COUNTER TERRORISM POLICING

HEADQUARTERS

CTPHQ

Policy for Prevent Practitioners

Management of CT/DE Risk within the Community

V 2.0 May 2018

Official – Sensitive

Version	Date	Distribution
0.9	9th January 2018	NCTPHQ Prevent Team
1.0	15th January 2018	All Prevent staff via RPCs
1.2	7th March 2018	Author only
1.3	18th March 2017	NCTPHQ Prevent Team
1.4	22nd March 2018	OSCT, Apollo Team and Local authority partners
1.5	7th April 2018	CTPHQ SLT
2.0	9th May 2018	CT Network Publication

This version published 9th May 2018

CONTENTS

Section One – Foreword

Within a continuing and protracted period of the "severe" threat from terrorism, 2017 saw a significant uplift in the agility and frequency of terrorist attacks and attack planning. These were underpinned by low sophistication methodologies, and all too often inspired through online communication that is an integral feature of our everyday lives. Social media and the internet provides whole communities of people that can be exploited by radicalisers across all forms of extremism, and self-radicalising over short timescales is amplified when vulnerable people are drawn into private groups that become echo chambers of narrow and poisonous perspectives. This is set to remain a constant challenge for policing and our partners for the foreseeable future.

There is a need for Prevent to learn from the attacks in 2017 and continue to build on the fantastic work to respond to over 6000 annual concerns raised about potentially vulnerable people. We must innovate and improve our approach where reviews have indicated that better information sharing, better risk assessments, more intensive safeguarding interventions and risk management, or a greater degree of challenge and support across services and partnerships could have made a difference. In order for Prevent to be highly effective in intervening early, we must ensure our responses are robust, consistent and underpinned with sound professional judgement. All specialist Prevent officers and staff must possess the ability to identify, assess and manage CT/DE risk effectively if we are to continue to improve our success in preventing terrorism.

To underpin our continuous professional development, the launch of the PGA and DIF tools, based on rigorous academic study, provide for the first time a way for Prevent staff to identify and manage risk consistently across the country. The Prevent policy has been designed as a framework that allows regions to identify, promote and build upon existing good practice across the network. The policy is intended to be a living document that is flexible and adaptive to future changes in the CT/DE threat, and it underpins the delivery of the national Prevent strategic plan.

The creation of a framework which encompasses the breadth and depth of the different operating environments experienced by Prevent teams across the UK has been challenging and I am thankful to both the CTPHQ team who have developed this product and to all those front line practitioners who have contributed to the process.

Nik Adams

National Co-ordinator for Prevent

Counter Terrorism Policing Headquarters

Section Two – Policy Overview

The Current Threat

Five 'successful' attacks within seven months costing 36 lives and 23 disrupted attacks in the last four years, including 10 since March 2017. Four of these 10 involved an XRW ideology. There has been significant new emerging risk and sustained additional demand across CT policing making effective prevention activity even more important.

Strategic Objectives for Prevent

This policy is a key part of delivering the strategic objectives for Prevent, namely:

Increasing trust and confidence: Clear guidance and consistency will improve delivery locally, which will improve confidence in Prevent amongst communities.

Identifying vulnerability, threat and risk: The use of the Police Gateway Assessment and Dynamic Investigate Framework will improve our ability to identify both vulnerability and risk within the cases we are managing.

Safeguarding the vulnerable: A defined process combined with use of the Police Gateway Assessment will improve our ability to identify and refer those cases which should be managed within Channel, calling on the skills and resources of key partners to safeguard those at risk.

Manage risk: The Dynamic Investigative Framework will help us to identify specific risk issues within a case and develop a Case Management Plan to manage and mitigate that risk as far as is possible.

Professionalism and consistency: This policy provides an overarching framework for local teams to work within, providing a clear step-by-step process for staff and promoting a consistent approach to Prevent work.

CT/DE Risk Management Methodology

This new policy simplifies the methodology for management of CT/DE risk by breaking it down in a smaller number of identified core activities, which must be completed for each case. To support staff in this a number of new tools have been developed to aid the assessment and prioritisation of risk and the subsequent management process. This means staff will be aware of their responsibilities at each stage of the process and more importantly will be properly equipped to assess and manage identified risk.

The biggest change is the creation of the Police Case Management Tracker (PCMT) which will replace all local recording practices on spreadsheets from July 2018 and provide a national IT system for the recording of cases and associated police activity. The PCMT has been designed to implement the same workflow as this new policy to further support staff in effective management of cases.

The Core Activities of CT/DE risk management have been identified as the following:

1. **Case Referrals**

This is the initial receipt of a referral potentially suitable for CT/DE Management, whether directly or via an Intelligence Management Unit (IMU). This section of the policy outlines clearly the requirement to record referrals on the PCMT at the earliest possible opportunity as well as the necessity for de-confliction and assessment of cases by IMUs before any activity is undertaken locally. This also addresses issues such as case responsibility where a subject is active across multiple CT(i)Us.

2. **Police Gateway Assessment**

This is the application of the Police Gateway Assessment (PGA) to identify whether the case should be managed under Channel as a Multi-Agency Led case or as a Police Led case (previously Prevent Case Management / PCM).The PGA will also identify cases unsuitable for management and exit them appropriately from the process.

3. **The Intelligence Cycle**

IMUs are the only part of the police CT Network, which have the potential to see the whole intelligence picture. It is essential that intelligence obtained through the CT/DE risk management methodology is passed back to an IMU to allow for proper assessment of any risk/threat and identification of escalation of risk. It is also critical that Chanel Panels and Chairs are fully cited on all intelligence held by police which is necessary for them to be able to make effective decisions regarding risk.

4. **Police Led Cases**

Where a case is unsuitable for Channel the ongoing case is assessed by use of the Dynamic Investigation Framework (DIF), which aids in the creation of a Case Management Plan (CMP) to identify the actions required to address vulnerabilities and reduce risk.

5. **Multi-Agency Led Cases**

These cases are managed under Channel however the police retain key responsibilities and remain responsible for any CT/DE risk. This also addresses when cases should move out of Channel and either be escalated to Pursue or be treated as a Police Led case.

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

Decisions around case closures should be made on the basis of the CT/DE risk present as opposed to any interventions made. The circumstances in which case closure is appropriate and how closures can be made are detailed here.

7. **Supervision**

Supervisors have clear responsibilities at each stage of the methodology. Proper supervision of Police activity is a golden thread that runs throughout the entire methodology.

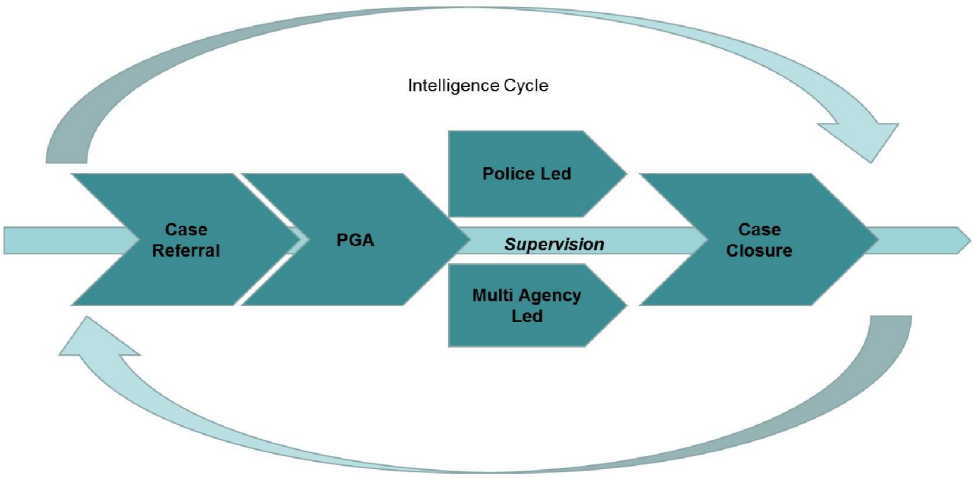


Figure 1: Component parts of the management process and how they fit together

PCMT

PCMT is a web based application which will be accessible to all CT(i)Us via their normal IT platform. The security marking for the system is Official Sensitive which means the tool will be accessible via the PNN/PSN network and will also work on laptops and tablets providing they are operating within PNN/PSN. As the platform is Official Sensitive any intelligence obtained which is Secret or above must not be recorded on PNN and instead recorded on the appropriate system as per local force guidance.

Use of the PCM Tracker is mandatory and from July 2018 this will be the only system from which Police Prevent performance data will be collated in conjunction with CMISv2.

See Appendix A for the PCMT case flow diagram.

How to use this document

- Bullet points contain the policy itself. These points consist mainly of activities which must be undertaken at certain stages of the management process, however on some occasions these points will also detail activities which must **not** be undertaken.
- A small number of points will contain considerations, here the activity being raised **must** be considered, and a rationale recorded for why it was appropriate or inappropriate to undertake the activity at the time.

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

Section Three – The Role of the CT Case Officer (CTCO)

What are CT Case Officers?

CT Case Officer (CTCO) refers to any officer or member of police staff who is actively managing cases under the CT/DE risk management methodology detailed in this policy, predominantly these will be Prevent cases. Such staff may be referred to locally as Prevent Officers, Prevent Staff, Local Operations Officers or by another name entirely. CTCOs are those who have direct responsibility for the management of a case and are distinct from supervisors and 2nd Line Managers.

Responsibilities

Training and System Access

CTCOs will:

- Be the CT Policing lead for any individual, institution or ideology under management within Prevent regardless of whether the case is managed as Police Led or Multi-Agency Led.
- Be vetted to at least Security Clearance (Enhanced) (SC(e))
- Complete the National Prevent Foundation Course (NPFC) within six months of starting role or complete equivalent NPFC Lite refresher course for those already in post
- Have current access to the PCMT (from July 2018)
- Have current access to CMISv2
- Have access to all required local force intelligence and crime systems

CTCOs will be responsible for:

Case Referrals

- Creating a PCMT record whenever a referral or potential referral is received
- Submitting any referrals for CT/DE Management to the relevant IMU for assessment and de-confliction

Police Gateway Assessment

- Upon receipt of a de-conflicted referral applying the Police Gateway Assessment (PGA) to determine the most appropriate management process (Police or Multi-Agency Led or exit from management)

Intelligence Cycle

- Ensuring all relevant intelligence obtained throughout the management process is fed back into the IMU
- Ensuring that there is a flag (or nearest equivalent for forces which do not use 'golden nominal' systems) on local force system(s) to identify interest in subject
- Identifying all activities and incidents involving a subject (e.g. missing person reports, crime allegations etc) and ensuring the relevance of all intelligence is assessed and submitted to an IMU where appropriate.
- Flagging subjects on PNC where appropriate

- Requesting flagging as Prevent case on NCIA (For NCIA forces)

Police Led Cases

- Applying the Dynamic Investigation Framework (DIF) to assess the case
- Identifying the priority banding for the case
- Using the completed DIF to create a Case Management Plan (CMP)
- Undertaking any and all activities/interventions identified within the CMP as necessary to reduce CT/DE risk and safeguard the subject
- Reviewing the DIF and CMP as frequently as required based upon risk and upon receipt of intelligence which represents a significant (or potentially significant) change to the circumstances of the case

Multi-Agency Led Cases

- Referring cases assessed via the PGA as suitable for Multi-Agency led management to the Local Authority Channel Coordinator or non Dovetail equivalent.
- For non Dovetail sites creating and maintaining the CMISv2 record
- Recording the s.36 CTSA 2015 referral justification on CMISv2
- For non Dovetail sites undertaking information gathering from partners and then completing the Vulnerability Assessment Framework (VAF).
- For Dovetail sites providing all relevant intelligence to the Local Authority Channel Coordinator (LACC) to allow them to complete the VAF
- Attending the Channel Panel as a statutory partner and fulfilling the police role as articulated within current Police Channel Guidance
- Ensure the Channel Panel is fully cited on all intelligence held by police, which is necessary for them to be able to make effective decisions regarding risk
- Risk assessing any deployment of Intervention Providers (IPs) to a subject
- Identifying any Channel case in which the risk has escalated to the point where it could be considered a potential IHM lead or Priority Operation and referring them to an IMU for urgent assessment

Outcomes and Closures

- Ensuring all policing activity has been accurately recorded on the PCMT (and CMISv2 for non Dovetail Channel cases) including the use of activity flags to show specific interventions
- Ensuring closure of cases only occurs when the vulnerability has been addressed and any risk has been appropriately managed
- Ensuring the correct closure code is recorded on the PCMT (and CMISv2 where appropriate)
- Ensuring any flagging used during management (PIW, PNC, NCIA, local systems) is removed

Section Four – The Role of the Supervisor

What are Supervisors?

Supervisors are any officer or member of police staff who are in a supervisory rank and who have direct line management responsibility for CTCOs. Non-supervisory ranks (e.g. constable or lowest band police staff) should never undertake the role of supervisor. Acting ranks are acceptable providing it has been officially sanctioned by the local force.

Responsibilities

Training and System Access

Supervisors will:

- Be vetted to at least Security Clearance (Enhanced) (SC(e))
- Complete the National Prevent Foundation Course (NPFC) within six months of starting role or complete NPFC Lite refresher course for those already in post
- Have current access to the PCMT (from July 2018)
- Have current access to CMISv2
- Have access to required local force intelligence and crime systems

Supervisors will be responsible for:

Police Gateway Assessment

- Allocation of cases for management to CTCOs
- Supervision of the PGA

Police Led Cases

- Supervision of the DIF
- Supervision of the CMP

Multi-Agency Led Cases

- For non-Dovetail sites, supervision of all police entries on the CMISv2 record
- Supervision of the s.36 CTSA 2015 referral justifications on CMISv2
- For non-Dovetail sites supervision of the VAF
- Ensuring appropriate police attendance at the Channel Panel

Outcomes and Closures

- Supervision of closure justification
- Completion of all supervisory tasks on both PCMT and CMISv2
- Confirming correct outcome code has been selected on PCMT (and CMISv2 where appropriate)
- Closure of case on PCMT
- Confirming removal of any flagging used during management (NCIA, PNC, PIW etc)
- Overall supervision of each case, ensuring CTCOs are applying the CT/DE management methodology appropriately and to the required standard

Section Five – Case Referrals

- Regional Prevent Co-ordinators (RPCs), CTCOs and supervisors should promote the use of the national Prevent referral template with all partners in their area where appropriate.

There are a number of advantages to a single National Prevent referral document. The document ensures a minimum level of information (e.g. biographical information, nature of vulnerability, and CT/DE risks) is provided which will improve the quality of referrals overall. It also clearly signposts to IMUs that CTCOs are the intended output for the referral. CTPHQ cannot mandate the use of these forms by partners but RPCs and CTCOs can promote and support adoption in local areas. It is acknowledged that some partner agencies will have standard referral forms for wider purposes or processes that make it inappropriate to adopt the national form.

- Where a partner contacts a CTCO asking for advice on a matter not previously referred then it must be made clear to that partner whether this is considered to be a referral or not.

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

- Where local practices (such as a MASH or other 'front door') result in partner referrals being sent to an IMU prior to any Prevent team, IMUs must consider early dissemination to Prevent teams to allow the recording of referrals on the PCMT at the earliest possible stage.

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

- CTCOs will provide acknowledgement to the referrer that a referral has been received. It is a matter for local teams as to whether more detailed information about the case is provided.

- All referrals and potential referrals received by a CTCO will be registered on the Police Case Management Tracker (PCMT) at the first point of receipt, even if this is pre-de-confliction by an IMU.

This ensures that referrals are not 'lost' within the system during de-confliction. It gives local teams an opportunity to follow up with IMUs in cases where a referral is not received back following de-confliction (For example, due to a 'no CT/DE relevance' assessment under RADO).

- All referrals received by a CTCO must be submitted to an IMU for de-confliction and assessment, if this has not already been carried out.
- No activity must be carried out before de-confliction and assessment by an IMU. The only exceptions to this are:

    - When the quality of referral is insufficient and the referrer needs to be contacted to provide more information
    - The IMU specifically requests activity to assist in the assessment process
    - Obtaining supplementary biographical data from local policing systems

    De-confliction is not considered complete until a date of de-confliction is provided by the IMU alongside a reference number (e.g. NCIA reference or other internal log number).

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

- All referrals assessed by a IMU which:
    - Are submitted on the National Prevent Referral Template;
    - Are clearly intended by the referrer for Prevent; or
    - Include a subject with an identified or potential vulnerability to radicalisation

    must be disseminated to the local Prevent team regardless of whether it is assessed to have no CT/DE relevance. The only exception to this is when the referral outcome is assessed as a Priority Investigation or IHM Lead not suitable for Prevent.

- Where a referral has been submitted on a National Prevent referral template, the IMU must attach this to the disseminated product following de-confliction and assessment.

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

- At the point of dissemination to Prevent, IMUs should where possible provide full details of all research (excluding intelligence marked Secret and above) completed during assessment. This will include the NSIM minimum standard checks:

    - Secure CT intel system;
    - Local Intelligence and Crime Systems;
    - Police National Computer;

- Police National Database; and
- CT Holmes

Some IMUs complete more detailed checks than this, however these are the minimum standards.

IMU disseminations sometimes list the checks undertaken but not relevant results, this means CTCOs must duplicate the work of the IMU and check the same records. Where the dissemination process allows IMUs should provide the actual details of the research carried out.

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

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

- Where another part of the CT Network is requesting that CTCOs manage any aspect of CT/DE risk this should be treated as a Referral and subjected to this policy.

In the future other CT Network management processes may include Prevent as an outcome. If CTCOs are being asked to manage the risk then they should do so in line with the agreed process. This is separate from a tasking such as asking CTCOs to make a visit as part of an IHM lead process which would not be subject to this process nor recordable on PCMT.

Section Six – Police Gateway Assessment

- All cases relating to an individual disseminated to Prevent following IMU assessment and de-confliction will be assessed using the Police Gateway Assessment (PGA), **within 5 working days** where possible. This includes cases where an IMU have assessed no CT/DE relevance.

Historically CT/DE relevance has not been defined within NSIM leading to an inconsistent application across the country, particularly with regards to Prevent. NSIM v3.0 now defines CT/DE relevance in such a way that it is expected that the wider remit of Prevent will be acknowledged during assessment, and this is supported by new training for assessors within IMUs. However it is expected that it may take time to embed these new definitions and processes within IMUs and the PGA provides an additional contingency during this time to ensure that all cases potentially suitable for Prevent are seen and appropriately considered.

- The PGA also replaces the previous 3Ms checks. Where the PGA results in a case exiting Prevent there is no necessity to create a CMISv2 record to record this as it will be recorded on the PCMT.
- The subject must be researched against the following intelligence indices prior to assessment under the PGA
    - Police National Computer Record
    - Police National Database
    - Local force crime database
    - Local force intelligence database
    - Open Source

  These checks (with the exception of Open Source) will have been completed already during IMU assessment and de-confliction and there is no requirement to repeat them providing the results of these checks are known to the CTCO applying the PGA and there has been no significant time delay between the IMU assessment and the completion of the PGA.
- In the majority of cases further enquiries with Partner agencies will not be required to complete the PGA however where a particular agency clearly has significant relevant information regarding any individual which would aid the PGA then of course this should be requested.

The PGA has been designed as an initial assessment and triage tool and as such should not require additional research with partner agencies. The Dynamic Investigation Framework (DIF) and the Vulnerability Assessment Framework (VAF) come after the PGA and both require more detailed research.

- The completed PGA must always be submitted to an IMU as part of the intelligence cycle.
- Where the subject is a foreign national then consideration must be given to contacting the Foreign and Commonwealth Office (FCO), ACPO Criminal Records Office (ACRO) and Immigration Services to identify whether subject has any

convictions abroad or whether other intelligence about activities outside the UK is held.

- Where the concern is related to domestic extremism (DE) then consideration must be given to contacting CTP-NOC to see if any intelligence is held.
- Full details of the assessment under the PGA must be recorded on the PCMT
- A visit to the subject should not be necessary to complete the PGA. Where the CTCO or their supervisor deems a visit necessary at this early stage then consideration must be given as to who is best placed to carry it out. In many cases a partner agency such as education, health or social services may have an existing relationship with the individual or family and may be better placed to attend, either by themselves or as part of a dual visit with a CTCO. **Any consent issues for Channel/Dovetail should not be addressed directly with the subject at this early stage** unless the subject themselves raise the issue.

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

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

Section Seven – The Intelligence Cycle

- IMUs are the only part of the police CT Network who have the potential to see the whole intelligence picture. It is essential that intelligence obtained through the CT/DE management methodology is passed back to an IMU to allow for proper assessment of any risk/threat and identification of escalation of risk. Predominantly Prevent teams will be engaging with Fixed Intelligence Management Units (FIMUs) but on some occasion may also be working alongside OIMUs (Operations Intelligence Management Units).
- All biographical information obtained on a subject or associates during the Prevent process must be submitted to the IMU
- Any intelligence, which either does, or has the potential to change the DIF assessment, Case Management Plan or VAF must be submitted to an IMU, this includes intelligence obtained through attendance at a Channel panel or other partnership interaction as well as PGA, DIF or VAF assessments. It must be made clear on the intelligence submitted whether the risk in the case is escalating, de-escalating or remaining static. **This must be undertaken for both Police and Multi-Agency led cases.**
- If no other submissions have been made to an IMU then an up to date summary should be submitted to the IMU every 3 months.

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

- For Multi-Agency Led cases all relevant intelligence necessary for the effective management of risk must be shared with the Channel Panel and Chair.
- All CTCOs must consider adding a flag (or nearest equivalent for forces which do not use 'golden nominal' systems) on local force system(s) to identify interest in subject.
- All CTCOs must consider whether to flag subjects nationally on PNC via an overt and/or covert intelligence marker. Any overt markers must include 'a do not disclose to subject' text. The marker should explain the potential vulnerability and need for information to be passed back to the CTCO. Consideration and decision must be recorded on the PCMT.

Overt flagging ensures that where a subject is encountered outside of the CT network then officers will be able to identify that the subject is under management and if necessary contact the CTCO with any urgent intelligence. Covert flagging ensures that CTCOs are made aware whenever there is an interest in a subject.

It is desirable to obtain a national policy position on flagging of subjects on PNC which presents a clear position and standard wording of such flags. This requires further work with the National PNC board and Chief Officers and will be form part of later versions of this policy document.

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

- All Prevent teams must have access (directly or via IMUs or Force Intelligence Units) to the Police National Database (PND) to allow regular checks with other UK Police Forces to see if subjects have come to notice elsewhere in the country.
- Where necessary the CTCO must make further enquiries in relation to crime investigations, missing person enquiries or other non CT policing incidents in order to ensure they have a full understanding of the relevant incident, including any intelligence products that have been generated (eg. cell site data, phone downloads etc)
- Any intelligence received or generated which is relevant or potentially relevant to another force must be transferred to them through the local force transfer process (e.g. an intelligence report marked up as suitable for dissemination to another area).
- For any subjects who show a propensity to travel to areas of conflict or who are juveniles, consideration must be given to requesting CTP-POC create a Police Intelligence Watchlist (PIW) entry.
- Where a PIW request is made CTCOs must ensure that both CMISv2 (where appropriate) and PCMT records clearly articulate the travel risks and any other relevant information staff at ports may require in order to make a decision under schedule 7 of the Terrorism Act 2000 or other relevant legislation.

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

Section Eight - Police Led Cases

- Police Case Management (PCM) / Police Management (PM) of cases will now be known as Police Led (PL) cases

Police Case Management or Police Management implies the management of the case is by police alone and there is no role for partners. The reality of management outside of channel is that partner agencies are often just as involved. The move to Police Led and Multi-Agency Led makes it clear who is leading on the management but also allows for partner involvement

- The Dynamic Investigation Framework (DIF) must be applied to all Police Led cases within five days of PGA completion.
- The minimum research which must be undertaken prior to completion of a DIF is the same as the PGA with the addition of a request for any relevant partner intelligence

The DIF is a more detailed assessment than the PGA and helps to create the associated Case Management Plan (CMP). For that reason there must be a much wider consideration of the risk including partner held intelligence so that all risks are identified.

- Every Police Led case must have a priority grading (High or Standard) informed by the DIF and recorded on the PCMT

Priority Banding Definitions

HIGH PRIORITY: suggesting potentially higher or imminent or explicit risk factors – e.g.: the presence of one or more Mobilisation behaviours, or a cluster of other factors that are particular concerning within the OIC's assessment of their context in relation to the Subject.

STANDARD PRIORITY: suggesting potentially moderate or developing or inferred risk factors – e.g.: at least one corroborated risk factor identified through the DIF, requiring further investigation or intervention. Most Police Led Subjects will likely fall within this band.

- Every Police Led case will have a current Case Management Plan (CMP). This CMP should be based on the DIF assessment and each risk identified during the DIF should have an associated action on the CMP.
- Actions within the CMP must have clear timescales for completion and should include contingency planning where appropriate.
- DIFs, Case Management Plans and priority grading must be reviewed on a frequency agreed between the CTCO and the supervisor. The assessed risk and priority grading will inform the frequency of review and this frequency should be recorded on the CMP itself. The maximum frequency between reviews should be no more than four weeks for High Priority cases and eight weeks for Standard Priority cases. These timescales do not apply to cases which are being monitored (see case closure section).

- The DIF, CMP and priority grading must be reviewed whenever there is a **significant change** in the case. A significant change is defined as any information or intelligence received which has the potential to change either the assessment of the case (DIF), priority banding or CMP.

This ensures the creation of a plan to address all risks identified as a result of the DIF process. The use of both a fixed and dynamic review criteria ensures that the assessment of the case and associated CMP are both regularly reviewed but also respond to changes in the case as management continues.

- The initial DIF must always be submitted to an IMU as part of the intelligence cycle. For subsequent DIFs it is necessary to submit only those factors which have undergone any sort of change since the last assessment.
- Consideration should be given to a referral to Mental Health Hub where appropriate as per any local process
- Any intervention or action by Police or a partner must be recorded on the Actions page of the PCMT except where it does not match one or more of the pre-existing list of activities. Regardless of whether a suitable option exists within the page, an entry must be made on the notes page of the PCMT detailing what has taken place.

Section Nine – Multi-Agency Led Cases

- Multi-Agency Management of Prevent cases will now be known as Multi-Agency Led

Multi-agency management implies a lack of role for police within the process when the reality of management within Channel is that police still lead on CT/DE risk. The move to Police Led and Multi-Agency led makes it clear who is leading on the management but also allows for partner/police involvement.

- Subjects who are a current Subject of Interest (SOI) or who are the focus of a current covert investigation cannot be a Multi-Agency Led case and must be dealt with as a Police Led case.

This is a requirement from the OSCT, such cases should be extremely rare as they will normally sit within the Pursue space.

- Dovetail Sites:
  - Cases assessed as suitable for Multi-Agency Led must be referred to the Local Authority Channel Coordinator (LACC) **within 5 days** of FIMU assessment and de-confliction.
  - The decision to refer to the LACC must be endorsed by a supervisor (Sergeant or above, or police staff supervisor). This must be recorded on the PCMT.
  - The Police must ensure that all relevant police intelligence is available to the Local Authority Channel Coordinator who will create the VAF.
- Non-Dovetail sites:
  - The Police must create the CMISv2 record and ensure the minimum standards for data entry are complied with as per CMISv2 standards.
  - The Police must undertake information gathering with partners and then complete the Vulnerability Assessment Framework (VAF) **within 20 days** following IMU de-confliction and assessment. See Appendix B for all Channel time scales

Within Dovetail sites the LACC will take responsibility for creating and maintaining the CMISv2 record and completing the VAF. For non-dovetail sites this responsibility remains with the Police.

- For both Dovetail and non Dovetail sites a police decision must be taken to determine the suitability of the case for Channel under s.36 of the Counter Terrorism and Security Act 2005. This must be taken **within 20 days** of IMU de-confliction and assessment. In Dovetail sites the LACC will approach the police to make this decision. In all instances, this decision must be endorsed both on the PCMT system and CMISv2 by a police supervisor.

The decision to refer to Channel is a legal one under s.36 of the CTSA 2015. The current Dovetail/Channel guidance requires a police supervisor to make this decision.

- The Police will attend every Channel Panel held within their local authority area as a statutory partner and fulfil the role as outlined in the current Channel Guidance document.
- In all cases the CTCO must ensure that the LACC, Channel Panel and Channel Chair are supplied with all relevant Police Intelligence necessary to allow the panel to effectively the manage the risk in the case.
- The CTCO must ensure that all intelligence obtained through the Channel process, whether it be from the LACC, Partners, Channel Panel meetings or via minutes, is submitted to the IMU.
- In cases where there are reasonable grounds to suspect the CT/DE risk is escalating to the point where it may satisfy the requirements of an IHM lead or Priority Investigation, the case must be discussed with the local IMU and consideration given to removing it from Multi-Agency Led management. Whilst approval of the chair should always be sought in such circumstances, in the event of a dispute the police retain an executive power to remove such cases.

This prevents cases which escalate in risk during management from remaining inappropriately within Channel. The new processes around feeding back intelligence should prevent these circumstances from occurring however this requirement provides a safety net should risk escalate quickly.

- Where a Channel panel rejects a case as unsuitable, the CTCO must consider whether a CT/DE risk remains. If so then it must be dealt with as a Police Led case. Where there is no CT/DE risk but a safeguarding risk remains the case must be exited to the appropriate safeguarding service (e.g. local MASH).
- Where Channel have accepted a case and subsequently closed it, should the CTCO believe that a CT/DE and/or safeguarding risk remains consideration should be given to whether the case should be dealt with as a Police Led case or exited to a safeguarding function such as a MASH.
- Except where the CT/DE risk has escalated, the police cannot remove a case from Channel without the agreement of the panel. Where there is a dispute between the police and other agencies on this issue it should be recorded on the PCM Tracker. If the dispute cannot be resolved between supervisors or 2nd line managers, then it should be referred to the Regional Prevent Co-ordinator or their deputy.
- Consideration should be given to a referral to a Mental Health Hub by the Channel Panel and completed by the CTCO where appropriate, as per any local process
- The CTCO must risk assess all deployments of an Intervention Provider (IP). This assessment must focus on whether the subject being deployed to poses any risk of harm to the IP as opposed to an assessment of general CT/DE risk.
- Any intervention or action by Police or a partner must be recorded on the Action page of the PCMT except where it does not match one or more of the pre-existing list of activities. Regardless of whether a suitable option exists within the Action page, an entry must be made on the notes page.

Section Ten – Outcomes, Case Closures and Case Transfers

- Cases in either space (Police Led or Multi-Agency Led) can only be closed where:
  - The subject could not be located
  - The case was escalated to the Pursue space
  - There was no actual CT/DE concern
  - There was no actual CT/DE concern however there was a non-CT issue referred on
- Additionally Police Led cases can be closed where:
  - The risk in the case has decreased to a level at which management is no longer necessary in order to protect the subject from the risk of radicalisation or the public from harm.
  - Otherwise with the permission of the Regional Prevent Co-ordinator. Such cases must show a clear justification on PCMT as to why management or escalation cannot be undertaken despite a CT/DE risk remaining
- Additionally Multi-Agency Led cases can be closed where:
  - The Channel panel has adequately addressed all CT/DE and Safeguarding concerns
  - The Channel panel has determined that the subject already has sufficient support in place to address all CT/DE and Safeguarding concerns

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

- If it is necessary to observe the subject for a longer period of time before judging the impact of management on risk then such cases must not be closed. Instead the case must be shown as monitored by changing the priority banding to 'monitored' and a new DIF and CMP completed to show the frequency with which the case will be reviewed. Intervals between review of monitored cases must be no longer than three months. Monitored cases must be shown as open. Monitoring may also be used for circumstances where an individual is not in the community for a short period, e.g. is going abroad for three months, or has been sentenced to a short custodial period (e.g. 12 weeks), but it is not appropriate to close the case.

Priority Banding Definition:

MONITORING – outcomes demonstrate that, depending on behaviour actions and personal context: Voluntary desistance of the specific Risk Priorities identified, the specific Risk Priorities have been deterred from, or denied continuation, apparent and progressing disengagement from concerning Associations / Ideologies

- All cases closed at initial assessment must have a completed and supervised PGA.

- All relevant activities which have taken place during case management must be selected within the PCMT Actions page and described in detail on the notes page.

Activities have replaced the Deter, Deny, Prosecute outcome codes. The use of activities allows for more accurate recording as multiple interventions can be recorded against a single case and do not require case closure to be counted.

- All cases under Police Led Management must have a DIF completed and supervised at the point of closure.
- Supervisors can authorise case closure for all cases except where a case is closed with an unaddressed CT/DE risk (RPC authority is required for such cases).

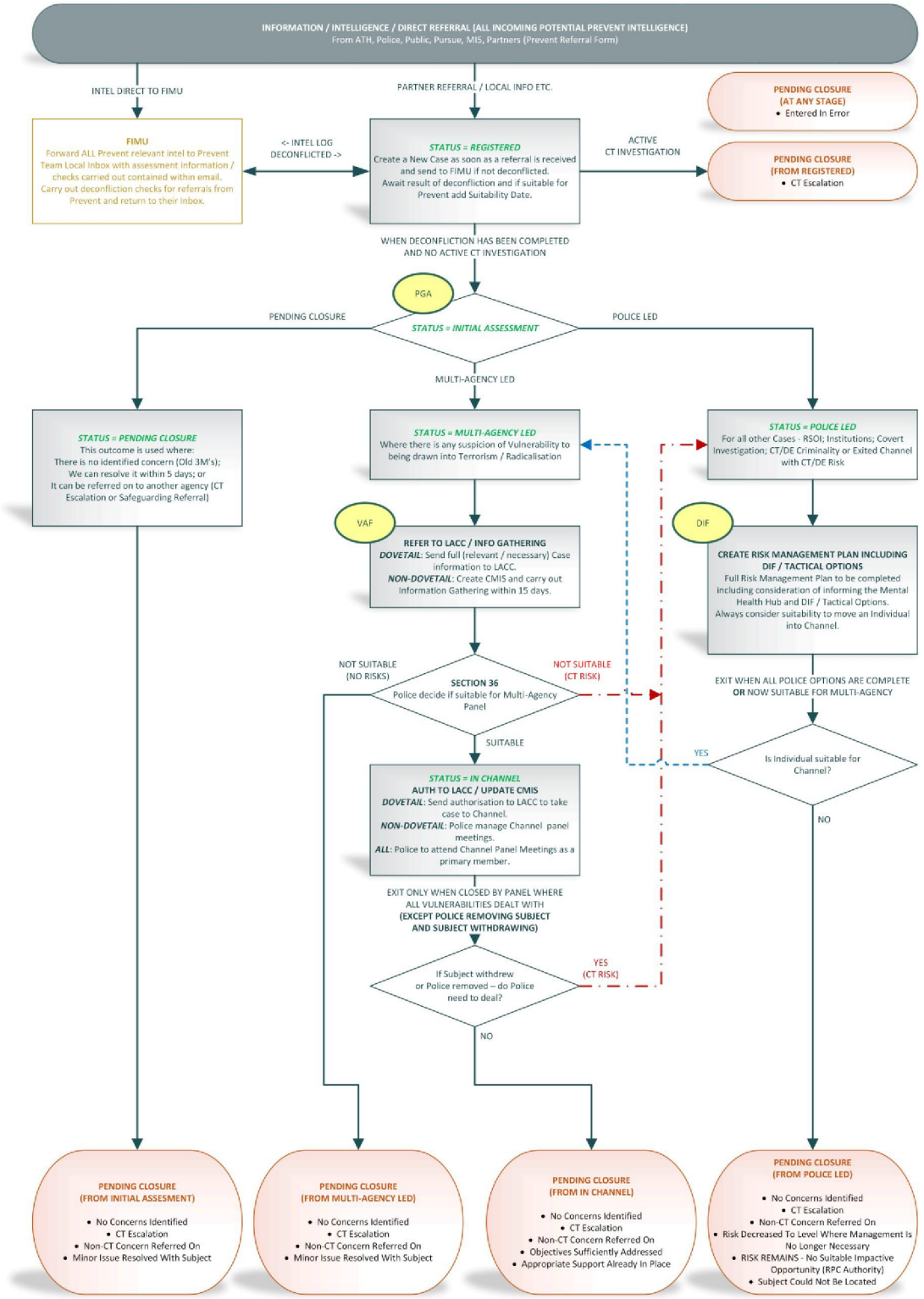
These requirements ensure that the risk is assessed at the end of management to confirm it is stable and not escalating.

- In the event of a case transfer between areas, the outgoing force must contact the new force at the point at which the move or potential move first becomes known
- The general principle is that cases should be managed where the risk is and the NSIM multi-equity principles should be applied. In cases where a subject is detained under mental health or immigration legislation in an area outside of their normal place of residence, the relevant areas should discuss the case and decide upon the area must suited to continue management of the case on the basis of risk. Where such cases are under Channel, transfers are not a police decision and instead sit with the Channel Panel. In such cases Home Office Channel Guidance must be followed.
- Any case transferring between areas must have a DIF/VAF completed at the point of transfer by the outgoing force (with the exception of Dovetail cases in which the LACC will complete an outgoing VAF if appropriate).
- The receiving force must complete a new DIF/VAF upon receipt of the case (with the exception of Dovetail area cases) and if it is a Police Led case a new CMP must also be completed and supervised reflecting the change in circumstances arising from the move between areas.

Section Eleven – Supervision

- Supervisors must be of at least the rank of Sergeant or Police Staff supervisor (acting ranks are allowed providing the force has formally approved the acting rank). Constables and lowest Police Staff grades must never supervise cases.
- Supervision is mandatory for all PGAs, DIFs, Police created VAFs, Closure Reports, Case Management Plans and Police generated CMISv2 entries, and must be recorded on the PCMT.
- Cases must be supervised with a frequency of no less than four weeks for High Priority Cases or eight weeks for Standard Priority Cases unless the case is monitored.
- Monitored cases must be supervised at least every three months.
- Supervisors should ensure that firstly the correct process is being followed under policy and then secondly that the process is completed to the required standard. This includes reviewing use of the PGA, DIF and VAF to ensure they have been completed to the required standard and that associated CMPs address all of the identified risks and that the proposed actions are specific, measurable, achievable, proportional and timely.
- 2nd line managers must ensure that they establish a process to review a proportional number of cases within their area to ensure a consistent standard of decision making, case management and supervision.

Appendix A – PCMT Process Map



Appendix B – Channel Timescales