite carefully selected (and 'vetted') community members, where appropriate, to join Regional CT Advisory Groups (R-CTAG).

**Additional Training**

- **CTCOs may require additional specialist skills or training. As such, they are encouraged to seek the following where possible:**
  - PND.
  - COSII.
  - NCIA.
  - CT / Prevent Contact Officer.
  - CT / Prevent Consequence Management.

# Section 6 – CTCO Supervisor: The Role

## What are CTCO Supervisors?

Refer to the CTCO Guidance document for a more detailed breakdown of the following areas.

CTCO Supervisors are any officer or member of police staff who are in a supervisory rank and who have direct line management responsibility for CTCOs.

Non-supervisory ranks (e.g. constable or lowest band police staff) should never undertake the role of CTCO Supervisor.

Acting ranks are acceptable providing it has been officially sanctioned by the local force.

**Basic Requirements**

- **CTCO Supervisors will:**
- Be vetted to at least Security Clearance (Enhanced) (SC(e))
- Complete the National Prevent Foundation Course (NPFC) as soon as practicable of starting role or complete online course (in development).
- Have supervisory access to the PCMT and CMIS, an open source terminal (where possible) and NCIA (where possible).
- Have current force-led officer safety and first aid training (or equivalent) for staff and officers (if working in a public facing role).
- Ensure that all members of the team have received the required training to effectively risk assess, manage cases and access appropriate systems.

**General Duties**

- **CTCO Supervisors will:**
    - Support & manage CTCOs day-to-day.
    - Bear joint responsibility for CTCO decisions within PCM.
    - Supervise and quality check all CTCO PCM work & ensure its timely completion.

**PCM Basics**

- **CTCO Supervisors will:**
    - Allocate all received referrals, ensuring that regular updates on all PCM action or decisions are recorded on the PCMT.
    - Supervise DIFs completed for PGAs, ensuring they are completed within 5 working days of receipt from FIMU.
    - Ensure all referrals received by CTCOs directly from Partners or members of the public are submitted to the FIMU for de-confliction and "Pursue Assessment" prior to any CTP-Prevent work commencing.
    - Supervise Gateway Decisions and their rationales, assess the suitability to close a case and apply the appropriate closure code from drop down boxes.

**Channel**

- **CTCO Supervisors will:**
    - Supervise CTCO decisions around suitability for Local Authority led management and ensure the prompt referral such cases to Channel Coordinators (or non-Dovetail equivalents).

- Ensure at least one CTCO attends each and every Channel Panel meeting as CT SME and fulfil the Police role as statutory partner, disclosing Police held intelligence necessary to make effective risk management decisions.
- Risk assess deployment of Intervention Providers (IPs) to a Subject.
- Identify risk escalation in Channel cases with potential IHM lead or Priority Operation. Refer to FIMU for urgent assessment.
- **Non-Dovetail:**
  - Supervise rationale for S.36 for Local Authority led management of referral within 20 days of FIMU de-confliction.
  - Supervise CTCOs completed VAFs.
- **Dovetail:**
  - Ensure CTCO provides all relevant data / information / intelligence to LA Channel Coordinator (LACC) in a timely manner for their ongoing management of the case.

**Police-led Partnership:**

- **CTCO Supervisors will:**
  - Quality assess and supervise every completed DIF.
  - Ensure all paperwork is uploaded to the PCMT in a timely manner, including PLP Panel minutes and actions. This means either copying the relevant information into the relevant case notes (marking them clearly), or, once the facility to store documents on the PCMT has been added to the system, physically uploading the relevant documents into the relevant casefile for storage.
  - Supervise rationales for S.36 Decisions leading to PLP management, within 20 working days of FIMU de-confliction.
  - Ensure continual reassessment of cases throughout the PLP process, including:
    - CTCOs assessment of Prevent relevant risks.
    - Agree the priority banding for the case.
    - Oversight & approval of PLP Case Management Plans (CMP).
  - Chair PLP Panels and ensure that:
    - Findings and recommendations of VSH are considered
    - Approved Intervention Providers are risk assessed before deployment
    - Activities/interventions within the CMP are to reduce Prevent relevant risks and vulnerabilities, and to safeguard Subject.

**Disruptive Activity:**

- **CTCO Supervisors will:**
  - Ensure appropriate disruptive activities are considered throughout the PCM process.
  - Coordinate with Partners to utilise their unique powers to disrupt and deter persons believed to be extremists[2] or people who escalating towards extremism, including events which support or promote extremism.
  - Ensure CTCOs capture evidence and build files to support the Local Authority to take safeguarding action, including Wards of Court.

[2] As per the CTP-Prevent operational definition of "extremism" and "extremists" provided within the CTCO Guide.

- Support CTCOs to explore opportunities to investigate and prosecute individuals of interest for non-TACT offences to undermine their status/credibility and limit their activity.
- Provide disruptive capacity to Pursue-led operations by completing tasks as directed as an overt response option.

**Outcomes and Closures**

- **CTCO Supervisors will:**
  - Ensure the correct closure code is recorded on the PCMT / CMIS.
  - Ensure any flagging used during management (PIW, PNC, NCIA, and local systems) is removed.
  - Ensure all policing activity has been accurately recorded on the PCMT / CMIS including the use of activity flags to show specific interventions.
  - Ensure closure of cases only occurs when the identified case priorities around risk and vulnerabilities have been addressed and any risk has been appropriately mitigated, or at least evidence and justification that all management options have been exhausted.

**Partnership Working Outside of the Police**

- **CTCO Supervisors will:**
  - Support existing Intervention Providers & help identify potential new ones.
  - Provide to Local Authority Partners, where appropriate, details of the Police Counter Terrorism Local Profile (CTLP).
  - Work with Partners to develop a common understanding of roles & responsibilities, thus empowering specified agencies & other Partners to fulfil their Prevent Duty.
  - Support Prevent co-ordinators, regional further & higher education co-ordinators, regional health Prevent leads & regional NOMS Prevent co-ordinators in carrying out their work.
  - Wherever possible, support Partners with targeted engagement in order to help improve their processes and increase the quantity and quality of referrals into Prevent.
  - Work with Partners within multi-agency boards driving the Prevent program, (e.g. Contest boards, Prevent boards, Prevent steering groups).

**Partnership Working Within the Police Family**

- **CTCO Supervisors will:**
  - Work with Police Partners to assess and monitor community tensions particularly after executive actions and CT consequence management.
  - Support CTP Partners outside of Prevent in the management of their cases where they intersect with Prevent policing.
  - Provide support in the production of Counter-Terrorism Local Profiles (CTLP) and assist Partners with action plan development and the delivery of objectives and activities outlined.
  - Coordinate the delivery of Prevent (activities, awareness and training) with police staff and officers across the force or region (Prevent Champion / SPOC network, training etc.) to fulfil its obligations under the CTSA 2015.
  - Develop strategies to support CT Operations and act as a Prevent subject matter expert / tactical advisor.

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

**Community Engagement**

- **CTCO Supervisors should:**
  - Identify, engage and maintain relationships with key individuals, institutions and groups within the community to:
  - Promote and support the delivery of Prevent at a local and national level,
  - Support community resilience building, to challenge extremist and terrorist ideologies,
  - Invite carefully selected (and 'vetted') community members, where appropriate, to join Regional CT Advisory Groups (R-CTAG).

**Additional Training**

- **CTCO Supervisors may require additional specialist skills or training. As such, they are encouraged to seek the following where possible:**
  - PND.
  - COSII.
  - NCIA.
  - CT / Prevent Contact Officer.
  - CT / Prevent Consequence Management.

# Section 7 – Prevent Referrals

Refer to the CTCO Guidance document for a more detailed breakdown of the following areas.


*Figure 2: How information first enters the PCM process.*

Regional Prevent Co-ordinators (RPCs), CTCOs and CTCO Supervisors should promote the use of the National Prevent Referral Form with all Partners in their area where appropriate.

There are a number of advantages to a single National Prevent Referral Form. The document ensures a minimum level of quality information directly relevant to completing a gateway assessment is provided, which will improve the quality of referrals overall. It also clearly signposts to FIMUs that CTCOs are the intended output for the referral. CTPHQ cannot mandate the use of these forms by Partners but RPCs and CTCOs can promote and support adoption in local areas. It is acknowledged that some partner agencies will have standard referral forms for wider purposes or processes that make it inappropriate to adopt the national form.

Where a partner or member of the public contacts a CTCO asking for advice on a matter not already referred (so perhaps as part of the "**Check**" stage of the "**Notice, Check, Share**" process), it must be:

**a)** made clear from the outset whether the partner / member of the public is making a referral or simply seeking advice, and;

**b)** made clear that if the CTCO's concerns are raised enough during the conversation, they may have to act upon the information given irrespective of whether it was not initially intended as a referral.

There is no simple definition of a Prevent referral. Where a partner contacts a CTCO asking for advice this may result in a referral however the conversation **must** end with a clear direction from the CTCO, preferably in writing over email, whether this has been recorded as a referral or simply advice given. This ensures no confusion between agencies as to whether an individual or institution has been referred to Prevent or not. Advice should not be recorded on the PCMT, however it may be considered good practice to retain a record on local systems or within a pocket book or similar.

- Where local practices (such as a MASH or other 'front door' processes) result in partner referrals being sent to a FIMU prior to local CTP-Prevent teams, FIMUs must consider early dissemination to CTP-Prevent teams to allow the recording of referrals on the PCMT at the earliest possible stage.
- CTCOs will provide acknowledgement to the referrer that a referral has been received. It is a matter for local teams as to whether more detailed information about the case is provided.
- All referrals and potential referrals received by a CTCO will be registered on the PCMT at the first point of receipt, even if this is pre-de-confliction by a FIMU. This ensures that referrals and Subject data are not 'lost' within the system during de-confliction.
- All referrals received directly by a CTCO must be submitted to a FIMU for de-confliction and Pursue assessment, if this has not already been carried out.

Referrals logged on PCMT at the earliest possible stage help to ensure accurate data in terms of volume of referrals from Partners and assists with clear identification of the original referral source. Acceptable practice for partner referrals includes sending them directly to the FIMU (marked as Prevent referrals), or sending them directly to Prevent Policing teams, who then log the case on the PCMT before submitting it to their FIMU for de-confliction and "Pursue Relevance" assessment. Where local practices such as MASHs make this impractical CT(i)Us and forces need to ensure that Prevent teams have a mechanism by which they are made aware of referrals at the earliest possible stage. This could be achieved by either asking Partners to ensure Prevent teams are copied into any referrals submitted to a MASH or similar, or by making a requirement of FIMUs to make an early dissemination to Prevent teams of any case clearly intended for Prevent.

- No CTP-Prevent activity must be carried out before de-confliction and assessment by a FIMU. The only exceptions to this are:
    - When the quality of referral is so insufficient that the referrer needs to be contacted to provide basic relevant information.
    - The FIMU specifically requests activity to assist in their assessment process.
    - Obtaining necessary basic biographical data from local policing systems or initial referrers.
- De-confliction is not considered complete until a date of de-confliction is provided by the FIMU alongside a reference number (e.g. NCIA reference or other internal log number).

These requirements ensure that all cases are Subject to de-confliction and that no activity is undertaken until this is complete. The requirement to obtain a reference number ensures de-confliction has been fully completed and avoids pre-emptive action.

- As per Annex B of the NSIM Guidance, referrals must be forwarded to the local CTP-Prevent team regardless of whether it is assessed to have no CT relevance by the FIMU. The only exception to this is when the referral outcome is assessed as a Priority Investigation or IHM Lead not suitable for Prevent. This also applies if the FIMU's RADO assessment is that there 'no CT relevance' at all.
- So FIMUs must pass on to Prevent all referrals that they deem **not** relevant for Pursue, but which:
    - Are submitted on the National Prevent Referral template in whatever form, or;

- Are clearly intended by the initial referrer for Prevent, and;
- Include an Individual, Institution or Ideological expression (e.g. an extremist or hate-based leafleting or stickering campaign, etc.) with either a potential vulnerability to being drawn into any terrorism related offending or activities, or which are Prevent relevant in any other sense (see the CTCO Guide's **"Prevent Relevance"** section for further guidance).

- Where a referral has been submitted on a National Prevent Referral template (in whatever form), the FIMU must attach this to the product disseminated to the relevant CTP-Prevent team following de-confliction and assessment.

These requirements ensure that the only referrals to Prevent that are not received by the local teams are those where the matter has escalated to the Pursue space. This means CTP-Prevent teams will be aware of all referrals which were intended to reach them.

- At the point of dissemination to CTP-Prevent, FIMUs should where possible provide full details of all research (excluding intelligence marked Secret and above) completed during assessment. This will include the NSIM minimum standard checks:
  - Secure CT Intel system.
  - Local Intelligence & Crime Systems.
  - Police National Computer (PNC).
  - Police National Database (PND).
  - CT Holmes.
- Some FIMUs complete more detailed checks than this, however these are the **minimum** required standards.

Where the FIMU dissemination process allows, FIMUs should provide actual details of the research carried out on referrals they forward on to CTP-Prevent. FIMU disseminations sometimes list the checks undertaken but not information discovered during those checks that may be relevant to Prevent assessments. In these cases, CTCOs must ask the FIMU for the relevant details. If this proves impossible, the CTCO will have to duplicate some the work of the FIMU and check the same records. A complete list of relevant background checks can be found in the CTCO Guide.

- Where a referral has an equal footprint across multiple geographical areas, the NSIM multi-equity process must be applied to identify the primary team who will manage the referral (in practical terms this will done by the FIMU during assessment and de-confliction). The predominant principle is that the case should be managed where the risk is. Inter-area conflicts within a CT(i)U should be referred to the RPC for a decision, where there are disputes between CT(i)Us the CTPHQ Prevent team should be contacted.

In rare situations where a Subject resides across multiple differing areas or is active across areas there is an existing policy under NSIM for dealing with such issues, this ensures CTCOs adopt the same approach. Such cases will be very rare and FIMUs should apply these rules during assessment.

- Where another part of the CT Network is requesting that CTCOs manage any aspect of CT risk, CTCOs and CTCO Supervisors must clarify whether this is a "tasking" or request for tactical help requiring Prevent practitioner expertise, or whether this is an actual referral into the PCM process. If it is the latter, the request should be treated as a Prevent Referral and subjected

to a PGA and the usual PCM flow and processes detailed within this policy. If the request is a discrete tasking for a particular and limited activity, that case still belongs to the other unit within the CT Network and does not have to enter the PCM process.

# Section 8 – Prevent Gateway Assessment

Refer to the CTCO Guidance document for a more detailed breakdown of the following areas.

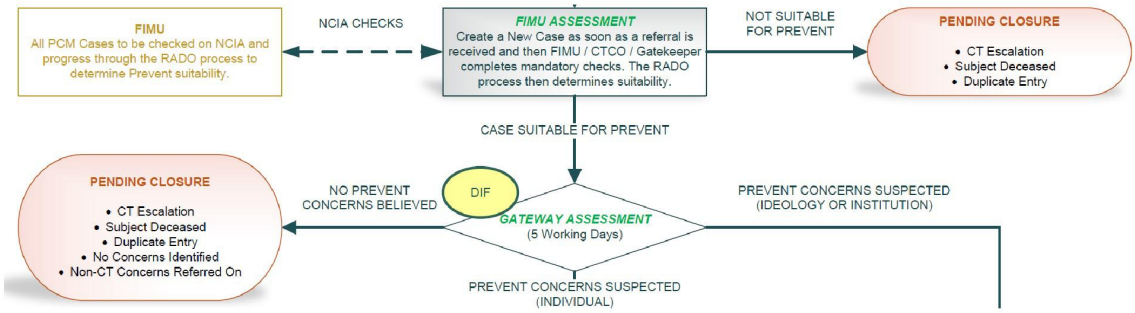


*Figure 3: The Prevent Gateway Assessment & Outcomes.*

The **Prevent Gateway Assessment** (**PGA**) is the name given to the initial screening & triage phase that CTCOs must complete on all de-conflicted Prevent referrals. It is a CTCO's **first use** of CTP-Prevent's dedicated threat, risk & vulnerability assessment tool, the **Dynamic Investigation Framework** (**DIF**). The PGA must be completed even for cases where the FIMU has designated the referral as containing no CT relevance.

- The PGAs must be completed within 5 working days of receipt from a FIMU, following de-confliction, or as close to 5 working days as is reasonably practicable within the unique circumstances of the Case. CTCOs and CTCO Supervisors should be aware of Cases that have exceeded this 5 working day period and update them accordingly.
- Only one PGA is ever completed in the lifetime of a single Case. It comes after FIMU de-confliction and must happen before any further screening, triaging or assessments by Local Authorities or other Partners.
- In order to complete the DIF form for a PGA, the Subject must be researched against the following intelligence indices either prior to, or as a fundamental part of, the PGA phase:
    - **PNC,**
    - **PND,**
    - **NCIA,**
    - **Open Source,**
    - **Local Crime & Intel Systems,**
    - **CT Holmes** (where available).
- These checks (with the possible exception of some Open Source) will have been completed already during FIMU Pursue assessment and de-confliction, and there is no requirement to repeat them *providing the results of these checks are known to the CTCO completing the PGA*, and there has been no **significant** time delay between the FIMU assessment and the completion of the PGA.
- **Contacting Partners:** In the majority of cases, Partner agencies should not be contacted in order to complete a PGA. Partners are involved during the *Information Gathering Phase* **after** a PGA has been completed and a Gateway Decision has been made. However, if a particular agency clearly has clear and significant relevant information regarding a referred individual that may negate the suspected the Prevent issue at hand, then this may be requested to aid the PGA process. This should not be regarded as a "business as usual" request, however.

- **Visiting the Subject:** A visit to the Subject is not recommended and is not necessary at the PGA phase. In very exceptional circumstances where both the CTCO and CTCO Supervisor deem a visit absolutely necessary (perhaps due to a pressing safeguarding concern) at the PGA stage, then a visit **may** be necessary, however consideration must be given as to who is best placed to carry the visit. In many cases a partner agency such as education, health or social services may have an existing relationship with the individual or family and may be better placed to attend, either by themselves or as part of a dual visit with a CTCO. **Any consent issues for Channel/Dovetail should not be addressed directly with the Subject at this early stage** unless the Subject themselves raise the issue. Even then, decisions should be explained and deferred until after a PGA Decision has been made and uploaded to the PCMT, a S.36 Decision has been registered, and the case has been referred to a Channel Panel.

There is recognition within the network that CTP-Prevent may not always be the best agency to make an initial approach to a Subject. An early visit by 'Counter Terrorism' Police may deter a Subject from further engagement and Partners may provide a mechanism by which any additional required information can be obtained without such issues occurring.

It is unnecessary to obtain consent for Channel at such early stages and it is considered best practice to discuss the matter of consent with Partners to identify which agency is best placed to make such an approach to an individual and their family. This may discussion may occur prior to, or even as part of the first Channel Panel.

- **Keeping Cases in PCM:** At the PGA stage, once a CTCO can demonstrate a *reasonable suspicion* of any Prevent relevant concern[3], the PGA Decision[4] will be to keep the Case within Prevent Case Management – within PCM.
- **Non-Dovetail Areas:** CTCOs do not have to decide at the PGA stage whether it is a Local Authority Led Channel case or a PLP case (although they *may*), because the next step will be to put the case into the *Information Gathering Phase* to develop the case further.
- **Dovetail Areas:** The CTCO needs only ascertain that there is a *reasonable suspicion* of a Prevent relevant concern and that the case in **unsuitable** for PLP, at which point the CTCO's Gateway Decision will be to refer the case to the LACC to complete Information Gathering, completed by the LACC. CTCOs are still expected to complete any outstanding police-specific Information Gathering for this process, including police databases, open source checks and other dedicated CTP-Prevent tactics.
- **Dovetail & Non-Dovetail:** Once a Gateway Decision has been made and Supervised, CTCOs must upload the DIF with rationale onto the PCMT. Any Institutions or Prevent-relevant Ideological expressions (such as a leafleting campaign) where the person responsible cannot be traced in the first instance[5], should be referred straight into the PLP process from the PGA stage. There are some instances where Individuals may be forwarded straight into PLP processes without consideration for Channel, but these are rare circumstances and detailed within the CTCO Guide.
- **Closing Cases from PCM:** If a CTCO can demonstrate a *reasonable belief* that there are no Prevent relevant concerns associated with the case, or that there is a Pursue relevant concern that needs escalating out of Prevent, the Gateway Decision can be to close the case from PCM altogether without forwarding on to the Information Gathering Phase. This must be

[3] Anything that may suggest that an Individual is being radicalised or vulnerable to being drawn, groomed or coerced towards any terrorism related activities. Please refer to the CTCO Guide for a detailed breakdown of "Prevent relevance", with examples.
[4] The title given to the decision made by CTCOs and CTCO Supervisors at the completion of the PGA phase. It is the decision regarding the next 'step' for the case: remaining within PCM or being closed from it.
[5] Such as a racist or extremist "stickering" campaign, for instance.

demonstrated very clearly and carefully in the closing rationale and approved by CTCO Supervisors.

- **PGA Decision:** Once uploaded to the PCM Tracker, the results of this first use of the DIF and PGA Decision arising from it are final. Neither can be altered or revisited, although the decision to keep a case open within PCM arising from for the PGA may be reversed in the *Information Gathering Phase*, if new information arises. The Gateway Decision for the case must always be submitted to a FIMU as part of the intelligence cycle **except** where the PGA Decision is to close the case AND the FIMU has already deemed the case a **RADO 6** during de-confliction.
- Where the Subject is a foreign national then consideration must be given to contacting the Foreign and Commonwealth Office (FCO), the Criminal Records Office (CRO) and Immigration Services to identify whether Subject has any convictions abroad or whether other intelligence about activities outside the UK is held.

# Section 9 – The Intelligence Cycle

Refer to the CTCO Guidance document for a more detailed breakdown of the following areas.

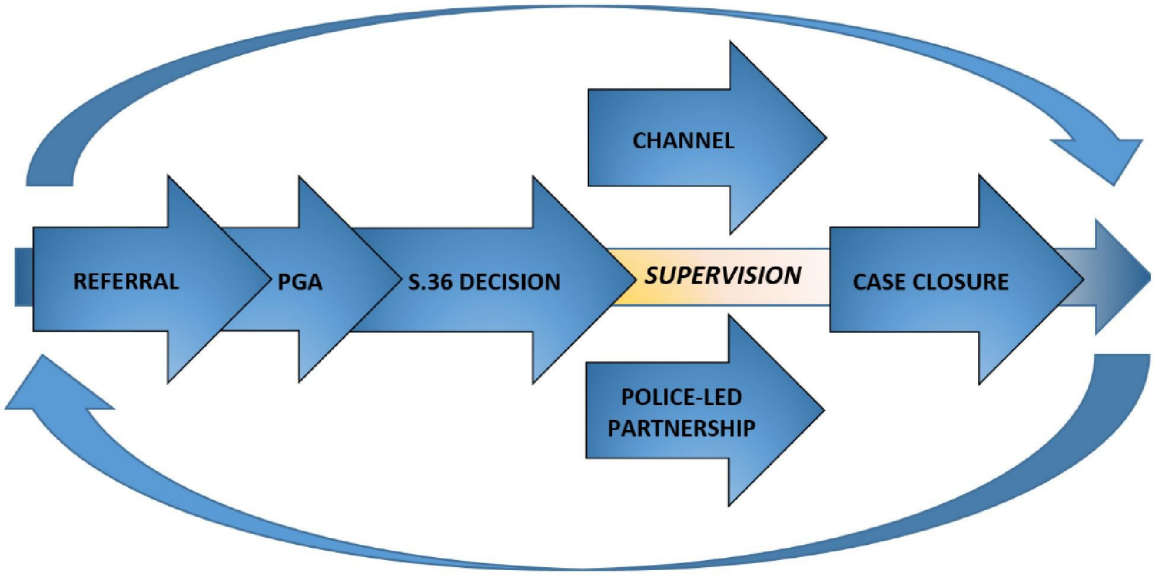


*Figure 2: The primary junctures for intelligence review*

- IMUs are the only part of the CTP Network that have the potential to see the whole intelligence picture. It is essential that intelligence obtained through the PCM methodology is passed back to the relevant IMU to allow for proper assessment of any terrorism threat and identification of dramatic escalations of risk. CTP-Prevent across the entirety of the UK network will be engaging predominantly with Fixed Intelligence Management Units (FIMUs) but on some occasions may also be working alongside OIMUs (Operations Intelligence Management Units).
- FIMUs must be informed of any significant changes in risk to a case or the case Subject throughout its lifetime in PCM, both Channel and PLP. This could include potential escalations in risk or threat around any issues of potential terrorism offending, (e.g.: concerning behaviours or contexts) within the case, or it could be the discovery of hitherto unknown contacts, addresses or phone numbers associated with the Prevent Subject that one might reasonably suspect could be relevant to wider CT picture held by a FIMU.
- This sort of information could arise at any point within PCM, but specific junctures to consider are: reception of the Referral, the PGA phase, the S.36 Decision after further Information Gathering, during Channel or PLP, and at the point of Case Closure.
- All biographical information obtained on a Subject or known associates during the Prevent process must be submitted to the FIMU.
- Any intelligence that has the potential to significantly change the DIF assessment, Case Management Plan or VAF must be submitted to a FIMU, this includes intelligence obtained through attendance at a Channel Panel or other partnership interaction as well as DIF or VAF assessments. It must be made clear on the intelligence submitted whether the risk in the case is escalating, de-escalating or remaining static. **This must be undertaken for both PLP and Channel cases.**

- If no other submissions have been made to a FIMU then an up-to-date summary should be submitted to the FIMU at least every 3 months.

These conditions ensure a regular flow of intelligence back into a FIMU throughout the lifetime of a case. Submission of VAFs and DIFs ensure the FIMU are cited on the risk assessment and how it is changing.

- For Channel cases, all relevant intelligence necessary for the effective management of risk must be shared with the Channel Panel and Chair.
- CTCOs must consider adding a flag (or nearest equivalent for forces which do not use 'golden nominal' systems) on local force system(s) to identify interest in Subject.
- All interactions between the Subject within PCM and CTP-Prevent / Partners must be assessed by the CTCO and any relevant intelligence reviewed and if appropriate submitted to a FIMU (e.g. missing person reports, crime reports etc.).
- All CTP-Prevent teams should have access (directly or via FIMUs or Force Intelligence Units) to the Police National Database (PND) to allow regular checks with other UK Police Forces to see if Subjects have come to notice elsewhere in the country.
- Where necessary, the CTCO must make further enquiries in relation to crime investigations, missing person enquiries or other non-CT policing incidents in order to ensure they have a full understanding of the relevant incident, including any intelligence products that have been generated (e.g. cell site data, phone downloads etc.)
- Any intelligence received or generated which is relevant or potentially relevant to another force must be transferred to them through the local force transfer process (e.g. an intelligence report marked up as suitable for dissemination to another area).
- For any Subjects who show a propensity to travel to areas of conflict or who are juveniles, consideration must be given to requesting CTP-POC create a Ports Intelligence Watchlist (PIW) entry.
- Where a PIW request is made CTCOs must ensure that both CMIS (where appropriate) and PCMT records clearly articulate the travel risks and any other relevant information staff at ports may require in order to make a decision under schedule 7 of the Terrorism Act 2000 or other relevant legislation.

PIW markers are not intended to generate specific activity (e.g. to stop a person travelling). Where the risk is such that a person should be detained at the border or have documentation seized CTP-POC should be contacted for advice as there are other type of flagging available which will generate different action from colleagues at Ports.

# Section 10 – Channel Cases

Refer to the CTCO Guidance document and the Channel Guidance (available on CTnet) for a more detailed breakdown of the following areas.

- Channel is the **Local Authority** led, multi-agency Prevent programme, designed to support and safeguard those who are at risk of being radicalised, groomed, coerced or otherwise drawn towards any unlawful terrorism related activities within the UK. Channel is the primary mechanism for managing and supporting Individuals entering into Prevent, after decisions under S.36 of the Counter Terrorism and Security Act 2015.
- More information can be found in the CTCO and CTCO Supervisor role profiles sections of this document, and within the CTCO Guide, but in overview CTCOs are responsible for:
    - **Non-Dovetail**: identifying Individuals that there are reasonable grounds to **believe** are *"vulnerable to being drawn into terrorism."*[6] This is the culmination of the Information Gathering phase and initiates the S.36 Decision to refer these Individuals to the Channel Panel *"for an assessment"*[7] on behalf of *"the Chief Officer of Police"*[8] in the CTCO's Force area.
    - **Dovetail:** identifying Individuals that there are reasonable grounds to **suspect** are *"vulnerable to being drawn into terrorism"* during the PGA phase, then passing these cases straight to the Dovetail-site Local Authority Channel Coordinator (LACC), who will complete the *Information Gathering Phase* (which the CTCO plays the police-specific role within) and then make the S.36 Decision.
    - **Dovetail & Non-Dovetail:** Representing the Police at every Channel Panel[9] and for updating the Panel on the Subject's risk of terrorism offending (which remains with the Police) and any other relevant intelligence / policing issue affecting the Subject that can be shared with Partners.
- Individuals who are a currently under covert or overt investigation by Pursue, or who are the focus of a current covert investigation, cannot be a Channel case and are unlikely to be appropriate for the PLP processes either, other than in the most exceptional circumstances. Please refer to the CTCO Guide for further guidance.
- **Dovetail Sites**:
    - Cases assessed as potentially suitable for Channel must be referred to the Local Authority LACC **within 5 working days** of receiving a de-conflicted referral after the FIMU assessment, or as close to this as is reasonably practicable.
    - The decision to refer to the LACC must be endorsed by a CTCO Supervisor. This must be recorded on the PCMT.
    - CTP-Prevent must ensure that all relevant Police data and intelligence is available to the LACC, who will create the initial VAF.
- **Non-Dovetail Sites:**
    - After the PGA Decision has been made, CTCOs will manage PCM cases on the PCMT throughout the Information Gathering process with Partners (after the PGA phase),

[6] *CTSA S.36 (1 & 3).*
[7] *CTSA S.36 (2)*
[8] *CTSA S.36 (3)*
[9] *CTSA S.37 (1b)*

until such a time as they are ready to make a S.36 Decision, although this must be **no more than 20 days** following FIMU de-confliction and assessment.

- At this point, the CTCO must complete the first VAF, create the CMIS record and ensure the minimum standards for data entry are complied with as per CMIS standards.

Within Dovetail sites the LACC will take responsibility for creating and maintaining the CMIS record and completing the VAF. For non-dovetail sites this responsibility remains with the Police.

- All CTCO decisions on CMIS and the PCMT must be endorsed both on the PCMT system and CMIS by a CTCO Supervisor. This **does not** mean that every routine entry made by CTCOs requires Supervisor endorsement, with the caveat that Supervisors and CTCOs share **joint** risk around case activities recorded on the PCMT.
- CTCOs will attend every Channel Panel held within their local authority area as a statutory partner and fulfil the role as outlined in the current Channel Guidance.
- In all cases the CTCO must ensure that the LACC, Channel Panel and Channel Chair are supplied with all relevant Police data and intelligence necessary to allow the panel to effectively the manage the risk in the case.
- The CTCO must ensure that **all** relevant intelligence obtained through the Channel process is submitted to the FIMU.
- In cases where there are reasonable grounds to suspect the CT risk is escalating to the point where it may satisfy the requirements of an IHM lead or Priority Investigation, the case must be discussed with the local FIMU and consideration given to removing it from Channel management. Whilst approval of the Channel Chair should always be sought in such circumstances, in the event of a dispute, CTP-Prevent retain an executive power to remove such cases from Channel.
- Where a Channel Panel rejects a case as unsuitable, the CTCO must consider whether the issue that brought case into Prevent still remains[10]. If so, then it must be dealt with as a PLP case. Where there is no CT risk but a safeguarding risk remains, the case must be exited to the appropriate safeguarding service (e.g. local MASH).
- Where a Channel Panel has accepted a case and subsequently closed it, should the CTCO believe that a CT risk or a serious enough Prevent issue remains, consideration should be given to whether the case should be dealt with as a PLP case or exited to a safeguarding function such as a MASH.
- Except where the CT risk has escalated, the Police cannot remove a case from Channel without the agreement of the panel. Where there is a dispute between the Police and other agencies on this issue it should be recorded on the PCMT. If the dispute cannot be resolved between CTCO Supervisors or 2nd line managers, then it should be referred to the Regional Prevent Co-ordinator or their deputy.
- The CTCO must risk assess all deployments of Intervention Providers (IPs). This assessment must focus on whether the Subject being deployed to poses any risk of harm to the IP as opposed to an assessment of general CT risk.

[10] Bearing in mind that Police hold, and have final say over, CT risk.

- Any intervention or action by Police or a Partners must be recorded on the PCMT and CMIS in the relevant places. If no suitable option or in a drop down menu exists to record the nature of the intervention, an entry **must** still be made on the notes sections.

# Section 11 - Police-led Partnership Cases

- Refer to the CTCO Guidance document (available on CTnet) for a more detailed breakdown of the following areas.
- **What is Police-led Partnership (PLP)?** PLP concerns the management of individuals, groups or institutions that are not suitable for Channel, but which have identified Prevent-relevant issues requiring support or mitigation, led by Police but working in partnership with other agencies.
- **Multi-Agency Working.** The fundamental basis of Prevent is multi-agency (or partnership) working to safeguard individuals and the public, in order to prevent terrorism related offending. The Prevent Duty Guidance requires Police to work: "in partnership with other agencies including the local authority" and to, "consider appropriate interventions, including the Channel programme, to support vulnerable individuals", with "vulnerable individuals" in this context refers to people who are "vulnerable to being drawn into terrorism", although this vulnerability may be exacerbated or caused by a combination of other complex needs.
- **Channel remains the preferred route for all individuals entering into Prevent**. However, Channel support is overt and voluntary. As such the programme is unsuitable for some cases. These cases can include, but are not necessarily limited to, the following scenarios:
    - The vulnerable individual refuses to engage with any of Channel's voluntary support plans.
    - The individual is a "hardened" extremist / radicaliser / extremist groomer whose activities need disrupting[11].
    - The case involves institutions, venues, or "leafleting / stickering" activities (etc.) that have Prevent relevance[12] but where no specific individuals can be identified for Prevent support or intervention.
    - There is a direct and concerning connection between the individual and an ongoing Pursue case[13]. This could prevent that individual being supported through overt and voluntary processes of Channel because:
        - Doing so may compromise national security, or;
        - There are case-specific restrictions on information sharing with non-Police Partners, or;
        - Referring to Channel would create an unacceptable risk to the safety of any individuals involved with that Pursue case, or the potential Channel case.
- **What PLP does:** where it is not suitable to manage an individual within Channel, or where an identified institution or group have Prevent relevant issues, the PLP process will provide management through disruptive activities, or multi-agency support, or a combination of these.

[11] Such as for Prevent-relevant ASB or criminal offences that fall **below** the IHM threshold for an escalation out of Prevent into the Pursue space.
[12] Refer to the CTCO Guide for examples of Prevent relevant vulnerabilities and risks.
[13] For instance, the individual may be a family member of an SOI currently under covert investigation, and referral to Channel may "tip off" the SOI, potentially placing the SOI's family members, or even the investigators themselves, at an increased risk of harm.

- **PLP Panels:** Though led by Police, PLP Panels are likely[14] to involve appropriate non-police Partners (such as the Local Authority). Partners might:
    - have ongoing contact with (and knowledge of) the individual being discussed, or;
    - they may be able to provide professional or subject matter expertise around safeguarding and mentoring, or;
    - for cases that require this approach, they may be able to provide disruption opportunities not normally available to Police acting alone[15].
- **Prior to PLP Panel Support:**
    - For cases referred to PLP straight from a Prevent Gateway Decision, CTCO Supervisors must ensure that there is a completed DIF with a full and clear rationale uploaded onto the PCM Tracker detailing the reasons.
    - For cases referred to PLP after Information Gathering, CTCO Supervisors must ensure that there is a completed DIF with a full and clear rationale uploaded onto the PCM Tracker detailing why the S.36 Decision (CTSA 2015) was to not refer the individual to a Channel Panel.
    - For cases that are being referred out of Channel cases into the PLP process, CTCO Supervisors must ensure that the closing VAF is extended into an opening PLP DIF, with a full and clear rationale uploaded onto the PCM Tracker detailing why the case could not stay within the Channel programme.
- **PLP Attendees & Chairs:**
    - Police must Chair PLP Panels. Wherever possible, PLP Chairs must be Sergeants / CTCO Supervisors or above, and the PLP Chair should not be the CTCO managing the cases discussed at the Panel[16].
    - Although the attendance of Prevent Coordinators may be beneficial for PLP Panel meetings, it is recognised that this may not be possible in every region nor for every Panel meeting.
    - It is good practice to involve Channel Chairs, where appropriate, at PLP Panels (in a non-chairing capacity) to offer advice and/or assist in the management of PLP cases where:
        - the individual concerned is suitable for Channel but rejects the programme, refusing to accept or engage with Channel support plans, or;
        - the CTCO & CTCO Supervisor have assessed that an individual being managed in the PLP Panel has decreased in risk / sensitivity to the extent that Channel is becoming the more appropriate case management pathway[17].
- It is good practice for PLP Panels to comprise of the same Members as Channel Panels. However, each PLP Panel must be constituted to meet the needs of the case, so there may be occasions where it is inappropriate for some (or all) regular Channel Panel Members to be present at a PLP Panel, depending upon the sensitivities of the cases in review. The

[14] Multi-agency working is the foundation of Prevent, and each PLP Panel will be constituted to meet the needs of its Subject. It **may** be unnecessary or inappropriate to involve safeguarding Partners for a PLP case requiring only very specific Police disruptions, or disruption Partners for a safeguarding case.
[15] For example: Social Services, UK Border Agency, Environment Agency, DVLA, National Crime Agency, Trading Standards, HMRC, Fundraising Standards Commission, the Intelligence Services, (etc.), could all be relevant Partners at a PLP Panel involving disruptive measures. All Panel Members should be invited on a case by case basis, as appropriate to the case at hand.
[16] It is recognised that this may not be possible across the entirety of the Prevent Policing network due to operational and/or staffing pressures.
[17] It is recognised that some Channel Chairs may wish to remain "independent" of the PLP Panel process, perhaps because they feel that doing so will better allow any future referral from the PLP process to Channel to be assessed entirely "neutrally" or at "face value" on the merits presented. This is the prerogative of the Channel Chair.

PLP Chair will decide and explain, on a case-by-case basis, who should be present at a PLP Panel and in what circumstances, and this must be recorded along with a rationale on the PCMT.

**PLP Panel Arrangements:**

- PLP Panels must operate separately from Channel Panels and PLP cases must not be heard as *Any Other Business* (AOB) at the end of Channel Panels.
- It is recommended that PLP Panels are held directly after Channel Panels wherever possible, particularly if relevant Partners are gathered together. It is recognised that this may not be possible across the entirety of the UK Prevent network and that alternative local arrangements might be required. These must be recorded on the PCM Tracker within the notes of each case.
- Where a PLP Panel cannot follow directly after a Channel Panel, the PLP Chair will decide where and when a PLP Panel will take place. Necessity may dictate that some PLP Panels need to sit at short notice.
- Where PLP Panels follow directly after Channel Panels, there must be no "overlap" between Channel and PLP cases. The Channel Chair will state clearly when the Channel Panel has finished, and the PLP Chair will state clearly when the PLP Panel has commenced. This should be clearly recorded in both sets of meeting minutes / actions.

- **PLP Panel Chair during Panel meetings:**
  - Identify anyone who should not be at the Panel.
  - Pass on the apologies of invited Members who cannot be present.
  - The PLP Chair will ensure that independent PLP Panel agendas, minutes and actions are generated.
  - The PLP Chair will ensure that all relevant activities arising from previous PLP Panel meetings concerning open cases are reported back to the Panel for discussion.
  - The PLP Chair will ensure that Police retain all records on the PCM Tracker, within the relevant cases. External Partners to the Police must not keep documents generated by the PLP meetings.
  - The PLP Chair will ensure that all actions and minutes arising from the PLP Panel are provided in a timely manner to the responsible CTCOs for the cases discussed.
  - The responsible CTCOs will update the relevant case on the PCM Tracker with the minutes and actions resulting from PLP Panels, along with all other relevant details and outcomes.

- **PLP Data Sharing Agreements:**
  - Data sharing between regional or force CTP-Prevent and Local Authority partners is permitted, and in some cases required, through existing legislation.
  - Irrespective of the above, data Sharing Agreements (DSAs) should be considered best practice within the PLP process.
  - DSAs streamline the information sharing process, laying out mutually agreed parameters to the uses, storage and deletion of the information shared. It is the responsibility of each region or force area to establish whether a PLP-specific DSA with Partners is required, in addition to DSAs that may already be in place for Channel Panels. There is an editable DSA template available on the Ctnet.
- **Data Protection Impact Assessments:**

- DPIAs are a legal requirement pursuant to s.64(1) DPIA where: "a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment."
- CTPHQ Prevent has established that a separate DPIA for PLP for every region every region or force is unnecessary in this case. We are in the process of agreeing the terms of a single national DPIA for CTP-Prevent as a whole, which includes PLP processes, the PCM Tracker and its uses.
- The PCMT is the only system upon which PLP Panel information will be stored and the information will continue to be used only for PLP (and in some cases Channel) cases. CMIS and the PCM Tracker are being merged into one database and information management system, so the DPIA will incorporate the uses for both systems.

# Section 12 – Assigning Priority to PLP Cases

**PLP Case Management – Prioritising Cases**

Please refer to the CTCO Guide for further detail. Every case entering PLP needs to have a priority level assigned to it. These are:

- **High Priority (Red)** – This rating is assigned to any Case that suggests potentially higher, urgent or imminent threat, risk or vulnerability factors, e.g.:
    - Any unmitigated Escalation or Mobilisation factors (noted in the DIF).
    - **Harm** – there is an apparent, imminent or escalating risk of harm to self or another.
    - **Mental Health** – the Vulnerability Support Hub or other MH professionals have identified urgent concerns.
    - **Time-Lock** – there is a deadline (like upcoming foreign travel) before which any concerning questions need to be answered.
    - **PURSUE Relevance** – This reflects the possibility that an individual involved in planning low-level, non-violent, terrorism offences (such as a groomed young person planning to travel to a conflict zone) **may** be recommended for inclusion in Prevent. However, anything that a CTCO or CTCO Supervisor suspect to be PURSUE-relevant. Bear in mind that if you suspect a case might be PURSUE relevant, your first goal is to escalate it through the FIMU as a potential lead, so the case is very unlikely to stay within Prevent.
    - **Professional Judgement –** anything that CTCOs & CTCO Supervisors believe to be particularly concerning within the unique context of the Case. Includes anything that officers believe might develop into, or encourage, critical or major incidents, or anything posing a significant risk to the reputation of Prevent or the operation of Policing processes more generally.
- High Priority Cases should ideally be looked at every week until the specific high priority factors are mitigated. At the minimum, a new DIF assessment MUST be completed (along with any updates to the CMP, CTCO Supervisory review and sign-off):
    - At least once every 4 weeks, or,
    - Before any PLP Panel meetings, or,
    - After any concerning changes in the Individual's complex needs, or,
    - After any other significant changes in the Individual's life more generally.
- **Standard Priority (Amber) -** This rating is assigned to any Case that suggests, within the professional judgement of the CTCO & CTCO Supervisor, moderate, developing or inferred risk / vulnerability factors, e.g.:
    - At least one Prevent-relevant factor/indicator identified through the DIF that the CTCO suspects requires further work.
    - Anything else that the CTCO and CTCO Supervisor agree requires work and/or corroboration, within the particular context of the Case.
- Standard priority Cases should generally be worked on every week or so until the specific standard priority factors are mitigated. However, at the barest minimum, a new DIF assessment MUST be completed (along with any updates to the CMP, CTCO Supervisory review and sign-off):

- At least once every 8 weeks, or,
- Before any PLP Panel meetings, or,
- After any noted change in the Individual's complex needs, or,
- After any other significant changes in the Individual's life more generally.

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

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

- Monitored cases must be shown as open. There are no fixed timelines around Monitored Cases. It could be quite a short period. Timelines need to be decided and justified between the CTCO Supervisor and CTCO within the unique context of each Case. That said, Monitored Cases do need to be wrapped up and Subjects in this space either exited from Prevent altogether (if the Case priorities associated with them have resolved), exited into Channel (if appropriate and the Individual is willing), or exited from Prevent and escalated into Pursue if their CT risk has increased enough. Generally speaking, Monitored Cases should be reassessed:
  - At least once every 3 months, or;
  - Before any PLP Panel meetings, or;
  - After any noted change in the Individual's vulnerability, or;
  - After any other significant changes in the Individual's life more generally.

# Section 13 – Outcomes, Case Closures and Case Transfers

- **Closing Cases (General):** Cases within PCM (PLP, Channel and prior to these) can only be closed where:
    - The Subject is deceased[18];
    - There was no actual CT concern;
    - The Subject could not be located;
    - The case was escalated to the Pursue space;
    - There was no actual CT concern however there was a non-CT issue referred onwards.
- **Closing at PGA Phase:** Cases closed at the end of the PGA phase. PGA Decisions can **only** be made on the back of a completed and supervised DIF that demonstrates a reasonable belief that there are no Prevent relevant concerns.
- **Closing PLP Cases:** Additionally PLP cases can be closed where the risk in the case has decreased to a level where management is no longer necessary to prevent the Subject being drawn into terrorism related activity or the public from harm, i.e.:
    - **Three "Ds":** It can be demonstrated that the previously-relevant Prevent issues have been successfully **diverted**, **deterred** or **desisted**, and the Individual is consistently disengaging from involvement with concerning Individuals, Institutions, Ideologies or other extremist or CT-related issues.
    - **RPC Authority required:** CTCO Supervisors can authorise case closure for all PLP cases except where a case is closed with an unaddressed CT risk. With the permission of the Regional Prevent Co-ordinator, **some** Cases may be closed with Prevent issues remaining, or some low level CT risk remaining. Such cases must show a clear and detailed justification on PCMT as to why management should not continue and why escalation cannot be undertaken despite Prevent-relevant concerns / CT risk remaining.
    - **Monitoring PLP Cases Prior to Closure:** If it is necessary to observe the Subject for a longer period of time before judging the impact of management on risk then such cases must not be closed. Instead the case must be shown as Monitored by changing the priority banding to 'Monitored'. The case notes must be updated, a new DIF and CMP completed to show the frequency with which the case will be reviewed.
    - **Actions:** All relevant activities that have taken place during PLP case management must be selected within the PCMT Actions page and described in detail on the notes page.
    - **Closing DIF:** All cases under PLP Management must have a closing DIF completed and supervised at the point of closure.
- **Channel Cases:** Additionally Channel cases can be closed where:
    - The Channel Panel has adequately addressed all CT and Safeguarding concerns.
    - The Channel Panel (including the CTCO member) has determined that the Subject already has sufficient support in place to address all CT and Safeguarding concerns.

[18] Where an Individual has died whilst PCM, standard protocols around deaths after police contact should be considered. Please refer to the CTCO Guide for further guidance in this area.

- All cases under Channel Management must have a closing VAF completed and supervised at the point of closure.

Using reduction of risk as the main closure criteria is in line with other developed risk management processes. It ensures that cases are not prematurely closed and focuses on risk reduction and the impact of activity rather than closure after the activity itself (e.g. closing following arrest).

These requirements ensure that the risk is assessed at the end of management to confirm it is stable and not escalating.

- **Transferring Cases:** In the event of a case transfer between areas, the outgoing force must contact the new force at the point at which the move or potential move first becomes known.
  - The general principle is that cases should be managed wherever there is relevant vulnerability and risk, and the NSIM multi-equity principles should be applied.
  - In cases where a Subject is detained under mental health or immigration legislation in an area outside of their normal place of residence, the relevant areas should discuss the case and decide upon the area must suited to continue management of the case on the basis of risk. Where such cases are under Channel, transfers are not a Police decision and instead sit with the Channel Panel. In such cases Home Office Channel Guidance must be followed.
  - Any case transferring between areas must have an up-to-date DIF/VAF completed at the point of transfer by the outgoing force (with the exception of Dovetail cases in which the LACC will complete an outgoing VAF if appropriate).
  - The receiving force must complete a new DIF/VAF upon receipt of the case (with the exception of Channel cases in Dovetail area cases) and if it is a PLP case a new Panel should be organised and a new CMP must be completed and supervised reflecting the change in circumstances arising from the move between areas.
- **Review Closed Cases**: All cases that have been adopted into the PCM process must be reviewed by the CTCO and Panel (if one was convened for the Case).
  - Reviews happen at 6 months and 12 months from the point of closure. Where there is no formal process to flag the 6 and 12 month reviews within CMIS or the PCMT, other calendar notices should be set up to ensure that reviews take place.
  - At the point of closure, it is the responsibility of the CTCO to accurately record the closure on the PCMT to ensure review triggers are flagged at the appropriate time. This review process must be undertaken for **all** PCM Cases, Channel & PLP. This includes those cases that are adopted into Channel or PLP, but which are subsequently referred elsewhere.
  - Reviews should be completed within five working days of the relevant date, or as close to this as is practicable.
  - The review process should be informed by relevant information from Channel/PLP Panel Partners and Police systems, as well as changes of circumstances, relevant offending, current social care and known mental health issues, any concerns since case closure, and wherever possible and appropriate contact with the initial referrer. In any event, must involve the completion of a new VAF/DIF, depending on whether the case exited Prevent from Channel or PLP respectively.
  - Supervisors must read and evaluate all CTCO case reviews before final approval.

# Section 14 – Supervision

- CTCO Supervisors must be of at least the rank of Sergeant or Police Staff CTCO Supervisor (acting ranks are allowed providing the force has formally approved the acting rank). Constables and lowest Police Staff grades must never supervise cases.
- Supervision is mandatory for all DIFs, Police created VAFs, Closure Reports, Case Management Plans and Police generated CMIS and PCMT entries.
- Cases must be supervised with a frequency of no less than four weeks for High Priority Cases or eight weeks for Standard Priority Cases unless the case is monitored.
- Monitored cases must be supervised at least every three months.
- CTCO Supervisors should ensure that firstly the correct process is being followed under policy and then secondly that the process is completed to the required standard. This includes reviewing all CTCO uses of the DIF and VAF to ensure they have been completed to the required standard and that associated CMPs address all of the identified risks and that the proposed actions are specific, measurable, achievable, proportional and timely.
- 2nd line managers must ensure that they establish a process to review a proportional number of cases within their area to ensure a consistent standard of decision making, case management and supervision.

Return to Contents

# Appendix A – PCMT Process Map (Non-Dovetail)