OFFICIAL SENSITIVE

COUNTER TERRORISM POLICING

DATA PROTECTION IMPACT ASSESSMENT (DPIA)
Prevent Case Management Tracker (PCMT)

Classification	Official - Sensitive
Suitable for Publication?	No
Title	Prevent Case Management Tracker (PCMT)
Purpose	To deal with privacy issues and risks arising from data held on Prevent Case Management Tracker
Summary	Assessment of impacts arising from the processing of personal data in respect of Prevent Case Management information
Author	S.40(2) [redacted]
Version	3.0, (draft 8.6)
Supervisor	S.40(2) [redacted]
Creating Unit	CTPHQ - Prevent
Date Created	28 November 2025
Review Date	10 May 2025
DPIA Ref	DPIA 155

COUNTER TERRORISM POLICING

Version control

Version	Author	Completion date	Summary of changes
1.0	S.40(2)	07/01/2020	Draft
1.1	S.40(2)	08/06/2020	Amendments
1.3	S.40(2)	29/06/2020	Amendments
	S.40(2)	02/09/2020	Amendments
	S.40(2)	06/01/2021	Amendments
2.0	S.40(2)	27/01/2021	Amendment to page 11 and final version confirmed and approved
3.0, draft 4	S.40(2)	19/4/2022	Reflect the migration of the CMIS capability to PCMT, including use of the PCMT by Channel partners.
3.0, draft 5	S.40(2)	27/4/2022	Incorporates feedback from S.40(2) received by email dated 15/6/2022.
3.0, draft 6	S.40(2)	12/9/2022	Incorporates further feedback from S.40(2)
3.0, draft 7	S.40(2)	17/10/2022	Updated to reflect feedback from S.40(2)
3.0, draft 8	S.40(2)	28/2/2024	Updated to reflect feedback from Legal (S.40(2)
3.0, draft 8.1	S.40(2)	29/2/2024	Rephrasing in a couple of areas.
3.0, draft 8.3	S.40(2)	19/3/2024	Addresses feedback from S.40(2)
3.0, draft 8.4	S.40(2)	25/3/2024	Addresses feedback from S.40(2) including removal of annex D.

COUNTER TERRORISM POLICING

3.0, draft 8.5	S.40(2)	25/3/2024	Added a little more feedback on 'Channel-related' access control provided by S.40(2)
3.0, draft 8.6	S.40(2)	28/3/2024	Updated to reflect feedback from 'Data Sharing Agreement' involving HSG and CTPHQ.
3.0	S.40(2)	29.10.2025	Minor amendments to reflect CT investigation cases now being able to be held in Channel.
3.0, draft 8.7	S.40(2)	25/11/2025	Updated to reflect data being held on PMCT for family, significant others and associates family interventions pilot.

COUNTER TERRORISM POLICING

COUNTER TERRORISM POLICING

1. Introduction

1.1 Purpose

This document represents the Data protection Impact Assessment (DPIA) for the data processing activities undertaken on the Prevent Case Management Tracker (PCMT) application (enhanced to incorporate CMIS functionality).

It should be noted that Home Office has prepared a separate DPIA covering Channel data and use of the PCMT application hosted by CT Policing (CTP). Furthermore, where deemed appropriate for the protection of CTP interests, content from this document has been incorporated into the CTP DPIA for PCMT.

1.2 Background

1.2.1 Explain the project/initiative.

UK Policing has a specific requirement under S.26 of the **Counter Terrorism and Security Act (CTSA 2015)** to *"pay due regard to the need to prevent people from being drawn into terrorism"*[1]. For the purposes of this DPIA, Counter Terrorism Policing – Prevent (CTP-Prevent), is required to identify and help manage the risks and vulnerabilities around individuals primarily, but also around Institutions and Ideologies (or more specifically, extremist ideological expressions such as leafleting campaigns) identified as having a possible Prevent-relevant concern. Note individuals are referred to collectively by CTP Prevent as "Subjects".

"Prevent-relevance" suggests anyone who is "upstream" of any terrorism offending (as defined within the breadth of UK terrorism legislation) but where it is reasonable to believe after assessment that they are vulnerable to being drawn towards any such offending. The Prevent-relevant vulnerabilities can include, but are not necessarily limited to, concerns around Right Wing and Left Wing Terrorism (RLWT), Lone Actor, Anarchist and Single Issue Terrorism (LASIT), International Terrorism and religiously inspired terrorism.

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

COUNTER TERRORISM POLICING

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". UK CTP Prevent delivers on these requirements through Regional and Force based **Counter Terrorism Case Officers** (**CTCOs**), and their Supervisors, who together are responsible for identifying, managing and mitigating the Prevent-relevant threats, risks and vulnerabilities of Subjects referred to them, generally "upstream" of actual terrorism offending. CTCOs carry out Gateway Assessments into Prevent, which screen and triage cases to either remain in Prevent or be exited from its programmes. CTCOs also carry out more detailed multi-agency information gathering with CTP statutory partners on any case that they reasonably **suspect** may possess Prevent-relevant issues. If during this process CTCOs develop a reasonable **belief** that there are genuine Prevent-relevant concerns attached to the Subject of the case, they may refer the case to a Local Authority led Channel Panel or to a Police-led Partnership (PLP) Panel.

In January 2025 Channel policy changed, and now allows individuals who are subject to a CT investigation to access support in Channel. Historically they would have been placed into PLP. The investigations team will not have direct access to PCMT, S.24(1), S.31(1) [redacted]

Personal details of other individuals that have regular contact with the subject and may influence outcomes are also recorded such as parents, stepparents, siblings, close family, care givers etc. This will be covered in more detail below.

1.2.2. Explain the methods to be used.

1.2.2.1 Definitions

Prevent Case Management, or PCM, is simply the catch-all term used by CTP Prevent to describe **all** case management activities within Prevent, whether it is by Police or the Local Authority. The core activities of PCM are:

Processing Prevent Referrals: This is the initial receipt of a referral potentially suitable for PCM, having been "de-conflicted" with ongoing Pursue cases by an Intelligence Management Unit (IMU).

Prevent Gateway Assessment (PGA): Or simply the "Gateway Assessment", this is the term given to the initial screening & triage phase that CTCOs must complete on all de-conflicted Prevent referrals.

The Intelligence Cycle: Intelligence Management Units (IMUs) are the only part of the CTP Network that have the potential to see the whole intelligence picture. It is

COUNTER TERRORISM POLICING

essential that intelligence obtained through PCM is passed back to a Fixed Intelligence Management Unit (FIMU) to allow for proper assessment of any risk/threat and identification of escalation of risk.

Channel Cases: Channel is a Local authority-led, multi-agency Prevent programme, designed to support and safeguard people who are at risk of being drawn into terrorism offending within the UK. It is the primary mechanism for managing and supporting individuals entering into Prevent, after FIMU de-confliction and the Gateway Assessment phase. Note Channel panels are typically chaired by a senior representative from the Local Authority.

Channel Partners: In the context of this DPIA, this refers to HSG and Local authorities supporting Prevent through the Channel process.

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

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

Supervision: CTCO Supervisors have clear responsibilities at each stage of the PCM process, whether a case is managed within Channel or PLP.

As a general guideline, subjects suitable for management through the Prevent process include people who:

1) MAY be under a CT investigation;
2) MAY be under a police criminal investigation;
3) WILL have been assessed, first via the PGA and then on an ongoing basis, as having some form of Prevent-relevant vulnerability or risk.

In addition, family members, carers or significant others of Prevent subjects will also receive support as part of the Prevent process. This is known as family interventions work. By families and significant others, we mean the '*fundamental social group that provides support, care and guidance to its members, regardless of biological or social ties'.* The Intervention will consist of mentoring, advice, and signposting to help families and significant others understand radicalisation risks and build protective factors at home.

COUNTER TERRORISM POLICING

Channel is 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 Channel's voluntary support plans.
- The individual is an extremist / radicaliser / extremist groomer whose activities need disrupting.
- The case involves institutions, venues, or "leafleting / stickering" activities (etc.) that have Prevent relevance, 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 investigation. This could prevent that individual being supported through the overt and voluntary processes of Channel because:
  - Doing so may compromise national security, the prevention and detection of crime or public safety, 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.

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 provides management and mitigation through disruptive activities, or multi-agency support around, or a combination of these.

Though led and chaired by Police, PLP panels often involve appropriate non-police partners (such as the Local Authority). These 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.

Channel cases

The process adopts a multi-agency approach to identify and provide support to individuals who are at risk of being drawn into terrorism. Channel panels are held across all Local Authorities in England and Wales.

Information sharing is also carried out by statutory partners. These partners also attend the Channel Panels to discuss cases and build support plans. For further details on Channel Panels and partners, please refer to the Channel Duty Guidance (https://www.gov.uk/government/publications/channel-guidance).

The management of these cases is generally completed by Counter Terrorism Policing.

COUNTER TERRORISM POLICING

In support of Channel: The Home Office (Homeland Security Group) access data from cases for statistical, quality assurance, policy development and oversight purposes.

Individuals associated with a Prevent subject—such as family members, caregivers, or guardians—are not directly subject to the Prevent process; however, their data may be processed at certain stages. S.24(1), S.31(1) [redacted] In the information-gathering stage, partners may provide details about the subject that include relevant information about associated individuals, which is also recorded. When consent for Channel is required for subjects under 18, the identity of the consenting parent or guardian is documented. Additionally, if a family intervention provider is deployed, reports relating to family members are uploaded to the system.

However, it is important to note that the legal basis for processing family member or significant other data does not rely on consent, but in furtherance of Prevent duties and policing powers.

1.2.2.2 Applications

Prevent Case Management Tracker

Due to the vulnerable nature of the Subjects within Prevent and the multi-agency safeguarding focus of Prevent, PCM Subjects require management outside of the usual police crime and intelligence processes, and this is undertaken by CTP Prevent using the secure online PCM Tracker (PCMT) application hosted on S.24(1), S.31(1) [redacted]

The Channel Programme also uses the same instance of the PCMT application as CTP for its purposes rather than the 'old' CMIS system. Access by staff is done using corporate laptops (and/or desktop machines) provided by Home Office.

Access is available to all cases referred into Channel, including information provided by CTP, with the following exceptions: (i) Any note, file, activity that is marked as Police Only, (ii) The instructions information for the PAF [2], (iii) PLP Panels, and (iv) Case Management Plans.

Any updates to cases are accessible (immediately) via the PCMT application subject to Cases being closed - see below (or marked as 'Police only').

Key points regarding cases (and RRD policy):

- If Channel data were deleted from CTP view, a hole in the CT risk picture would occur and undermine CTP's ability to discharge its obligations to manage the CT risk an individual poses. This would be particularly problematic if CTP assessed that we have a policing purpose to retain data that HSG assessed that they did not have a lawful

[2] Prevent Assessment Framework (PAF)

COUNTER TERRORISM POLICING

reason to retain it and so deleted it. This means that CTP and HSG must be able to individually remove their access.

- Cases that enter Channel, if necessary, can be escalated by CTP into Pursue (where TACT offences are suspected) or PLP (if consent for Channel is refused or the risk is such they need to be managed outside of Channel). Therefore, cases do not always close direct from Channel because of a Channel Panel decision. If police disagree with a decision by a Channel Panel to close a case, the individual will be referred to PLP for continued risk management. The system must be able to account for cases moving out of Channel, in which case, HSG access to information will be limited to the Channel data only.
- As such, cases that are no longer required by:
  - Home Office / Channel - The case shall be marked as 'CLOSED' from a HSG perspective. Furthermore officers shall be bound by the SOP for 'Prevent Case Management' (HSG version) not to access the case (unless another referral for that individual is received). Note any access shall be logged and subject to audit. Note the Case shall be retained until it is no longer required by CTP (in accordance with RRD policy);
  - CTP - The case shall be marked as 'CLOSED' from a CTP perspective. Furthermore officers shall be bound by the SOP for 'Prevent Case Management' (CTP version) not to access the case (unless another referral for that individual is received). Note any access shall be logged and subject to audit. Note the Case shall be retained until it is no longer required by Home Office / Channel (in accordance with RRD policy).

S.24(1), S.31(1) [redacted]

Reporting capability (Tableau)

PCMT Reporting is provided by a Tableau server running on S.24(1), S.31(1) [redacted] It is used to provide a live view of data contained within the PCMT Application using charts, graphs, maps, grids and other presentation tools. There are a number of pre-created dashboards available within PCMT Reporting which provide national and regional overviews of Prevent Cases as well other local dashboards for obtaining Management Information and departmental access to specific sets of PCMT Data.

The Information available to users on PCMT Reporting is controlled by the Strategy Planning and Performance and Policy (SPP) Business Administrators who are also responsible for authorising users who require the ability to edit and publish reports and dashboards.

Access to PCMT Reporting will only be provided to those users who have a specific CT related business need to access Prevent Data and must be sponsored by a line supervisor who **must** be at least the rank of Sergeant or equivalent Police Staff member.

COUNTER TERRORISM POLICING

1.2.2.3 Data controller / Processor

Data controller

The Data controller for information in the PCMT application supplied by CTP officers / staff is the Commissioner (MPS)[3]. The Data controller for information in the PCMT application supplied by Channel is the Home Office.

CTP and Home Office share data via PCMT on a controller to controller basis, and in particular independently control the shared Channel data for their respective Approved purposes. Note CTP will only share information pertaining to Channel cases.

The Data controllers for CTP and Home Office process Approved data for their respective Approved purposes. It should be noted that the Purposes are related but different. Furthermore the Purpose for which CTP processes Approved data takes priority, and in particular where there is a need to disseminate data to Partners of CTP or retain shared data.

Data processor

CTP acts as a data processor for Home Office in that 'Channel data' is processed and stored using the PCMT application (S.24(1), S.31(1) Note a Data processing Agreement is contained in the Section 15 Agreement between CTPHQ and Home office. Pertaining to the use of the PCMT application.

CTP also acts as a data processor for Home Office with regard to specific PCMT functionality (and actions) which is not available to Home Office (but may be requested by Home Office), i.e.:

- Action a request from Home Office to delete a case that is no longer required by both CTP and Home Office (in accordance with their respective RRD policy). CTP staff shall make the necessary checks and delete from the PCMT application accordingly;
- Action a request from Home Office to delete a case that is no longer required by Home Office (in accordance with their respective RRD policy) but which is still required by CTP. For this type of request, the case will be made inaccessible to Channel staff using Role-based Access controls (RBAC), but will remains accessible to CTP staff for the Approved purposes, and until it is deleted in accordance with the CTP RRD policy. Note for the interim period it is asserted that the data is solely under the control of CTPHQ.

[3] The Commissioner (MPS) represents the interests of the wider Police community resourcing the Prevent scheme.

COUNTER TERRORISM POLICING

Data Sharing Agreement

An Information / data sharing agreement has been established between CTPHQ and Home Office to support the 'sharing' of information for the respective Approved Purposes.

Details of the Approved Data to be shared (together with any constraints) can be found in the Data Sharing Agreement at sections 2.2.4 to 2.2.8, however it is repeated here for ease of reading:

"Personal data (general):

- The name of any Data Subject;
- Age and date of birth of any Data Subject;
- Sex / Gender;
- In the case of children and young persons-Schools, Colleges, Universities and other education providers (connected to the Data Subject);
- Where relevant, locations of interest;
- Information pertaining to the relationships between Data Subjects;
- Relevant events or circumstances, including description of incidents and action taken;
- Any other information that is relevant to: (i) identifying and assessing the risks to a person, again as assessed on a case by case basis, and (ii) for the development of policy and review by Home Office.

The parties agree to share the following special categories of personal data to the extent allowed by DPA legislation:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Data concerning a natural person's physical or mental health or condition, sex life or sexual orientation.

The parties agree to share criminal convictions data as necessary to progress the Case, including but not limited to:

- Nature of concern/allegation/offence;
- Warning markers.

HSG has access to Tableau (S.24(1), S.31(1) for analytical reporting of Channel cases."

Finally, the classes of Approved data for sharing with Channel partners, including background details and references to actions by other Partners of CTP (where pertinent), shall permit an effective response to a Prevent referral to be provided. There are of course cases which remains Police-only, and this is for reasons stated at section 1.2.2.1 of the DPIA ('Police-led'); the SOP provides further detail.

COUNTER TERRORISM POLICING

1.2.2.4 Procedure relating to FOI and DPA requests

FOI and Subject Access Requests pertaining to information processed under the Prevent programme (using the PCMT application), shall be received via the following mailboxes:

- FOIA&DPArequests@met.police.uk (CTP);
- Channel@homeoffice.gov.uk (HSG)

Note this may include requests for:

- Access to records;
- Errors and/or proposed corrections to records;
- Deletion requests.

HSG and CTPHQ shall inform each other of FOI and DPA requests pertaining to a Channel case/Channel stats/data. Furthermore, both parties should then consult on the response with a view to agreement on the content.

A Standard Operating Procedure (SOP) for 'Prevent Case Management' shall be maintained by each of the Parties to whom requests may be made. Furthermore the SOPs shall detail the process for Parties to follow when receiving requests.

Note a copy of the SOPs (CTP and HSG versions) will be available via CTnet (also accessible from the S.24(1), S.31(1)).

1.2.3. Detail the personal data (including special category data) to be processed.

The following personal and special category data is stored on PCMT. We have organised the data into three sections, each containing only the minimum information required for processing (additional data may be captured).

Rows shown in *italic* indicate potentially sensitive data. Such data may be withheld from individuals requesting access, in line with applicable exemptions under the DPA or FOIA (as the case may be) – see also Part 3 of the DPIA.

Prevent Programme personal data

- Last Name;
- First Name;
- Middle Name;
- *Warning Description e.g. Violent / Drugs / Weapons;*
- Date of Birth;
- Age (calculated from Date of Birth);
- Address (note town and street, as a minimum)

COUNTER TERRORISM POLICING

- Gender;
- Country of Origin;
- Ethnicity;
- Religion;
- Educational Institution
- Employment type;
- Military affiliation;

Plus any additional relevant data.

Family members personal data

- First name
- Last name
- Middle name
- DOB
- Relationship to the Prevent subject

Plus any additional relevant data.

Associates personal data

- First name
- Last name
- Middle name
- Nature of association with Prevent subject

Plus any additional relevant data.

Case files may include:

- Subject biographical details, details of the referral that brought the Subject into Prevent, relevant information about the Subject provided by statutory partners, assessments and analyses of the Subject in context, minutes and actions from panel meetings and case management plans;
- Phone numbers; e-mail; social media usernames; occupation; primary language; languages spoken; immigration status; mental health status. Case files may also include additional relevant data relating to family members, significant others and associates', as indicated earlier in paragraph 1.2.3

COUNTER TERRORISM POLICING

Counter Terrorism Case Officers (CTCO) will upload Channel Panel meeting minutes and case management information discussing the progress of the case/subject.

1.2.4 Data storage

Storage and retention of data will be managed on the Prevent Case Management Tracker, hosted on the S.24(1), S.31(1)

Government Security Classification (GSC) should be adhered to when dealing with any information contained within PCMT. Any information shared to Police, Statutory Partners and 3rd Sector Parties should carry the relevant handling conditions in line with GSC guidelines.

Any information printed off from the PCMT should be managed, stored and disposed of appropriately as per GSC guidance. Handling conditions must accompany any information that is printed off the PCMT and be provided to the recipient.

See Annex A – Government Security Classification.

CMIS cases ('CLOSED')

Old CMIS case records which have been migrated over from CMIS prior to the launch of the enhanced PCMT will be stored in the Home Offices internal SharePoint system. This is in order to meet the Data Retention policy of 6 years. All servers based in UK.

1.2.5 Data processing

1.2.5.1 Application Ownership

The PCMT application belongs to the Mayor's Office for Policing and Crime (MOPAC) which is the statutory authority which governs the Metropolitan Police.

COUNTER TERRORISM POLICING

1.2.5.2 PCMT Roles

CT

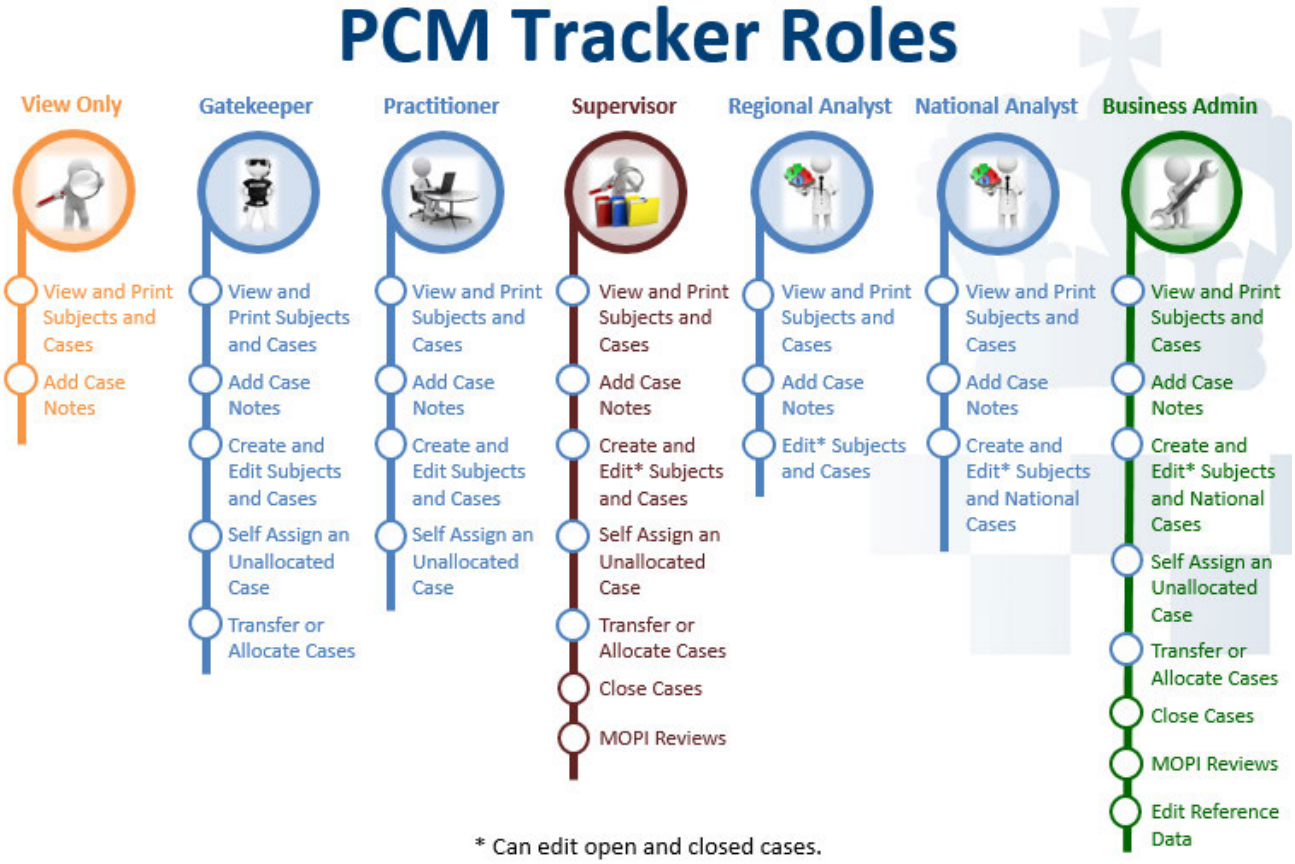


Figure 1: CTP-related roles on PCMT application

**View only operators do not require any formal training to use PCMT as they DO NOT manage cases on the system. FIMU and Prevent staff who have not received mandatory training are provided with view only access to the system accompanied with a Quick Reference Guide to use the application. All searches are completed on a need to know basis and relevant to their individual roles.*

As of 11/12/2025 , these are the current CTP PCMT user numbers per user role:

COUNTER TERRORISM POLICING

User Role	Total
Business Administrator	18
Gatekeeper	76
National Analyst	11
Practitioner	386
Regional Analyst	83
Supervisor	303
Authorised PCM Tracker User (View Only)	1671
Total	**2548**

HSG

Staff in HSG Counter Terrorism Analysis and Insight require regular access to PCMT - The team produces national statistics, which takes place on an annual basis. Note the information accessible to HSG staff shall be restricted to those cases which have been referred into Channel on a S36 CTSA decision.

Staff from the Channel team (HSG) require regular access to cases that have passed the S36 decision for referral to Channel (only) - The team may review the quality of panels and case management; and use trends in data to develop new policy. They also require access to fulfil their obligation to inform seniors and ministers following a terrorist incident and persons of interest's interaction with the Channel programme.

HSG's position regarding data associated with Channel cases, is that it is necessary and proportionate for them to have access to all of the data for the cases that have gone through Channel (including police data); note this position was 'supported' by Legal Counsel. Finally, further details (with justification) are being sought from HSG in respect of particular user groups.

Note the QA team within the Prevent Directorate provides quality assurance – with reference to the Channel Duty Guidance (issued under CTSA 2015) and policy documents - in relation to the performance of Channel panels in two main ways:

1. Providing advice/ guidance on specific, active cases to practitioners where appropriate (both on request and on the HO's own review of Channel cases), and

2. Carrying out checks on active cases, both routinely and in response to particular operational issues or demands.

COUNTER TERRORISM POLICING

Access to only statistical information (e.g. what I understand "Tableau" to mean be) would not be sufficient for either but especially for (2). Equally, access to cases on an ad hoc basis / on request of specific case details would be impractical for the latter - at (2) - and could frustrate the purpose of the checks, which are intended to be ongoing and routine (in addition to any targeted checks). In carrying out these checks, the QA team are putting themselves into the shoes of the panel and it is considered that they should have the ability to consider the same information.

The Home Office works directly with local authorities in carrying out this QA function since they chair Channel panels and, as such, it is difficult to see CTP's role in determining whether and when the QA team can access the relevant details to scrutinise a particular Channel case if general access is not provided. Such gatekeeping seems impractical, given the scope and routine nature of QA checks.

An example of the importance of checks from an operational policy perspective is that, following a series of Channel cases taking their own lives in a particular region, the QA team (which is a limited cohort of security cleared officials) were able to undertake a "deep dive" in relation to that region's caseload. This allowed them to assess the extent to which the risk of suicide was being considered and appropriately handled where a risk was identified in that region's case management.

The QA function is considered vital to the HO's responsibility for the Channel programme and its ability to ensure that practitioners have the tools they need to deliver Channel and that the programme is delivered correctly, seeking to reduce vulnerability to being drawn into terrorism whilst managing other risks to the individuals concerned consistently and effectively across the various areas.

A request was received by CTP (March 2024) for 46 staff from HSG to have access to PCMT.

Local authority staff

Local authority staff supporting channel cases (e.g. sitting on Channel panel) do not have access to PCMT[4]. Information from cases will be presented to Channel panels by, for example, CTCOs.

1.2.5.3 Volume of Cases

The number of Prevent referrals vary on a yearly basis. In the year ending 31 March 2025, there were 8,778 referrals to Prevent due to concerns that an individual was susceptible to radicalisation.

Prevent referrals can originate from a variety of sources, including but not limited to those detailed in Annex B

[4] Note the 'Channel Coordinator' and 'Channel Coordinator Supervisor' roles have been disabled.

COUNTER TERRORISM POLICING

There will be a slight increase of cases who are under a CT investigation within Channel – but this number should not exceed 100 nationally.

1.2.5.4 Security controls

This sub-section describe the security controls:

- that have been implemented to safeguard personal information being processed and/or stored in PCMT;
- that are being investigated by the IT Pillar (CTPHQ) as a means of exercising further control (or protection) of personal information, for which CTP is responsible, to safeguard 'need to know' (as required by the Data Protection Act), and mitigate outstanding risks as shown in Table 4.1.

The PCMT application runs on the [redacted] operated by CTP, which is hosted on a private cloud computing platform belonging to the Foreign and Commonwealth |Development Office (FCDO),[5] and residing within secure premises in the UK (owned by the UK government).

Key controls:

1. The application and platform has been designated as OFFICIAL-SENSITIVE and cannot be used to hold information at SECRET or above. Note information at SECRET or above must be redacted by the originating force and permission granted to allow storing within the PCMT.
2. All user activity within the application is logged with a time stamp and date.
3. Read and Write access with regard to the information processed and stored using PCMT is subject to Role-based access Controls (RBAC). In particular:
   - Cases which are 'Police-only' will be inaccessible to representatives from Channel (non-CTP);
   - Access to Cases by users from HSG is 'read only'.
4. PCMT is encrypted and hosted on a secure CT server.
5. Access to PCMT requires all users to possess a minimum security clearance of [redacted] All users are subject to a review of security clearance on an annual basis. Failure to adhere to annual reviews will result in vetting being downgraded and access to PCMT being removed.

<u>The following controls are subject to investigation:</u>

- CTP is investigating the potential use of obfuscation techniques with regard to data shared with HSG;

[5] Formerly the Foreign and Commonwealth Office Services (FCOS)

COUNTER TERRORISM POLICING

- CTP to investigate whether particular types of information associated with each Case can remain as 'Police-only';
- CTP to investigate whether access to Channel data by some HSG groups could be restricted to information presented via Tableau, i.e. control what is exported to Tableau;
- Access to PCMT by individuals from HSG needs to be subject to a well-defined authorisation / de-authorisation process. Furthermore authorisation needs to be based on a sound justification.

1.2.6 Deletion of personal data

Review, Retention and deletion Policy

Upon case closure, a review date, 6 clear years after the closure of the Case, will be added to the Subject in order to review, retain and dispose of information no longer required in line with RRD policy. If the decision is to retain, in line with MOPI 3 review times, subsequent reviews shall be done every 5 clear years until deletion.

Note there is a 'triggered review' process as well, should for example, an individual/court request deletion.

Supervisors are responsible for carrying out any MoPI reviews and the final deletion of data shall be completed by an Inspector (or above) with the MoPI Approver role, or by the SPP at S.24(1), S.31(1)

Data is also subject to an ongoing Business Assurance Process (BAP) led by CTPHQ, this includes national dip sampling of data for control quality assurance.

Family, significant others and associate data

Data relating to family, significant others or associate of the Prevent subject will not be reviewed independently to the Prevent subject's data. If the reviewer considers it proportionate to retain the case data, all the information relating to the case should be retained to allow any subsequent use of the data to be reviewed holistically. Removing parts of data could result in missed risk.

Duplication

Any duplicate entries recorded on PCMT must be brought to the attention of Strategy Planning and Performance (SPP) to ensure errors are rectified and conform to UK GDPR guidelines and MOPI compliance.

COUNTER TERRORISM POLICING

2. Data Protection and 'Privacy Law' Assessment

2.1 European Convention of Human Rights

Article 8: Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right, except such as is in accordance with the law, and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

CTPHQ is hosted by the MPS, which is a public authority, and is therefore, subject to a statutory duty under HRA Article 6(1) not to act inconsistently with a Convention right. The relevant Convention right for the purposes of this processing is Article 8(1) of the Convention.

Q1	**Does this project / initiative address a Pressing Social Need?**

Yes, the project fulfils a legitimate aim, namely the prevention of radicalisation and terrorism in the UK. It is manifestly a pressing social need that subjects are prevented from being radicalized and perpetrating acts of terrorism.

With the early identification of vulnerable persons who are suspected of being radicalised towards terrorism, this initiative will contribute to addressing a pressing Social Need in

- Safeguarding individuals and keeping the public safe
- Maintaining National Security
- Disrupting criminality

Recent terror attacks in the UK and across Western Europe have involved people who have become radicalised or drawn towards any terrorism offending through any other means, either online or in person.

We seek to prevent the loss of life and injury caused by terrorist attacks, and indeed all other terrorism-related offending as per the breadth of the UK's counter-terrorism laws. To achieve this involves identifying people within our communities who are vulnerable and/or at risk of being drawn towards terrorism by any means, including grooming, direct radicalisation or even coercion, and providing early intervention to mitigate any potential terrorism risk either to themselves or the public. This supports of Her Majesty's Government CONTEST policy.

COUNTER TERRORISM POLICING

Q2	**Are your actions / data sharing a proportionate response to the social need this project/initiative has identified?**

Yes, in order to address the pressing social need it is necessary and proportionate to process the data of Prevent subjects on a national database.

It is necessary and proportionate to share data with law enforcement and partner agencies to ensure risk assessments can be completed and assess what interventions may be required for persons being referred into Prevent.

The headline privacy design features for the PCMT include:

- A robust policy and standard working procedures created to outline the restrictions as to who, what, why, when and how requirements of processing this information
- Suitable vetting S.24(1), S.31(1) and confidentiality arrangements (PCMT Code of Conduct) are in place between CTP and Data Processors.
- Appropriate technical and organisational measures are in place to safeguard against any unauthorised loss, disclosure or destruction of data

The deployment and future developments of the PCMT capability will be subject to strict yearly reviews lead by CTPHQ Prevent Senior Leadership Team, which will take into account all Public complaints submitted to CTPHQ either directly or through regional CTP Prevent teams, regarding the use of this software application.

The proposed processing is plainly proportionate as:

1. The objective of preventing radicalisation and terrorism behind the interference with the subjects' rights is sufficiently important to justify limiting their rights. Subjects who are vulnerable to radicalisation must be prevented from engaging in extremism and terrorism.
2. Prevent, as part of the National CONTEST strategy, is co-ordinated by CTPHQ. As a national programme, there must be a central database to ensure that the information is lawfully managed. The processing allows Prevent practitioners across the UK to effectively manage subjects who are vulnerable and divert them from terrorism, including through effective and accountable sharing of data with other Specified Authorities and law enforcement partners; for example, people regularly move across policing areas, the only way to ensure the subject has continuity in their programme, is through the maintenance of a national database, which allows for sharing of information with relevant partners is necessary. In the case of Prevent, Section 26 CTSA dictates: "A specified authority must, in the exercise of its functions, have due regard to the need to prevent people from being drawn into terrorism." The Prevent program and PCM system have been designed specifically to meet this objective. The processing is thus rationally connected to the objective.
3. The processing goes no further than is necessary to accomplish the objective:

a. Managing Prevent cases through the PCMT is the least intrusive means of achieving the objective. The PCMT prevents unnecessary duplication by being the single repository for the national Prevent data. Prior to the development of PCMT, the forces had to rely on spreadsheets on a local and national level to track the progress of the subjects. This could have led to duplication and a higher likelihood of data not being updated/corrected. It was also a less secure means of managing the data.

b. Decision makers appreciate and mitigate the impact of the processing:

   i. **Safeguards**: both the PCMT and the data sharing practices have safeguards designed into them. For example, practitioners must all be vetted (as set out above) and receive training on the systems. The PCMT itself is auditable and provides prompts for carrying out RRD. Data sharing is carefully managed through, for example, data sharing agreements.

      With proportionality being understood as a variable, and with each case under a system of constant circumstantial review, it should necessarily follow that no disproportionate action will be taken when conducting research into Prevent subjects (necessary to inform a risk assessment of their vulnerability to radicalisation / terrorism), and that the only actions that will be taken are ones that are strictly necessary for the successful completion of the Prevent mission.

      The decision maker much record the proportionality of all actions taken on the PCM system.

   ii. **Least possible interference**: CTPHQ and Channel partners recognises the importance of the data subjects' privacy expectations and human rights concerns. Ensuring that the data is managed from a single national database has allowed for the implementation of national standards and stricter controls to ensure the data protection principles are met.

      If in the instance that an action is taken where there was a less intrusive option available, the decision maker must explain why they did not opt for the least intrusive method.

   iii. **Public awareness**: The public are aware of the PCMT system (e.g. recent press articles), however details of the technical solution and protective measures have been withheld on security grounds. Note the public would expect the police to have a single, secure and auditable system for management of the sensitive information that is created as a result of a Prevent referral.

   iv. **Alterative policing tools**: Prior to the development of PCMT, as set out above, the data was managed on a series of spreadsheets. It was not viable for CTPHQ to co-ordinate the police's response to the Prevent duty in this way. In terms of policy – given the CTPHQ's role as co-ordinator of the response, there would be no suitable alternative to offering guidance

from the central location to ensure quality of data processing practices across the country. To have forces or even regions drafting their own policies may result in a data management "post-code lottery".

Use of the PCMT by Channel Partners, instead of the separate CMIS system, enhances the delivery of Prevent. Moreover having a centralised database of cases enables effective management of Channel cases by having all the information in one place. It also allows for oversight of Channel data by the Home Office - this oversight is used to develop policy and quality assure standards of Channel case management.

In some instances limited data will be shared with Home Office approved Intervention Providers (IP). IPs are processors of data. Note IPs are contracted to mentor vulnerable individuals and are vetted to SC level. IPs are not given access to the system, and the extent to which any information is shared with the IP is at the discretion of the CTCO/CC/SIO

Where a case is under a CT investigation and the IP reports are shared with the investigation team, the impact on the privacy rights of the individual will be considered on a case-by-case basis. IP reports will only be shared where it is assessed to be necessary and proportionate to do so to mitigate risk and to prevent and detect crime.

4. Taking the proposed processing in the round, the processing strikes a fair balance between the rights of the subject and the interests of the wider community. On balance, the need to undertake processing for the discharge of the prevent duty outweighs the interests of the human rights and the data rights of the subjects. The use of the PCMT for ensures that subject's data is managed safely and in accordance with the data protection principles. It minimises the risk of safeguarding opportunities, or even pursue matters, being missed. Managing the data on the single platform saves lives.

   In the case of Prevent the case must continuously be reviewed to ensure that proportionality and justification continue to exist. Decision makers must have an appreciation of the impact of processing an individual and must use this understanding to inform their own judgement regarding the proportionality of the action.

It is plainly proportionate to engage in the processing of personal data through the use of PCMT for the purpose of discharging the Prevent duty.

COUNTER TERRORISM POLICING

2.2 Common Law Duty of Confidence:

A breach of confidence will become actionable if:

- The information has the necessary quality of confidence.
- The information was given in circumstances under an obligation of confidence.
- There was an unauthorised use of the information to the detriment of the confider (the element of detriment is not always necessary).

However, there are certain situations when a breach of confidence is not actionable. Those situations are:

(1) If a person has provided consent for the processing of their information.
(2) If there is a legal requirement to process the information.
(3) If it is in the public interest to process the information.

It is our view that points 2 and 3 above are applicable for the reasons already outlined in this DPIA.

COUNTER TERRORISM POLICING

2.3 Data Protection Act 2018

2.3.1 Principle 1

(1) Processing of personal data for any of the Law enforcement purposes must be lawful and Fair.

(2) The processing of personal data for any of the Law enforcement purpose is lawful only if, and to the extent that, it is based on law and either :

(a) The data subject has given consent to the processing for that purpose, or
(5a) The processing is strictly necessary for the law enforcement purpose, it must be stressed that there is no intention of CTP to provide wide access to this data corporately. Nor indeed is it our intention to process this data beyond our core policing purposes.
(5b) The processing meets at least one of the conditions in Schedule 8 is met.

COUNTER TERRORISM POLICING

CTP

CTP processes Prevent data under both UK GDPR and Part 3 DPA. When a case reaches the threshold for law enforcement processing, then it switches from the UK GDPR regime to the law enforcement regime. The point at which this occurs is case-specific, with the guiding principle being that the matter has escalated beyond purely safeguarding to where it is necessary to process the subjects (or associates of the subjects) data for "the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security" (s.31 DPA). This is unsurprising as CTP's role is to directly manage nominals, who are vulnerable to being drawn into terrorism and the purpose of Prevent is to divert nominals from the criminal justice system. However, in the exercise of CTP's functions it must constantly have regard for the risk posed to or by the subject, which may escalate, causing CTP to switch to law enforcement functions including to (e.g.) manage an emerging threat to the public.

The processing of police information must be linked to a policing purpose. The Management of Police Information (MoPI) Code of Practice defines policing purpose as:

a. Protecting life and property
b. Preserving order
c. Preventing and detecting offences
d. Bringing offenders to justice
e. Any duty or responsibility of the police arising from common or statue law

CTPHQ processes personal data for the law enforcement purposes as set out in s.31 (Data Protection Act 2018) namely 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."

The Law Enforcement Purposes will cover any operation or set of operations which are performed upon personal data or sets of personal data, whether by automated means or otherwise, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction of processing, erasure or destruction.

Consent from data subjects (or associate individuals) is not always relied upon as a legal basis to process data. This is because consent can be withdrawn by the data subject at any time. If consent is withdrawn, CTP must delete the data or demonstrate another legal basis to process the personal data.

Home Office (and Channel Partners)

The Home Office is processing the data for the purpose of the Home Office's official functions and the processing is in the public interest (Article 6(1)(e) UK GDPR). The lawful basis for processing special category data is Article 9(2)(g) UK GDPR (substantial public interest) and paragraph 6,

Part 2 of Schedule 1 DPA 2018 (statutory and government purposes and substantial public interest).

When special category personal data is being processed, HSG relies on substantial public interest to satisfy Article 9(2)(g) GDPR and paragraph 6 of Part 2, Schedule 1, DPA 2018.

Processing of personal data is necessary for the purposes of the various Channel duties set out in Chapter 2 of Part 5 of the Counter-Terrorism and Security Act 2015.

The Home Office uses the dataset to support Channel delivery locally and nationally. For example, policy officials are able to publish national statistics; quality assure case management; consider new policy initiatives to respond to the need of Local Authorities, e.g. improving mental health representation by liaising with the Department for Health and Social Care.

Policy officials also use this data to quality assure Channel delivery and context about a particular individual and the performance of the CT system i.e. in the aftermath of a terrorist incident. The Home Office involvement is of substantial interest to the public (Article 9(2)(g) UK GDPR and paragraph 6, Part 2 of Schedule 1 DPA 2018). The merge of CMIS onto PCMT will ensure that the system is easier for users to input information, reduce double-keying, and therefore produce one higher quality dataset.

Q1.	**Describe whether you are relying on consent to process personal data, and how this will be collected?**

Prevent does not rely on consent to process personal data. Prevent relies on statutory and common law powers for all work, from Prevent Gateway Assessment, through the Information Gathering phase, the s.36 CTSA decision and referral into Channel. If a case is accepted/adopted into Channel then the data would fall within the scope of UK GDPR, as Local Authorities are not Competent Authorities under the legislation[6]. Therefore at the point of an offer of support being made to the subject or their associates (so gaining consent) a leaflet *from the local authority* should then be provided to the subject stating their data subject rights. The Channel Chair will decide who is making this contact and therefore who will provide this leaflet.

Channel is a voluntary Home Office initiative and forms a key part of the Prevent strategy. The process is a multi-agency approach to identify and provide support to individuals who are vulnerable to being of drawn into any terrorism related offending. To facilitate sharing of information, a Data Sharing Agreement (DSA) is in place between CTPHQ and Home Office. Note it is assumed that separate agreements shall be established between Home Office and its channel partners (Local authorities) as deemed necessary.

The MPS has a comprehensive Privacy Notice. This notice includes full details of how a subject may exercise their Principle 6 rights.

[6] A 'Competent Authority' refers to an organisation (or person) specified in Schedule 7 of the DPA 2018; or any other person if, and to the extent that, they have statutory functions to exercise public authority or public powers for the law enforcement purposes.

COUNTER TERRORISM POLICING

Q2.	Describe the legal basis you will be using if obtaining consent would prejudice the purpose for which the personal data is collected?

1. CTP

CTPHQ relies on statutory and common law powers to process information on PCMT for the law enforcement purposes as set out in s.31 DPA. From the outset, it is noteworthy that the processing of third-party data does not rely on consent. Rather, the processing of third-party data isa necessary and proportionate measure in furtherance of Prevent duties and has a policing purpose. This is consistent with other policing practice, whereby personal data relating to witnesses, suspects or other relevant third parties may be processed without reliance on consent in order to fulfil statutory and common law policing functions, including safeguarding, risk management, and the prevention of crime and threats to public safety,

1.1 Statutory Powers

Processing data in discharge of the Prevent duty has a statutory basis, namely s.26 Counter Terrorism and Security Act 2015:

> "A specified authority must, in the exercise of its functions, have due regard to the need to prevent people from being drawn into terrorism."

Schedule 6 CTSA sets out the specified authorities, which include chief officers for police areas in England and Wales.

The Home Office-issued guidance pursuant to s.29 CTSA, Revised Prevent duty guidance: for England and Wales (Updated 10 April 2019) (the "Guidance"), explains, 'The term "due regard" as used in the [CTSA] Act means that the authorities should place an appropriate amount of weight on the need to prevent people being drawn into terrorism when they consider all the other factors relevant to how they carry out their usual functions.'

In order for specified authorities to discharge their Prevent duty it is necessary to process information relating to persons 'at risk of radicalisation' in order to give them 'appropriate support (for example on the Channel programme)' (para 21 the Guidance). This processing is achieved through the PCMT.

1.2. Common Law

In addition to the statutory basis under s.26 CTSA, the Police may rely on common law powers to process information in the exercise of their policing duties and obligations (their "policing purposes", which include but are not limited to:

- protecting life and property;
- preserving order and preventing threats to public security;
- preventing and detecting crime;
- bringing offenders to justice; and
- upholding national security.

The legitimate aim to prevent radicalisation and terrorism engages the police's policing purposes. The power for the police to share and otherwise process data (in this case using PCMT), under common law is firmly established in case law, for example:

- *Rice v Connolly* [1966] 2 QB 414 at [419B – C]: '[I]t is part of the obligations and duties of a police constable to take all steps which appear to him necessary for keeping the peace, for preventing crime or for protecting property from criminal damage. There is no exhaustive definition of the powers and obligations of the police, but they are at least those, and they would further include the duty to detect crime and to bring an offender to justice.'
- *Regina v Chief Constable of the North Wales Police and Others, Ex parte Thorpe and Another* [1999] Q.B. 396 at [409-410]: '…When, in the course of performing its public duties, a public body (such as a police force) comes into possession of information relating to a member of the public, being information not […] generally available and potentially damaging to that member of the public if disclosed, the body ought not to disclose such information save for the purpose of and to the extent necessary for performance of its public duty or enabling some other public body to perform its public duty...'
- *Regina (Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland and another (Equality and Human Rights Commission and others intervening), Regina (T) v Commissioner of Police of the Metropolis (Secretary of State for the Home Department intervening)* [2015] A.C. 1065 at [1078]: 'At common law the police have the power to obtain and store information for policing purposes, ie broadly speaking for the maintenance of public order and the prevention and detection of crime.'

Processing the data on PCMT is strictly necessary, as it relates to a pressing social need (namely to prevent the radicalisation of the subjects, and thus prevent the commission of terrorism-related criminal offences and/or prevent threats to public security), and (as set out above in Section 2.1 Q.2) is not reasonably viable to address this legitimate aim through less intrusive means. The only viable way of ensuring that the Prevent strategy functions correctly is to build it around a common secure database that the relevant practitioners can access.

2. Channel Partners

Channel Partners will not process information for which they are Data controllers without consent, e.g. from the data subject. There is of course data that is controlled by CTP which may be provided to representatives from Home office to support the decision as to whether a Case is suitable for entry into Channel.

CTPHQ is putting in place an Information Governance Strategy and Structure, until this is in place MPS processes will be followed. It should be noted however that CTPHQ operates a:

- Comprehensive set of policies and procedures;
- Compliance & Assurance unit, incorporating a Information security Team, Physical security, Information Sharing, and Compliance & Protective Monitoring Unit.

COUNTER TERRORISM POLICING

The MPS has an Information Governance Strategy and Structure in place which incorporates the requirements of the MPS to be open and transparent around the nature in which (sensitive) personal data are to be processed (where possible). The MPS has a comprehensive Privacy Notice. This notice includes full details of how a subject may exercise their Data Protection rights.	
Q3.	**If you are relying on consent, how will you tell individuals about the use of their personal data?**
CTP (Prevent) does not rely on consent as a legal basis to process personal data. There is a legislative requirement to carry out Prevent under the CTSA, as well as common law powers for police to discharge their policing purposes. Similarly, the processing of processing of third-party data does not rely on consent, as indicated above in Q2. Channel Partners: If a case is accepted/adopted into Channel then at the point of an offer of support being made to the subject (so gaining consent) a leaflet from the local authority should then be provided to the subject stating their data subject rights. Where family interventions are provided the family, significant others or associates involved will receive a leaflet which will include a link to further information regarding their data subject rights.	
Q4.	**Do you need to amend your privacy notices?**
No, I have read the MPS Privacy Notice and I am content that it sufficiently covers the intended processing.	

COUNTER TERRORISM POLICING

Q5.	Describe any special category data you will be using?

Special category data will be collected for the outlined purposes as explained in earlier sections of this document. The following table provides further detail.

Special category data (types)	To be processed?
Criminal conviction data	Yes
Race or ethnic origin (including nationality)	Yes
Political opinions	Yes
Religious or philosophical beliefs	Yes
Trade union membership	Yes
Genetic data or biometric data for the purpose of uniquely identifying individuals	No
Health	Yes
Sexual orientation or details of the sex life of an individual	Yes

The special categories of data processed and stored with regard to each data subject will reflect the particular circumstances (and 'drivers') behind their being drawn into terrorist-related activities. Hence the option to process and store special category data is there, however if it is not relevant then no data should be entered. Note the respective Case Officer / Channel coordinator will be able to provide further details.

In order to process and share special category data, **at least one condition relating to special Category data** below must be satisfied.

2.3.2 Schedule 8 Consultation for sensitive processing under Part 3

Section 1. Statutory etc., purposes
Section 2. Administration of justice
Section 3. Protecting individuals vital interests
Section 4. Safeguarding of children and of individuals at risk
Section 5. Personal data already in the public domain
Section 6. Legal claims
Section 7. Judicial acts
Section 8. Preventing fraud
Section 9. Archiving etc.

Q6.	**Describe the Schedule 8 condition(s) (outlined above) that are to be met for the processing of special category data?**

The following Schedule 8 Conditions are applicable to the processing:

<u>Statutory etc. purposes</u>

This condition is met if the processing—

(a) *is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and*

(b) *is necessary for reasons of substantial public interest.*

As set out above, there is a legislative requirement to implement the Prevent strategy created by the CTSA. The subjects' data is processed in order to comply with the Prevent duty and the police's common law duties and obligations as set out in 2.3.1. Q2 above. It is manifestly in the substantial public interest to process the data as it will prevent terrorist-related harm to the public.

Protecting individual's vital interests

This condition is met if the processing is necessary to protect the vital interests of the data subject or of another individual.

Certain processing activities carried out via PCMT will save lives, for example:

- in cases where it is necessary to share data into the Pursue space in order to prevent an imminent terrorist attack.
- In cases where early intervention within Prevent will prevent terrorist ideation maturing into terrorist attacks.

Safeguarding of children and of individuals at risk

(1) This condition is met if:

(a) the processing is necessary for the purposes of:
- protecting an individual from neglect or physical, mental or emotional harm, or
- protecting the physical, mental or emotional well-being of an individual,

(b) the individual is—
- aged under 18, or
- aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

The nature of Prevent is such that much of the daily business involves children and or vulnerable and at risk people, as these are often targets for extremist groomers and radicalisers. The children and vulnerable adults may be subject to harm by the groomers and need safeguarding.

The processing is necessary for the exercise of any functions conferred on a constable by any rule of law. The legal framework and existing body of guidance in which the CTPHQ relies on is provided by the following:

- The Data Protection Act 2018;
- NPCC Authorised Professional Practice (APP);
- NPCC (2005) Guidance on NIM, NIM Guidance and NIM Codes of Practice (2005);
- APP Intelligence Management Guidance;
- 2010 Guidance on the Management of Police Information;
- The APP Data Protection Manual of Guidance;
- CTP security policy (otherwise MPS security policy)
- MOPI;
- Retention, Review and Disposal Policy;
- Information / Data Sharing Agreements - Gateways, Exemptions & Explicit Powers;

Counter Terrorism & Security Act 2015

a. S.36(3) of the CTSA states: "A chief officer of police may refer an individual to a panel only if there are reasonable grounds to believe that the individual is vulnerable to being drawn into terrorism."
b. These are the first means, and requirement, by which Police share information with Partners in the Local Authority within Prevent.

Crime an Disorder Act 1998

a. Section 115 confers a power to disclose information to a "relevant authority" on any person who would not otherwise have such a power, where the disclosure is necessary or expedient for the purposes of any provision of the Act.
b. The "relevant authority" means a chief officer of Police in England, Wales or Scotland, a Police authority, a local authority, a health authority or a probation committee in England and Wales, and includes an individual acting on behalf of the relevant authority.
c. The purposes of the Crime and Disorder Act include, under section 17, a duty for the relevant authorities to do all that they reasonably can to Prevent crime and disorder.

Common Law Powers

a. Because the range of partners with whom the Police deal has grown - including the public, private and voluntary sectors, there may not be either an implied or explicit statutory power to share information in every circumstance.
b. This does not necessarily mean that Police cannot share the information, because it is often possible to use the Common Law.
c. The decision to share using Common Law will be based on establishing a policing purpose for the activity that the information sharing will support, as well as an assessment of any risk.
d. The Code of Practice on the Management of Police Information (MoPI) defines policing purposes as: protecting life and property, preserving order, preventing the commission of offences, bringing offenders to justice, and any duty or responsibility of the Police arising from common or statute law.
e. In general terms, if the sharing of the information is for a purpose related to policing (as above) and the conditions of the Data Protection Act are satisfied, then it will be lawful.

Local Government Act 1972

a. Section 111 provides for Local Authorities to have "power to do anything…which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their functions".

Local Government Act 2000

a. Section 2(1) provides that every Local Authority shall have the power to do anything which they consider is likely to achieve the promotion or improvement of the economic, social or environmental wellbeing of the area.

See the DPIA produced by the Home Office (section 3) for further detail pertaining to Home office (and Channel partners).

Q7.	**Optional additions: List any relevant legal requirements which necessitate this processing (This adds weight to the justifications provided).**

N/A

2.3.3 Principle 2

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The intended processing is in line with the purposes outlined above.

And specifically with regard to CTP, those listed in the Privacy Notice and our notification with the Information Commissioner's Office: Registration No: Z4888193.

Q1	**Have you identified potential new purposes as the scope of the project/ initiative expands? If the answer to this question is 'yes', then you must seek the advice of the CTPHQ Information Governance Team.**

Yes, the implementation of additional functionality into PCMT (as a replacement for CMIS), and for access by authorised staff from Home Office and Local Authorities. Note see section 2.3.7 for details of the protection afforded.

The Home Office now provide a family intervention service which allows family members, significant others and relevant associates of the Prevent subject to receive support from an intervention provider. This support is only available to those individuals who consent. The Intervention Provider will produce a report following the sessions which will be uploaded onto PCMT. This report may contain personal or special category data of the individuals involved in the intervention. Advice has been sought from CTPHQ Information Governance who advised an amendment to this DPIA.

2.3.4 Principle 3 Personal data processed for any of the law enforcement principles must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

It is not the intention to process exhaustive amounts of personal information on the loose premise that it may be useful now or in the future (excessive data collection is also a breach of the DPA 35(2)(b)). This approach would be highly time and resource intensive, as well as potentially costly.

If at any point, the data processed is found to be excessive to the purpose, then the processing may be ceased. The processing will be subject to periodic yearly review in terms of assessing the value that this product plays in enabling CTP and Channel to fulfil their respective purposes as described earlier in this document.

Q1.	**Detail why you need all the data sets you are collecting?**

The mission of Prevent is to safeguard both the subject of the referral and the public.

The only data collected and processed around individuals is targeted with that specific safeguarding objective in mind. This extent of the data collected and the uses it is put to vary between each individual, the specific complex needs, the Prevent relevant vulnerabilities associated with the case and the bespoke approach taken to address and mitigate these issues in each case.

Q2.	**Which personal data could you not use without compromising the needs of the project/initiative?**

None, all of the data sets are necessary for Safeguarding of a subject and subsequent triage of data to mitigate any potential CT-related vulnerabilities and risks.

2.3.5 Principle 4

Personal data shall be accurate and, where necessary, kept up to date and erased or rectified without delay.

Data subjects are at liberty to make requests under the FOIA and DPA 2018 as stated in section 1.2.2.4. Note this includes requests to access records, highlights errors (and propose corrections) and deletions, however the response by CTP and Home Office is subject to processes described in the SOP for 'Prevent Case Management'.

CTP and Channel are mindful of the potential damage and distress to the data subject, the organisation and to third parties if the data processed was inaccurate in any way. To mitigate this, an ongoing examination of the accuracy and quality of the data must occur throughout the course of the processing. This takes the form of regular re-assessments of the data subject, the case context and any other relevant material, assuring that vulnerabilities, risks and threats associated with the referral subject are managed and mitigated expeditiously in conjunction with partners who provide their own expertise and challenge.

Caseworkers are responsible for correcting data in the first instance.

Data will be managed as per MoPI guidelines.

Prevent practitioners are trained in the use of PCMT to ensure data quality.

COUNTER TERRORISM POLICING

An ongoing Business Assurance Process (BAP) is conducted by CTPHQ :The process has been designed in order to provide a consistent framework for use (primarily by CTPHQ) across the Prevent policing network to achieve the following objectives:-

1. Demonstrate how our statutory responsibilities from the CTSA are being discharged;
2. Ensure national policies are being implemented consistently;
3. Reduce the risks within case management;
4. Identify and share good practice; and
5. Identify and resolve barriers to effective working.

Q1.	**If CTP is procuring new software, does it allow the data to be amended/ deleted when necessary? (The answer to this question must always be yes. The software should be designed with functionality to record that the accuracy of information is challenged and why).**

No new software is being procured. Data held on PCMT can be deleted and amended by business assurance staff with relevant account permissions. Before deletion the information is checked for accuracy and a rationale subjected to challenge wherever appropriate.

Q2.	**How is CTP ensuring that personal data obtained from individuals or other organisations is accurate?**

Prevent referral data is provided in the majority of instances by professional individuals who have a legal duty under the CTSA 2015 to provide accurate information in a lawful and proportionate manner. Other data can be provided directly from members of the public around concerns they may have. One way or another, this data is checked for accuracy by Fixed Intelligence Management Units (FIMUs) before any work is completed around the case by CTP Prevent. FIMUs also assure that the information is not a duplicate referral and that there are no immediate terrorism threats or ongoing Pursue-led investigations around the data subject that are not apparent from the initial referral. If neither of these are the case, the data is then passed to CTCOs (Prevent Police / staff) who complete a Prevent-specific screening and triage for relevant vulnerabilities and risks. This process involves a review of police databases and speaking with the initial referrer of the data wherever possible, in order to clarify details and clear up any uncertainties. When entering subject details onto the PCMT, the application makes the user search for information already held on the system, this provides additional preventative security around the duplication of data. Any other reporting is also checked in the same way for accuracy.

Staff from Channel partners (Home Office and Local Authorities) operating as case workers are similarly professionals and aim to provide accurate information in a lawful and proportionate manner.

Finally where data does need correcting then this shall be undertaken by the officers / staff from CTP or Channel Partners as appropriate, and decisions and actions taken based on the original data shall be reviewed – with any concerns raised for management's attention in a timely manner.

2.3.6 Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose for which it is processed.

The information will be retained in line with the Retention, Review and Deletion policy – see the 1.2.6 for details.

Q1.	**What retention periods are suitable for the personal data CTP will be processing?**

The personal data will be retained in line with MOPI guidelines.

The PCMT has built in a review date that is set when a case is closed for a subject. Once a review is required the PCMT will be updated by a supervisor.

In the event an early deletion request is received, local deletion procedure but **must not** be carried out by a person below the rank of chief inspector or staff equivalent. They will assess its ongoing necessity to retain for law enforcement purposes, applying the NRAC criteria, and the APP Information Management.

Q2.	**Are you procuring software that will allow CTP to delete information in line with our retention periods? (*The answer to this question must always be yes)***

No new software is being procured but the current PCMT has a built on facility to apply a MoPI status upon closing the case.

2.3.7 Principle 6

Personal data shall be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures. Appropriate security includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Security incidents pertaining to the (actual or potential) misuse of the PCMT application (or associated data) shall be reported, where relevant to Channel cases, to the CTPHQ and HSG SPOCs for Prevent without undue delay of occurring or no later than 24 hours after becoming aware of it. This is to allow CT Policing to risk assess the security incident.

Q1.	**How do you manage security of personal data? Describe the security measures in place including the process for reporting incidents and breaches.**

The PCMT application and S.24(1), S.31(1) are subject to security accreditation by CTPHQ. Furthermore the underlying 'private' cloud platform provided by FCDO is also subject to its own security accreditation.

Security documentation includes:

- RMADS for PCMT S.24(1), S.31(1)
- SyOPs for S.24(1), S.31(1) and Code of Conduct (and other user guidance) for use of the PCMT
- DPIA;
- EIA;
- Classification assessment and Business Impact Assessment (BIA).

Other security-related activities / artefacts include:

- IT security health check;
- IT support procedures operated by CSC;
- Design documentation ('approved' by STAG[7])

Access to the S.24(1), S.31(1) restricted to secure networks operated by Police Forces (and a small number of criminal justice partners). Furthermore access from these networks to the S.24(1), S.31(1) (and PCMT) is subject to domain-based authentication and role-based access controls (RBAC) based on an authorisation/de-authorisation process controlled by the CPMU in CTPHQ. Note the corporate network operated by Home Office, accredited to process and store OFFICIAL-SENSITIVE, has access to S.24(1), S.31(1)

All transactions / requests undertaken using PCMT (S.24(1), S.31(1) each User are logged for audit purposes.

Instances of misuse or breaches of security policy and/or procedures shall be reported in accordance with the CT corporate incident reporting procedure (linking through to Channel partners as appropriate).

Details as per Balanced Risk Assessment below (section 4)

2.3.8 Miscellaneous Considerations

1	Complaint Handling
Complaints about the use of Personal Information in relation to this project should be handled by the CPTHQ Data Protection and Freedom of Information Officer.	
2	Freedom of Information Act 2000 (FoIA)

[7] Security Technical Architecture Group (STAG)

COUNTER TERRORISM POLICING

CTPHQ and Channel partners shall demonstrate a commitment to openness and transparency regarding this processing, subject to any limitations posed by security or confidentiality requirements.

CTPHQ is hosted by the MPS, who are a public authority for the purposes of the FoIA 2000. This means that any information held by CTPHQ is accessible by the public on written request, including this DPIA, albeit subject to certain limited exemptions as a result of:

- Legal Advice;
- Commercially Sensitive material;
- Personal Data Pertaining to the Consultation Participants;
- Information which would otherwise affect the operations of the CTP and/or Channel and is not in the public's interest to disclose.

All public requests for information should be directed to Freedom of Information Officer (CTPHQ). Note CTPHQ shall liaise with Channel partners as appropriate on receipt of an FoIA request.

3	Individual Rights

UK GDPR Recital 1(1) the protection of natural persons in relation to the processing of personal data is a fundamental right. (2) Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

4	International Transfers

Part 3, Chapter 5 deals with when you can transfer personal data to a third country.

Q1.	**Are you going to transfer data outside the UK? If so what data, and to whom?**

No

COUNTER TERRORISM POLICING

3. Consultation Results

Stakeholder Consultation

Stakeholders	Roles and Responsibilities - Provision of guidance on completion of the DPIA and Pilot Exercise.	Outcomes – Advice Issued
Home Office	CMIS replacement project	Provided a copy of their DPIA for usage of the PCMT application.
CTP and Home Office	Legal representatives (and Project representatives from Home Office and the ICT Pillar and Compliance & Assurance from CTPHQ)	Decisions covering the Data controller and Processor responsibilities, and associated documentation.

Additional consideration has been given to other possible stakeholders; however they are not currently relevant to this process at this stage.

Public Consultation

It is NOT possible to conduct a full / public consultation.

PCMT is neither a pilot nor a trial but is an established system.

Public confidence in CTPHQ, hosted by the MPS, to safeguard and process all (sensitive) personal data we hold fairly and lawfully is of paramount importance to the Service. There are considerable security concerns within the data held on PCMT, as such no public consultation has been sought. Doing so may have an impact both on Domestic and International security.

In addition to the above, the privacy by design features outlined within this document will form part of the annual review of this DPIA to ensure adequacy of the protections they afford to the processing.

COUNTER TERRORISM POLICING

4. Balanced Risk Assessment

4.1 Risks

COUNTER TERRORISM POLICING

	Describe the risk and potential impact on individuals	Likelihood of harm	Impact	Mitigations/ Solution	Result	Residual Risk
		1 Remote 2 Reasonable possibility 3 More likely than not	1 Serious harm 2 Some impact 3 Minimal impact	Describe the mitigation and whether it will be implemented	Is the risk • Eliminated • Reduced • Accepted	• High • Medium • Low If the residual risk is High, please consult with the CTPHQ Information Governance Team
1	Any leakage of sensitive data into the community may result in physical harm (e.g. to Prevent subjects, those individuals raising their concerns through Prevent, or Police officers / staff contributing to the PCMT) due to the very nature of the information relating to terrorism. Information taken out of context may cause discrimination.	2	2	PCMT users are all S.24(1), S.31(1) [redacted] cleared at a minimum and sign a user agreement which outlines their responsibilities and expectations when dealing with sensitive data. Each officer / staff receives relevant training on PCMT for their role. The PCMT is hosted on a secure CT platform which is only accessible to authorised officers / staff from CTP (Prevent / FIMU) and Home Office (Channel). Police / Staff will also have completed Data Protection – Information and You NCALT package to ensure compliance with Data Protection matters.	The risk is reduced due to stringent levels of security being adopted.	Low
2	Reputational damage and embarrassment is an issue should information be leaked into the community regarding the details held on PCMT. This could lead to loss of public confidence and civil litigation	2	2	PCMT users are all S.24(1), S.31(1) [redacted] cleared at a minimum and sign a user agreement which outlines their responsibilities and expectations when dealing with sensitive data. Each officer / staff receives relevant training on PCMT for their role. The PCMT is hosted on a secure CT platform which is only accessible to CTP (Prevent /	The risk is reduced due to stringent levels of security being adopted	Low

				FIMU) and Home Office (Channel). Police / Staff will also have completed Data Protection – Information and You NCALT package to ensure compliance with Data Protection matters		

COUNTER TERRORISM POLICING

3	Risks to individuals: In the event of a breach of the security of data or information relating to an individual held on the PCMT, the following scenarios can be termed as 'potential risks' to the individual; 1. The first, and arguably most obvious risk to the individual in the event of a breach of the security of the information held about them in the PCMT, is that they would suffer a breach of the rights afforded them by Article 8 of the Human Rights Act, which grants an individual a right to a reasonable level of privacy. While this is a qualifying right, it is a right that should be adhered to in the context of the PCMT. 2. Should the apparent anti-establishment/extremist ideology of the individual become known to the wider society, it is conceivable that the individual's physical safety could come under threat, which is to say that they may suffer violence, or the threat of violence, or intimidation. 3. Should the identity of the individual become known to local authorities they may suffer undue attention and/or scrutiny, which could constitute harassment. 4. Should it come to light that the individual is under police supervision, and that the nature of	3 2 1	3 2 2	The scenarios considered in this document have been identified as risks that a subject of the PCMT could be subjected to in the event of a breach of the security surrounding the PCMT that resulted in data/information held within it being disseminated inappropriately/unlawfully. To give proper considerations to measures that are to be put in place to adequately mitigate against the potential for these risks to be realised, consideration must be given to relevant legislation and applicable corporate policy. These include, but are not limited to; Police ICT end user policy, The Data Protection Act, The General Data Protection and Regulations Act, The Computer Misuse Act. In order to ensure the security of the information relating to an individual being held on the PCMT is not compromised, the following measures will be implemented; 1. All users of the PCMT will abide strictly by their own constabularies ICT end user policy, specifically with regard to restricting access to the PCMT through their own user area to themselves only, and will not allow any third party to access the PCMT via their log-in/user area, regardless of the vetting	Provided the mitigating actions detailed in this document are followed, and that all officers and staff concerned follow protocol and adhere to policy, all identified risks can be mitigated against adequately enough to ensure the safety of any individual held on the PCMT resulting in an eliminated risk.	Low Low Low

	that supervision is in relation to concerns that the individual fosters an extremist ideology, a desire to introduce distance between anybody or organisation may lead to the individual suffering discrimination or prejudice, potentially resulting in denial of services or opportunities? 5. It should be noted, that as with any case of dishonestly appropriated data/information that there exists the possibility for identity theft. Note it seems reasonable to attribute a low level of risk here as it is extremely unlikely that a person minded to steal another's identity, would assume the identity of a subject vulnerable to being radicalised or drawn into terrorism offending who is already under police supervision. 6. A breach of the PCMT programme does have the potential to cause damage to the reputation of an individual. The Prevent objective is to deter individuals at risk of radicalisation or being drawn into terrorism offending by rehabilitating their attitudes towards whichever individuals, groups, communities or societies are the target for their actual or potential offending through police and other local authority intervention. Assuming this mission is successful, and that the individual in question re-integrates into society, a revelation that they were/are being monitored by	1 1 1	2 3 2	level or Professional capacity of the third party in question. 2. In accordance with general police ICT policy, no authorised PCMT user will agree to access the PCMT on behalf of any unauthorised third party, regardless of the vetting level or professional capacity of the third party in question. 3. Bearing in mind the stipulations of The Computer Misuse Act, no unauthorised personnel, regardless of vetting level or professional capacity, will attempt to access the PCMT through any user area/log-in other than their own. 4. The only users, whether a member of police staff or a police officer, that will have access to the PCMT will be vetted to an appropriate level and will be adequately trained in the use of the PCMT to ensure competence with the system. 5. All users of the PCMT must undergo and successfully complete a training package, designed to develop an understanding of their duties and obligations with regard to data protection and security. 6. No information from the PCMT will be emailed, dictated, printed, photographed, handwritten, or otherwise		Low Low Low

	counter terrorism police would likely result in damage to their personal reputation within their community, and could result in a shunning, giving rise to the risk of social disadvantage, especially when looked at in the context of employment and leisure/social/community activities. 7. A breach of the PCMT data/information and the difficulties it could impose on an individual with regard to seeking employment, do stand, if realised, to place the individual in a position of economic hardship, and further social disadvantage.	1	2	conveyed from an authorised or unauthorised PCMT user to any unauthorised third party, regardless of the vetting level or professional capacity of the third party in question. 7. There will undoubtedly be times where 'hard copies' of PCMT data will be required. These hard copies, when no longer required, are to be stored securely in an appropriate, locked filing cabinet, or destroyed by way of high security cross-cut shredder, at the earliest opportunity, and at no time left unsupervised or in a position where the contents of such a document could be viewed or interpreted by an unauthorised person. 8. The PCMT files are to be held on a secure platform, which is only accessible by counter terrorism police. 9. The PCMT system is to be held on a secure platform, which is only accessible by counter terrorism police. 10. Any subject of the PCMT will maintain their rights with regard to data protection legislation, namely; to view any information held about them on the PCMT, to have erased any information held about them on the PCMT that is no longer relevant (provided there is no over-ruling		Low

				reason to retain it under other legislation), and to have amended any information about them that it incorrect.		

COUNTER TERRORISM POLICING

4	Theft of laptops used by officers / staff to access the PCMT application.	2	3	1. Laptops provided to staff have been 'built' to a high security standard by Home Office, including the requirement for 'strong' authentication with regard to the 'disk encryption' and Operating system. 2. Laptops are required to be managed in accordance with SyOps provided by Home Office. Note laptops / mobile computing devices used by officers / staff from CTP are likewise subject to their respective 'local' security policies and procedures (which are required to comply with the Governance and Information Risk review) and the S.24(1), S.31(SyOPs.	The risk is reduced due to stringent levels of security being adopted.	Low
5	Oversharing of data CTP may be deemed to have shared too much data in contravention of the Data Protection Act. In practice this would be where CTP allows HSG to access data which is not required to fulfil its particular lawful purpose(s) (i.e. oversight, etc). In effect, the more access that the CTP grants to its systems, the more likely it will be in breach of the rights of the subjects because it will progressively be less able to demonstrate that the sharing is proportionate.	2	2	'Police-Only' cases will not be accessible by Channel Partners Note these Cases are the most sensitive and are excluded in accordance with criteria described in the DPIA (see section 1.2.2.1) and SOP. Details to be shared via PCMT are listed at section 1.2.2.3, 'Data Sharing agreement'. Further details may be found in the Data Sharing Agreement. CTP is investigating the potential use of obfuscation techniques with regard to data shared with HSG.	Reduced. Note the risk will increase as the number of HSG users increases.	Medium-High

	Potential impacts: 1. From the information commissioner: (i) Fine, (ii) Enforcement action (in the worst case scenario, being required to stop the processing), and (iii) An opinion that we have breached DPA with recommendations on actions CTP must take (this would likely be remedial actions to be completed by a certain date, failing which, options (i) and (ii) would be available). 2. Data subjects: (i) Damages on a large scale given the number of nominals, who go through Channel, and (ii) Costs			CTP to investigate whether particular types of information associated with each Case can remain as 'Police-only'. CTP to investigate whether access to Channel data by some HSG groups could be restricted to information presented via Tableau, i.e. control what is exported to Tableau. Access to PCMT is logged and subject to audit. Ensure that this requirement is implemented with regard to users from HSG. Access to PCMT by individuals from HSG needs to be subject to a well-defined authorization / de-authorisation process. Furthermore authorization needs to be based on a sound justification.		

Table 4.1

.

COUNTER TERRORISM POLICING

4.2 Implementation of DPIA Outcomes Responsibilities

	Action to be taken	Date for completion of actions	Responsibility for action
1	CTPHQ to provide relevant training materials for PCMT to Prevent trainers and practitioners.	30/01/2020 (Completed)	CTPHQ – Prevent (Managed Risk)
2	Review officer help guides within PCMT application to ensure information is kept up to date in relation to policy / legislation.	01/08/2020 (Completed)	CTPHQ – Prevent (Managed Risk)

COUNTER TERRORISM POLICING

5. Conclusion

The PCMT application (and information) benefits considerably from the protection afforded by the accredited S.24(1), S.31(1) operated by CTPHQ. In addition, the PCMT application has been enhanced to accommodate access by HSG, in respect of Channel cases (and excluding 'Police-only' cases). Finally, CTPHQ is investigating whether further control (or protection) of personal information, for which CTP is responsible, to safeguard 'need to know' (as required by the Data Protection Act), can be exercised to mitigate outstanding risks as shown in Table 4.1.

A review of the DPIA will take place on an annual basis and will be amended if any changes are made to the application in the future.

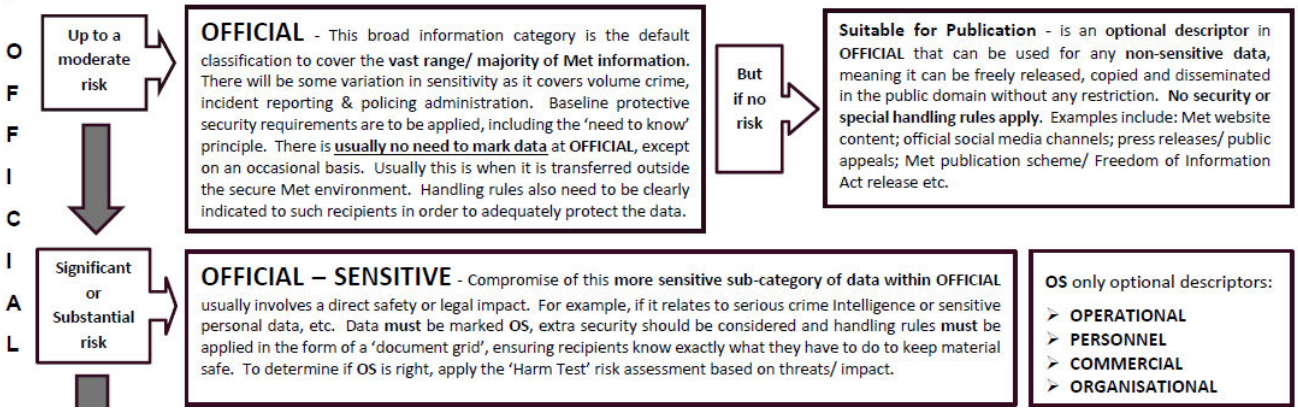
COUNTER TERRORISM POLICING

6 DPIA Sign-off

1	**Project Sponsor / NPCC Lead/ Operational Lead**
	Sign Below: Name: Position: Date:
2	**Head of Compliance & Assurance, on behalf of Data Protection Officer**
	Sign Below: Name: S.24(1), S.31(1) Date: 09/05/2024 re- signed 18/03/2025 Comment: Any future ICT technology solutions and processes are updated within the document and RRD functions and roles and responsibilities are updated in the SOP.

COUNTER TERRORISM POLICING

Annex A - Government Security Classification



COUNTER TERRORISM POLICING

Annex B - Main sources of Prevent referrals

Anti-Terror Hotline
Charity Commission
Child Protection
Community
[redacted]
Employer
Environmental Health
Faith Sector / Leader
Family
FE
Friend
HE
Health
Immigration / Border Force / HMRC
Local Government
[redacted]
MASH
Member of the public
Mental Health Hub
Mental Health Service
Military
National Probation Service
OFSTED/ESTYN
Other
Policing (CT)
Policing (Non CT)

COUNTER TERRORISM POLICING

Annex C – ACRONYM'S

Term	Acronym	Description
Counter Terrorism	CT	**Counter Terrorism** (**CONTEST**) **CONTEST** is the UK's **counter terrorism** strategy. It aims to reduce the risks from **terrorism**, so that people can go about their lives freely and with confidence. **CONTEST** has four strands: **Prevent**: to stop people becoming terrorists or supporting terrorism **Pursue:** to stop terrorist attacks **Protect:** to strengthen our protection against a terrorist attack **Prepare:** to mitigate the impact of a terrorist attack
Counter Terrorism Policing Headquarters	CTPHQ	Around the UK there are eleven regional counter terrorism units (CTUs) and intelligence units (CTIUs). These units collaborate daily to confront the threat from terrorism. They have officers and staff working in a range of specialist fields such as investigations, forensics, digital exploitation, financial inquiries, community liaison and communications. At the centre of the network sits the Counter Terrorism Policing Headquarters (CTPHQ), which devises policy and strategy, coordinates national projects and programmes, and provides a single national Counter Terrorism Policing voice for key stakeholders including government, S.23(1) and other partners.
Data Controller		Has the same meaning as in section 1(1) of the DPA, that is, the person who determines the manner in which and purposes for which Personal Data is or is to be processed either alone, jointly or in common with other persons
Data Protection Act 2018	DPA	Includes all codes of practice and subordinate legislation made under the DPA from time to time

Data Subject		Has the same meaning as in section 1(1) of the DPA being an individual who is the subject of Personal Data
Freedom of Information Act 2000	FOIA	Includes the Environmental Information Regulations 2004 and any other subordinate legislation made under FOIA from time to time as well as all codes of practice
Homeland Security Group	HSG	
Human Rights Act 2018	HRA	Includes all subordinate legislation made under the HRA from time to time
Information		Any information however held and includes Personal Data, Sensitive Personal Data, Non-personal Information and De-personalised Information. May be used interchangeably with 'Data'
Information Commissioner's Office	ICO	The independent regulator appointed by the Crown who is responsible for enforcing the provisions of the DPA and FOIA
Metropolitan Police Service	MPS	The police force for the London metropolis area (excluding the City of London)
Management of Police Information	MOPI	The principles of management of police information (MoPI) provide a way of balancing proportionality and necessity that are at the heart of effective police information management. They also highlight the issues that need to be considered in order to comply with the law and manage risk associated with police information.

COUNTER TERRORISM POLICING

Mayor's Office for Policing and Crime	MOPAC	The Mayor of London, as occupant of the Mayor's Office for Policing and Crime (MOPAC) is required by law to produce a plan that explains how the police, community safety partners and other criminal justice agencies will work together to reduce crime. The Police and Crime Plan reflects the Mayor's manifesto and priorities for making London a safer city for all Londoners and the Mayor's Office for Policing and Crime (MOPAC) is the strategic oversight body tasked with devising the Police and Crime Plan and ensuring that it is delivered over four years
S.24(1), S.31(1) [redacted]	[redacted]	CT secure server
Notification		The Data Controller's entry in the register maintained by the Information Commissioner pursuant to section 19 of the DPA
Prevent Case Management Tracker	PCMT	Data application for recording and managing Prevent cases
Personal Data		Has the same meaning as in section 1(1)(a) to (e) of the DPA, that is, data which relates to a living individual, who can be identified from it, or data that can be put together with other information to identify an individual and includes expressions of opinion and intentions.
Process		Has the same meaning as in section 1(1) of the DPA and includes collecting, recording, storing, retrieving, amending or altering, disclosing, deleting, archiving and destroying Personal Data
Pseudonymous		Information that has never referred to an individual and cannot be connected to an individual.

Special Category Data		Special category data is information relating to racial, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics, health, sex life / orientation, criminal convictions and offences, related security measures or appropriate safeguards.