

## National Counter Terrorism Policing HQ COVERING SHEET

This document is **OFFICIAL SENSITIVE**.

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

|                                         |                                                                                                                                                                                                           |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>STORAGE</b>                          | Stored in a CPNI approved Class 2 cabinet in an individual's tray, in a secure room.                                                                                                                      |
| <b>MOVEMENT WITHIN BUILDING</b>         | In an unsealed envelope by trusted hand.                                                                                                                                                                  |
| <b>MOVEMENT OUTSIDE OF BUILDING</b>     | By trusted hand in a single cover, or;<br>Using a signed for postal service under a single cover. No protective markings should be displayed and a return address must be on the reverse of the envelope. |
| <b>REVIEW</b>                           | In no more than 6 years' time from the originating dates of the document.                                                                                                                                 |
| <b>DESTRUCTION</b>                      | <b>Not</b> suitable for waste sacks - must only be cross-shredded                                                                                                                                         |
| <b>PROTECTIVE MARKING</b>               | <b>OFFICIALSENSITIVE</b>                                                                                                                                                                                  |
| <b>SUITABLE FOR PUBLICATION SCHEME?</b> | N                                                                                                                                                                                                         |
| <b>TITLE AND VERSION</b>                | Prevent Case Management Tracker (PCMT) Code of Conduct                                                                                                                                                    |
| <b>PURPOSE</b>                          | Policy and Procedure                                                                                                                                                                                      |
| <b>RELEVANT TO</b>                      | PCMT                                                                                                                                                                                                      |

# Prevent Case Management Tracker Application S.24(1), S.31(1) Code of Conduct

Version 2.0, draft 3.2

9<sup>th</sup> April 2026

## Document Ownership

This document is own/ed by CTPHQ.

## Document control

| VERSION CONTROL |            |                                                                                                  |           |
|-----------------|------------|--------------------------------------------------------------------------------------------------|-----------|
| Version         | Date       | Record of Change                                                                                 | Authority |
| V0.1            | 21/03/2018 | Initial draft                                                                                    | S.40(2)   |
| V1.2            | 01/06/2018 | Second Draft                                                                                     | S.40(2)   |
| V1.3, draft 1   | 6/5/2021   | Minor update.                                                                                    | S.40(2)   |
| V1.3, draft 2   | 11/5/2021  | Incorporates feedback from MoD                                                                   | S.40(2)   |
| V1.3, Issued    | 11/5/2021  |                                                                                                  | S.40(2)   |
| V2.0, draft 1   | 20/3/2023  | Review to support the use of the PCMT by Channel Partners, including input from Gareth O'Hanlon. | S.40(2)   |
| V2.0, draft 2   | 3/4/2023   | Updated to reflect feedback from S.40(2)                                                         | S.40(2)   |
| V2.0, draft 3   | 25/3/2024  | Updated to align with the DPIA.                                                                  | S.40(2)   |
| V2.0, draft 3.1 | 27/3/2024  | Updates to reflect feedback from meeting to review Data Sharing Agreement.                       | S.40(2)   |
| V2.0, draft 3.2 | 09/04/2026 | Document refresh, minor updates                                                                  | S.40(2)   |

## Contents

|     |                                                                           |    |
|-----|---------------------------------------------------------------------------|----|
| 1   | Document Purpose.....                                                     | 6  |
| 2   | Purpose .....                                                             | 7  |
| 3   | National Security Operating Procedures and Local Policy & Procedure ..... | 8  |
| 4   | Access to the PCMT .....                                                  | 9  |
| 4.1 | Staff Vetting.....                                                        | 9  |
| 4.2 | Training .....                                                            | 9  |
| 4.3 | Authorisation .....                                                       | 9  |
| 5   | Expectations of Conduct & Behaviour.....                                  | 10 |
| 5.1 | Breaches of PCMT Code of Conduct.....                                     | 11 |
| 5.2 | Logging and Monitoring.....                                               | 11 |
| 6   | Legal and Policy Context.....                                             | 13 |

## 1 Document Purpose

This code sets out specific rules governing the use of the Prevent Case Management Tracker application (PCMT) S.24(1), S.31(1) [REDACTED] Note this includes the enhancements to the original PCMT application required for use by Channel Partners.

**All PCMT users must read and comply with this Codes of Conduct regardless of their role, responsibility, permissions and use of the application.**

You are personally responsible for all actions undertaken (using your account login).

It is important that all users are aware and understand their responsibilities under this code. Users will be required to re-confirm this acknowledgement at regular intervals.

Should a prospective PCMT user be unclear about any part of this Code of Conduct, they should seek clarification from their supervisor, or alternatively CTPHQ via the mailbox S.24(1), S.31(1) [REDACTED]

## 2 Purpose

### General

The PCMT should be used specifically for the recording and case management of information related to Counter Terrorism (CT). And more specifically, must only be used for the following 'Approved' purposes:

- Protecting life and property;
- Preserving order;
- Preventing the commission of offences;
- Bringing offenders to justice;
- Any duty or responsibility of the police arising from common or statute law.

Note with the early identification of vulnerable persons who are suspected of being radicalised towards terrorism, the use of PCMT will contribute to addressing a pressing Social Need in:

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

The PCMT was commissioned to host information referred from the Police CT network along with statutory partners, other agencies and the public. All referrals made are subject to assessment for case management. PCMT is designed to support the agreed business policies and defined processes in respect of how this is achieved operationally. These include nationally agreed standards in respect of information assessment, management, linking and access (delivering data availability, integrity and structure).

Whilst there is a conscious effort to be as publicly open and transparent as possible, the CT network has to be discreet about the publicity of the PCMT, the information held and its usage, as well as techniques and coverage. Users should be mindful of the role that PCMT will play in the National Security effort and the fact that the information that will be contained within it will be subject to protective marking. Users should not reference in public or extensively brief to the wider policing network the existence of the PCMT, platform on which it operates S.24(1), or any associated applications without the prior approval of the Security Compliance & Government unit (SCGU) in CTPHQ:

S.31(1)

### HSG

Staff in HSG Counter Terrorism Analysis and Insight require access to PCMT S.24(1), S.31(1) for the purpose of producing national statistics. Note the information accessible to HSG staff is restricted to those cases which have been referred into Channel on a S36 CTSA decision.

### 3 National Security Operating Procedures and Local Policy & Procedure

This Code of Conduct is in addition to the Security Operating Procedures (SyOPs) for S.24(1), [REDACTED] and 'Standard Operating Procedure (SOP) for Prevent Case Management. Users are bound to comply at all times.

When using the PCMT all users are expected to adhere to the related training, policies and guidance for the management of information and cases, for example:

- CTP users: 'Police Information and Records Management', including 'Authorised Professional Practice' (APP) and CTPHQ Prevent PCMT RRD Policy with regard to RRD;
- Channel users: 'Approved purposes' and RRD policy (HSG).

Additionally, users are bound by any local policy or procedure concerning, printing, data transfer, or any other concerning the lifecycle of data held on or in relation to the PCMT.

## 4 Access to the PCMT

### 4.1 Staff Vetting

The user requirements to access the PCMT include;

- S.24(1), S.31(1)

The SCGU on behalf of the S.24(1) 'Senior Information Risk Owner' (SIRO) reserves the right to deny access or remove users, without notice, from the PCMT who do not meet the personnel security baseline requirements.

### 4.2 Training

In addition to the vetting requirements - Prior to being granted access to the PCMT all users must have completed the training required for their specific role. For example:

- Practitioners, Gatekeepers and Supervisors, Regional Analysts (PCMT) - must attend the one day training course
- Business Administrators (PCMT) – must attend a one-day training course
- PCMT View Only – Must complete the training guide provided detailing the functionality.
- National Analysts (PCMT) – Must complete the training guide detailing the functionality.

The SCGU on behalf of the S.24(1) SIRO reserves the right to deny access or remove users, without notice, who are not appropriately trained.

All Users should read the PCMT Standard Operating Procedures.

### 4.3 Authorisation

CT Police officers and staff are permitted access to the PCMT S.24(1), S.31(1) subject to the requirements of their respective role, and a commitment to adhere to the S.24(1) SyOps and PCMT Code of Conduct;

Staff from Channel partners, including the HSG, are permitted access to the PCMT using S.24(1), (corporate devices), subject to their respective role, and a commitment to adhere to S.24(1), SyOps and PCMT Code of Conduct;

Officers / staff from other Partner agencies (e.g. MoD Police) requiring access to the PCMT must be truly embedded within a police environment (or other operating environment approved by CTPHQ), supervised by police, and fully supported by the relevant Information Asset Owner (IAO). Note where this applies the "Embed Agreement<sup>1</sup>" should be completed and forwarded to the CTPHQ SCGU for retention and awareness; access is subject to approval by the SCGU in CTPHQ. Finally, access is subject to a commitment on behalf of the Partner organisation to adhere to the S.24(1) Code of connection, and from a user perspective, to adhere to the S.24(1) SyOps and PCMT Code of Conduct.

<sup>1</sup> As per Annex A of D866 Information Law Request Document

## 5 Expectations of Conduct & Behaviour

As part of Information Assurance, Information Governance and risk management approach, the SCGU on behalf of the S.24(1) SIRO retains the ability to permanently or temporarily exclude personnel and / or units from the S.24(1) and services including the PCMT S.24(1), S.31(1)

Users must ensure:

- They comply with S.24(1) SyOPs and 'SOP for Prevent Case Management'
- They only use PCMT within the scope of their defined role;
- Any data input or case management is done so in accordance with the national PCMT policy and guidance;
- They adhere to any dissemination caveats or handling codes relating to information held on the PCMT;
- Any information accessed is done so in line for a discernible CT policing purpose or safeguarding purposes in accordance with legislation and policy;
- If they are required to complete a task or action beyond the scope of their remit capabilities, or access rights, they will seek appropriate authority<sup>2</sup>, guidance and assistance.
- All use of the application will be undertaken with professionalism and integrity in line with, for example, Police Code of Ethics;
- Any search is structured in such a manner that is most likely to retrieve information that is relevant and minimise that which is not;
- Any data processing that occurs within or in relation to the PCMT must be necessary and proportionate, as well as done in an accurate, relevant and timely approach in line with any legal obligations;
- Any printing that occurs within the PCMT S.24(1), S.31(1) must be necessary and proportionate and done so using the print functionality within the application and in accordance with the PCMT guidelines. Furthermore any printed material shall be protected, stored, maintained and destroyed in accordance with its associated security classification throughout its lifecycle;
- Any potential or actual misuse of PCMT S.24(1), S.31(1) or its data must be reported to a supervisor at the earliest opportunity and subsequently brought to the attention of the SCGU;
- That sensitive data (e.g. relating to medical issues, mental health or other information of a personal nature) is appropriately marked as such on the system, particularly where that data was obtained from another agency (e.g. health services, social services, etc);
- That any material from the PCMT which is disclosed as part of a legal process (criminal or civil) or through subject access or FOIA is redacted to ensure that information which does not belong to the police (but which may appear in a PCM record) is not disclosed without permission from the information holder and must follow the ILDR D866 Policy;
- 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

<sup>2</sup>Prior authority from Supervisor, Head of Unit or Information Asset Owner

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).

#### Users must NOT

- Seek access to information for which there is not a 'need to know', e.g. POLICE ONLY information must not be accessed by Channel Partners;
- Circumvent any security measure associated with the application or alter the security or functionality;
- Undertake any action or activity which could potentially or actually prejudice the information held;
- Undertake any action or activity, which contravenes the S.24(1), SyOPs or any other policy or procedure associated to the S.24(1), S.31(1);
- Conduct any action or activity that promotes a personal interest or is for malicious gain;
- Conduct searches or access PCMT information or data for reasons other than a specific Approved purpose. Should a user do so for a personal or private business purposes, or do so in relation to themselves, other users, family members, friends, neighbours, acquaintances or public figures (without prior express approval<sup>3</sup>), they will be considered to have breached of the code of conduct;
- Alter or restrict the access or visibility of any information in a way that may or will negatively impact on the Approved purposes for which the PCMT is being used without prior approval<sup>2</sup>;
- Delete any information in a way that may or will negatively impact on the Approved purposes for which the PCMT S.24(1), S.31(1) is being used without prior approval<sup>2</sup>;
- Use the PCMT S.24(1), S.31(1) to generate or perpetuate discrimination based on age, race, religion, ethnicity, gender, sexual orientation or disability;
- Use the browser print function to print material from the PCMT application;
- Disclose information which belongs to another agency without permission from that agency.

### 5.1 Breaches of PCMT Code of Conduct

Any breach (or near misses) of the Code of Conduct, SyOPs or policy/procedure (e.g. SOP) shall be immediately reported to a local supervisor. In addition, all PCMT related incidents (or near misses) must be reported to the Security and Governance Unit (SCGU) (CTPHQ) via the CSC as soon as practicable (S.24(1), S.31(1)).

### 5.2 Logging and Monitoring

The PCMT is designed to make all use accountable for protective monitoring and compliance purposes.

Users should note that all activity undertaken on and in relation to the PCMT is auditable both locally and centrally by CTPHQ SCGU.

CTPHQ SCGU maintains awareness of roles, remits and the scope that a user should be operating within. From this information the protective monitoring functions identify misuse. System activity is also audited through sampling.

Any suspicious action or activity identified on the PCMT will be appropriately challenged and required to be justified to the relevant Information Asset Owner and CTPHQ SCGU.

Any such identified activity may result in local disciplinary procedures and / or criminal charges. PCMT users are personally responsible for any activity recorded from their account login.

---

<sup>3</sup> Prior authority from Supervisor, Head of Unit or Information Asset Owner

Failure to comply with PCMT Codes of Conduct may result in denial of access to the PCMT and/or S.24(1) services. The SCGU on behalf of S.24(1), SIRO reserves the right to remove users access, without notice, from the PCMT who do not adhere to these Code of Conduct or whilst specific incidents are being investigated.

## 6 Legal and Policy Context

All users are required to use the PCMT S.24(1), S.31(1) in a lawful and compliant manner at all times.

Users of PCMT should note that they are required to be compliant with the S.24(1) SyOPs and associated policies and procedures that govern access and use of the S.24(1).

All users must be familiar with and abide by the data protection principles described in GDPR and the Data Protection Reform Act 2018 and only access information held for a legitimate or authorised purpose. Users must not disclose information, to unauthorised recipients (whilst working or on leave) and understand by accessing personal data without authorisation they could be committing a criminal offence, regardless of whether they then disclose that personal data.

In addition, users should be cognisant of and abide by the pertinent sections of the following Acts of Parliament and the resulting impact upon the management of information within the S.24(1)

- The Freedom of Information Act (2000) [In Scotland this is The Freedom of Information (Scotland) Act (2002);
- The Regulation of Investigatory Powers Act (2000);
- The Human Rights Act (1998);
- The Criminal Procedure and Investigations Act (1996);
- The Computer Misuse Act (1990);
- The Official Secrets Act (1989);
- The Copyright, Designs and Patents Act (1988).

If you have any questions, issues or are unsure of any aspects of the PCMT Codes of Conduct please contact CTPHQ on: S.24(1), S.31(1)