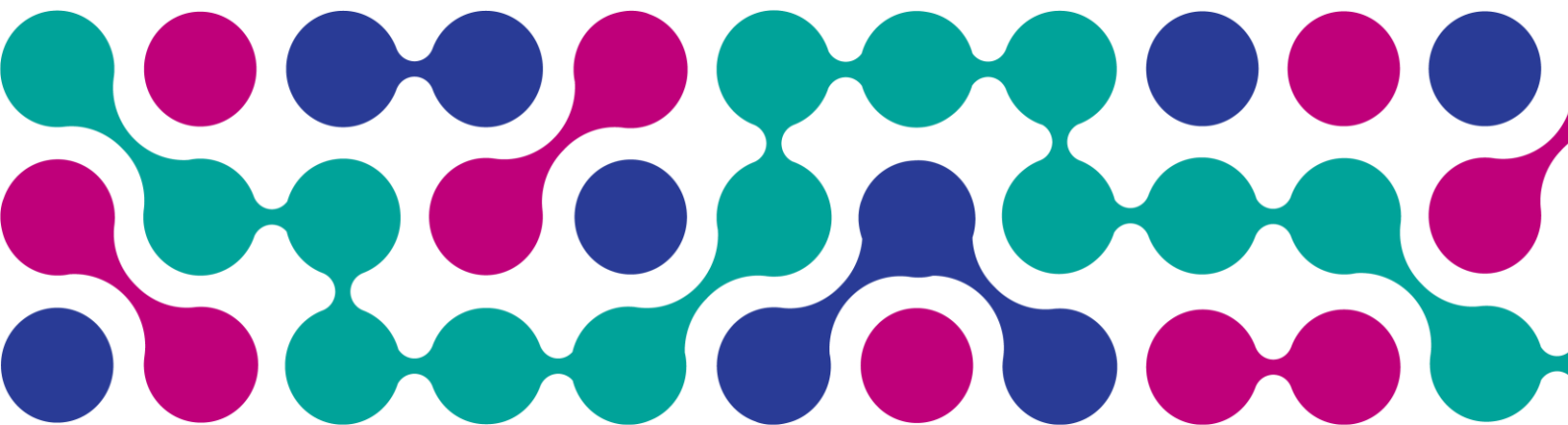




**Bath and North East Somerset,  
Swindon and Wiltshire**  
Integrated Care Board

# Prevent Policy 2021 - 2024

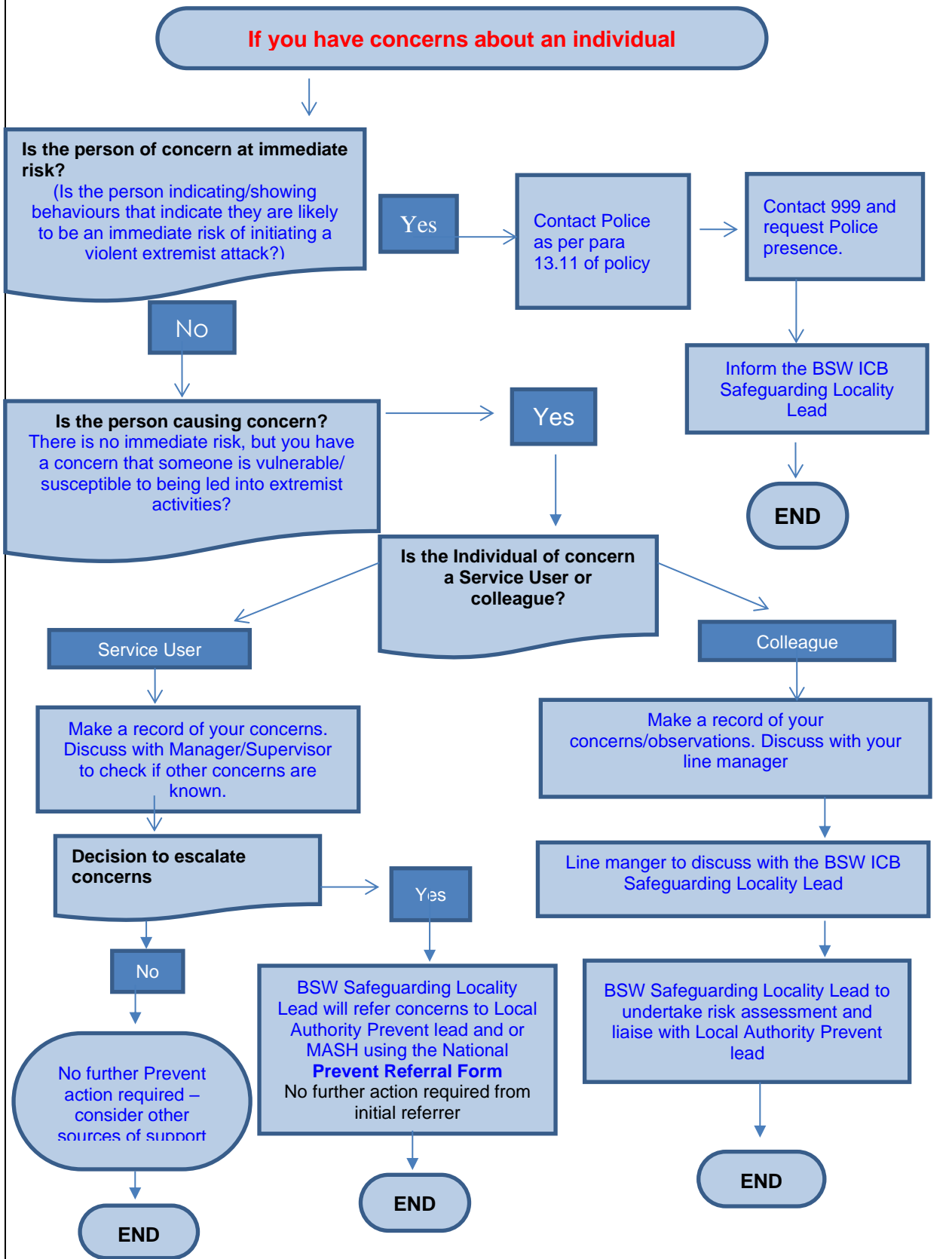


<b>Title:</b>	Prevent Policy 2021-24		
<b>Version:</b>	1.1	<b>Recommended Review Date:</b>	April 2024
<b>Approval Date:</b>	10.06.21	<b>Approving Committee:</b>	BSW ICB Quality, Outcomes & Governance Committee
<b>Document Manager:</b>	Colette O'Neill	<b>Document Sponsor:</b>	Gill May

<b>Purpose:</b>	The purpose of this Policy is to ensure that all BSW ICB colleagues are made aware of and able to address concerns about the risks from radicalisation to vulnerable people, children and colleagues.
<b>Key information:</b>	The ICB is committed to promoting an environment that values diversity. The ICB aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. This document has been equality impact assessed. No adverse impact or other significant issues were found and a copy of this can be found in Appendix 1.
<b>Specific colleagues/ teams:</b>	This Policy applies to all staff employed by BSW ICB either directly or indirectly, including volunteers, sub-contractors, and agency workers, both clinical and non-clinical and any other person or organisation that uses the BSW ICB premises for any purpose.
<b>Tables/ Flowcharts:</b>	

# Reporting flow chart for Raising Concerns

Action to take if you suspect an individual is being radicalised or self-radicalised into extremist activities



# Prevent Policy 2021-2024

## Table of Contents

1.0	Policy Aim	4
2.0	Summary	4
3.0	Introduction	5
4.0	Leadership and Responsibilities in support of the Prevent Duty, 2015	6
5.0	Staff Training	8
6.0	Implementation	8
7.0	Process of Exploitation	8
8.0	Internet	9
9.0	Raising Prevent Concerns about people receiving services	10
10.0	Escalating concerns in relation to Employees	11
11.0	Partnership Working	11
12.0	Counter Terrorism Local Profiles (CTLP)	12
13.0	Confidentiality, Information Sharing and Disclosure	13
14.0	Information Requests about an Individual raised by another organisation	14
15.0	Monitoring Compliance	15
16.0	Legislation Compliance & References	15
17.0	Review history	16
	Appendix 1 - Equality Impact Assessment	17
	Appendix 2 - Vulnerability Factors	18
	Appendix 3 - National Prevent Referral Form	20
	Appendix 4 - Information Sharing	24
	Appendix 4a - Practical Information Sharing for Prevent Purposes	28
	Appendix 5 - Definitions of Terms	32
	Appendix 6 - Reporting Flowchart for Raising Concerns	33

---

This Policy provides advice, guidance and information for BSW ICB staff should they need to raise concerns about an individual who may be at risk of being drawn into terrorism or committing terrorist acts.

---

## **1.0 Policy Aim**

- 1.1 The primary aim of this policy is to ensure that all adults at risk of harm and vulnerable children are protected from any form of radicalisation whilst employed, receiving services commissioned or directly funded by BSW ICB. Also, that our BSW ICB colleagues, including volunteers, are able to identify any possible signs of radicalisation and know how to raise their concerns.
- 1.2 Preventing someone from becoming a terrorist or supporting terrorism should be seen as being consistent with all safeguarding activity aimed at protecting vulnerable individuals from any form of exploitation such as child exploitation, sexual exploitation, financial exploitation etc. It operates in the pre-criminal space, before any criminal activity has taken place.
- 1.3 In addition, the policy aims to ensure that BSW ICB colleagues can understand the Prevent Duty and how they can utilise their existing knowledge and skills to recognise that someone may have been or is at risk of being radicalised and drawn into terrorism.
- 1.4 This Policy also sets out how Prevent related referrals will be managed within the ICB and how requests by external agencies to the ICB will be handled.
- 1.5 It also describes where staff can seek advice from and how to escalate their concerns within the ICB. Colleagues should be confident that their organisation will handle concerns in the appropriate way.
- 1.6 Where these need to be raised with external agencies, this Policy describes how referrals will be managed within the existing multi-agency safeguarding processes – including through the multi-agency Channel Panel process.

## **2.0 Summary**

- 2.1 The ICB operates a zero tolerance to those who abuse or neglect vulnerable people; this includes staff and the public. Investigations of all suspected cases of exploitation or radicalisation of patients whilst receiving commissioned or funded healthcare will be thoroughly reviewed within the ICB and with partner agencies as per the Prevent Duty Guidance.
- 2.2 The objectives of the policy are to provide clear guidance on reporting any safeguarding concerns or allegations of abuse or exploitation, and to set out the levels of responsibility to ensure that:
  - Colleagues are aware of the policy
  - Vulnerable children and adults at risk of harm are safeguarded against the influence of any form of radicalisation whilst under the care of commissioned or funded healthcare services

- ICB staff members consider the potential risk of radicalisation when commissioning services and can ensure that our commissioned services are confident in identifying and addressing suspected signs of radicalisation
- BSW ICB staff receive the appropriate levels of Prevent training
- Any concerns both within the ICB and commissioned services regarding radicalisation are reported and thoroughly investigated
- Appropriate action is taken to safeguard the vulnerable patient, service user or staff member or volunteer
- The ICB, both internally and within commissioned services ensures compliance with relevant legislation and partnership policies

### 3.0 Introduction

- 3.1 Since 2017, there has been a significant shift in the terrorist threat to the UK, with five attacks in London and Manchester that led to the deaths of 38 innocent people and injured many more. The recent attacks across Europe, New Zealand, Sri Lanka and the UK have demonstrated the speed, diversity and accessibility of methods, by which individuals who are vulnerable to these radicalising messages can prepare and commit violent attacks often with catastrophic consequences.
- 3.2 This includes an increasing threat from 'lone actor' attacks which has increased significantly in recent years, reflecting a trend towards low cost, low complexity and often spontaneous attacks using knives, or vehicles. Lone actors often derive their ideologies and perpetuate their grievances on social media sites and encrypted online chatrooms.
- 3.3 This has also had a profound effect on the threat to the UK, and the current UK National Threat level is SUBSTANTIAL (<https://www.gov.uk/terrorism-national-emergency>), meaning an attack is likely. Although Islamist terrorism is the foremost terrorist threat to the UK, right-wing National Action was the first right wing extremist group to be proscribed, under the Terrorism Act 2000. The Government took further action in September 2017, proscribing 'Scottish Dawn' and 'National Socialist Anti-Capitalist Action' as aliases of National Action. In February 2020, 'Sonnenkrieg Division', as well as National Action off-shoot, 'System Network' was also banned by the UK Government.
- 3.4 The CONTEST strategy was updated in 2018 to reflect the findings from a review of all aspects of counter-terrorism and to future-proof the strategy in its response to heightened threats.

The four 'P' work strands remain unchanged:

- **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.

The key objectives within the Prevent strand were revised as follows:

1. Safeguard and support those at most risk of radicalisation through early intervention, identifying them and offering support
2. Enable those who have already engaged in terrorism to disengage and rehabilitate

### 3. Tackle the causes of radicalisation and respond to the ideological challenge of terrorism

Health has a particularly important role in the Safeguarding element of the strategy. Healthcare staff are well placed to recognise individuals, whether service users, patients, or colleagues, who may be vulnerable and more susceptible to radicalisation by violent extremists or terrorists.

#### **4.0 Leadership and Responsibilities in support of the Prevent Duty, 2015**

- 4.1 The Prevent duty 2015 was introduced through the Counter-Terrorism and Security Act 2015 and the duty requires health bodies, local authorities, schools, colleges, higher education institutions, prisons, probation and the police to consider the need to safeguard people from being drawn into terrorism. It sits alongside long-established existing duties on professionals to safeguard vulnerable people from exploitation from a range of other harms such as knife crime, drugs, and sexual exploitation.
- 4.2 The duty is designed to help ensure that vulnerable individuals who are at risk of radicalisation are supported as they would be under other safeguarding processes. It does not require health professionals to do anything new and it sits within the recognised existing duty that we all have to safeguard vulnerable people.
- 4.3 Thus, BSW ICB has a duty to ensure safe environments where extremists are unable to operate or exploit others. It is essential, therefore, that all staff know how they can recognise and support vulnerable people (patients, service users, carers or members of staff) who they feel may be at risk of being radicalised or drawn into terrorism. Prevent is a legal duty for all NHS Trusts and Foundation Trusts and is a contractual requirement for any service provider who is subject to the NHS Standard Contract. It is also part of the everyday safeguarding routine for NHS staff and those providing NHS services.
- 4.4 Organisational strategic leadership is key to ensuring the organisation fully discharges both statutory and contractual requirements in relation to the Prevent duty.
- 4.5 For the health sector, along with all specified authorities, the Prevent duty expects that those in leadership positions:
- Establish or use existing mechanisms for understanding the risk of radicalisation;
  - Ensure staff understand the risk and build the capabilities to deal with it;
  - Communicate and promote the importance of the Duty; and
  - Ensure staff implement the Duty effectively.

#### 4.6 Specific duties include:

##### 4.6.1 The Chief Executive:

The Chief Executive is responsible for ensuring that the ICB has policies in place and complies with its legal and regulatory obligations. The Chief Executive will provide the means necessary to ensure that staff develop and promote good practice in Prevent. As such, the Chief Executive has delegated a number of responsibilities to the following managers and key workers within the ICB:

#### 4.6.2 Chief Nurse:

As the Executive Prevent Lead, the Chief Nurse will ensure that commissioned services submit quarterly Prevent returns, in line with NHS England guidance. This data relates to the Safeguarding clause of the NHS Standard Contract and that progress is being made by the organisation to implement the Prevent Duty requirements. This includes data relating to the number of referrals and staff attending Prevent Training.

#### 4.6.3 Associate Director for Strategic Safeguarding:

The Associate Director for Strategic Safeguarding is responsible for the development of policies and ensuring they comply with relevant standards and criteria where applicable. They are also responsible for ICB wide implementation and compliance with the Prevent Policy.

#### 4.6.4 The Director for People and Organisational Development:

The Director for People and Organisational Development is responsible for making arrangements for a suitable number of training places and events to be delivered to allow all relevant staff identified in the training needs analysis to access the Prevent training programme.

They are responsible for ensuring that a Training Plan is in place for Prevent Training at Levels 1-3.

They are also responsible for providing training reports for BSW ICB staff as required.

#### 4.6.5 Managers:

Managers are responsible for ensuring policies are implemented, communicated to their staff and that staff adhere to the policy details.

They are responsible for ensuring staff attend relevant training and supporting staff with the processes to escalate a concern. They are also responsible for liaising with the Human Resources Department if the concern raised is about a member of staff.

#### 4.6.6 Safeguarding Locality Leads:

The Designated Nurses within each locality will be the gatekeepers for Prevent referrals and enquiries from staff within the ICB. The post holder will act as a key person in supporting and guiding clinical, non-clinical and managerial staff. They will ensure careful consideration of each case and if required, referral onward in accordance with the local inter-agency safeguarding procedures.

They will ensure that Prevent activity within both the ICB and commissioned services is monitored on a quarterly basis in line with NHS England guidance. This includes collating organisational data relating to Prevent referrals and the numbers of staff attending Levels 1-3 of Prevent training.

The Safeguarding Leads will assist the Associate Director for Strategic Safeguarding in implementing, monitoring and reporting on the progress of improvements, uses and outcomes related to this policy.



#### 4.6.7 All Colleagues:

All BSW ICB staff have duties and responsibilities in relation to the Prevent duty and in keeping with statutory requirements and best practice guidance. All ICB colleagues, including volunteers, have a responsibility to familiarise themselves with this policy and to adhere to its process.

Any concerns must be reported to the relevant line manager. Staff members have a responsibility to respond sensitively to a safeguarding disclosure and act in a professional manner and take appropriate action.

### 5.0 Staff Training

- 5.1 To ensure contractual obligations in relation to safeguarding as set out in the NHS Standard Contract, BSW ICB will follow the guidance provided in the NHS England Prevent Training and Competencies Framework (September 2022) which provides clarity on the level of training required for staff. It identifies staff groups at levels one to six, from all staff through to board level.

This should be used in conjunction with the respective Safeguarding Competency Frameworks:

- adult safeguarding: roles and competencies for healthcare staff (Royal College of Nursing, 2018) (2018)
- safeguarding children and young people: roles and competencies for healthcare staff (2019)
- looked after children: roles and competencies for healthcare staff (2020)

- 5.2 The NHS funded service along with the ICB must have a Safeguarding Training Delivery Plan that includes Prevent and describes how the organisation will:

- Undertake and maintain a training needs analysis
- Ensure all staff receive appropriate basic Prevent awareness training
- Include refresher training delivery for all staff

### 6.0 Implementation

- 6.1 BSW ICB staff will be advised of this Policy by their Line Manager at induction. The Policy will be readily accessible on BSW ICB's Intranet.

It will be disseminated through:

- BSW ICB Induction Programme
- Local area governance groups within the localities
- Other relevant training opportunities
- The Intranet

### 7.0 Process of Exploitation

- 7.1 Radicalisation is a process and not an event and Government and academic research has consistently indicated that there is no single socio-demographic profile of a terrorist in the UK and no single pathway, or 'conveyor belt', leading to involvement in terrorism. Terrorists come from a broad range of backgrounds and appear to become involved in different ways and for differing reasons.
- 7.2 While there is no one single reason to cause someone to become involved in terrorism, several factors can converge to create the conditions under which there is a cognitive opening where radicalisation can occur. There are also certain engagement factors, sometimes referred to as "psychological hooks" related to personal circumstances which may make some individuals more susceptible to being drawn into terrorism.
- 7.3 However, the increasing body of evidence indicates that factors relating to the personal experiences of vulnerable individuals affects the way in which they relate to their environment and may make them more susceptible to exploitation or to supporting terrorist activities (see Appendix 2: Vulnerability Factors). Vulnerable individuals who may be susceptible to radicalisation can be patients, carers and/or staff and everyone's pathway is different.
- 7.4 Radicalisers often use a persuasive rational or narrative to promote their extremist ideology. They are usually charismatic individuals who can attract people to their cause which is based on an interpretation or distortion of history, politics and/or religion.
- 7.5 The key challenge for the health sector is to ensure that, where there are signs that someone is vulnerable to being drawn into terrorism, staff are aware of the support that is available and are confident in referring the person for further support.

## **8.0 Internet**

- 8.1 Islamist and Right-Wing Extremist radicalisers fully exploit the power, reach and speed of the internet to promote their narratives, influencing extremists within our own communities to disrupt our way of life through acts of violence. They groom the vulnerable and the young to join or support their cause, inspiring people within our own communities to harm others.
- 8.2 Vulnerable individuals may be exploited in many ways by radicalisers and this could often be through leaflets, direct face to face contact, or increasingly through the internet, social networking or other media.
- 8.3 The power of the internet in the radicalisation process cannot therefore be underestimated and radicalisers are making ever more sophisticated use of social media to spread their extremist messages and ideologies.
- 8.4 The internet provides a platform for extremists to promote their cause and encourage debate through websites, internet forums, gaming apps and social networking. It is a swift and effective mechanism for disseminating propaganda material and mobilising support, but is not always easy or possible to monitor or regulate.
- 8.5 BSW ICB staff should be aware of anyone making frequent unwarranted visits to websites showing extremist images and speeches or providing access to material from those involved in the radicalisation process, and how they should raise their concerns.

For members of the public, a dedicated website to report online material promoting terrorism or extremism is available at <https://www.gov.uk/report-terrorism>

- 8.6 For members of the public, Action Counter Terrorism provide a confidential Early Support Help Line, open every day 9am to 5pm at 0800 011 3764.
- 8.7 For members of the public, a dedicated website to report suspected terrorism or suspicions that some may be involved in terrorism is available at <https://www.met.police.uk/tua/tell-us-about/ath/possible-terrorist-activity>

## **9.0 Raising Prevent concerns about people receiving services**

- 9.1 During daily work, staff may face situations that give them cause for concern about the potential safety of a patient, or their family, or the staff who work with them. Early intervention can re-direct a vulnerable individual away from being drawn into criminality and terrorism – thereby harming themselves and others. The health sector will need to ensure that the crucial relationship of trust and confidence between patient and clinician is balanced with the clinician’s professional duty of care and their responsibility to protect wider public safety. Each NHS funded service have their own Prevent Lead. All concerns from within an organisation should be addressed to them and using their internal Prevent Policy in the first instance. In the event that BSW ICB staff have concerns that a patient, service user or their carer may be at risk of being drawn into terrorism or may be vulnerable to grooming or exploitation by others, the primary point of contact will be the Prevent Lead within the NHS Funded service. The locality ICB Safeguarding Lead should be notified.
- 9.2 In the case of patients who receive ICB funding, such as through CHC or Specialist Funding sources, all concerns should initially be discussed with the care team supporting the person and prior to referral. If agreed that a Prevent referral is appropriate, a conversation should always be held with the locality ICB Safeguarding Lead who makes the referrals on behalf of the ICB.
- 9.3 If an onward referral to the local authority is required, this should be undertaken by the BSW ICB locality Safeguarding Lead through the completion of the National Prevent referral form (see Appendix 3: Making a Prevent Referral) clearly identifying the precise nature of the concerns and reason for referral. The decision and rationale should also be clearly documented in the patient record.
- 9.4 All Prevent referrals are confidential and take place in the non-criminal space. In many cases, no further action will be required, or the vulnerability is assessed as not related to radicalisation and the individual concerned is signposted to other support which may be required. All patient/staff information must be shared in accordance with General Data Protection Regulations (GDPR)/Data Protection Act 2018/Caldicott Principles and Human Rights legislation and meet the same rigour required for sharing information for any other safeguarding concern. See Appendix 4: Information Sharing and Appendix 4a Practical information sharing for Prevent purposes).
- 9.5 The Home Office have introduced new Prevent awareness training which introduces users to the NOTICE-CHECK-SHARE procedure for evaluating and sharing concerns. The package shares best practice on how to articulate concerns about an individual and

ensure that they are robust and considered Home Office Prevent eLearning: Referrals. This does not replace the e-LFH training at levels 1 – 3.

## **10.0 Escalating concerns in relation to Employees**

- 10.1 Although there are relatively few instances of staff being at risk of radicalisation, encouraging others or becoming involved in extremist activity, it is still a risk that BSW ICB needs to be aware of and have processes in place within which to manage any concerns.
- 10.2 Where any employee expresses views, brings material into the ICB, uses or directs colleagues, patients, service users or carers to extremist websites or acts in other ways to promote terrorism, BSW ICB will look to use all potential safeguarding and non-safeguarding processes to address the concerns.
- 10.3 Where a staff member has a concern about a colleague, this should be raised with their Line Manager. The Line Manager will discuss the concerns with the BSW ICB Safeguarding locality Lead and Human Resources Department in the first instance. If deemed necessary, the Safeguarding Lead will support the completion of or complete the relevant National Prevent Referral Form on behalf of the staff member.
- 10.4 BSW ICB Safeguarding locality Lead will liaise with the Local Authority Prevent Lead to assess and manage any related safeguarding risk. The Human Resources Advisor will lead on advising the Line Manager in relation to the disciplinary process; should this be appropriate.

## **11.0 Partnership Working**

- 11.1 It should be stressed that there is no expectation that BSW ICB will take on a surveillance role or challenge extremist views when identifying or supporting a Prevent concern – we don't have the legal basis or the specialist knowledge and skills. Rather, we must work with partner organisations to contribute to the prevention of terrorism by safeguarding and protecting vulnerable individuals and making safety and harm prevention a shared endeavour.
- 11.2 The Safeguarding Locality Lead will engage with local partnership groups with the responsibility to share concerns raised within the organisation and represent BSW ICB as appropriate on the Local Prevent Steering Group/Oversight Board and attend Channel meetings as required and in accordance with the Channel Duty Guidance.
- 11.3 Channel is the multi-agency safeguarding process through which statutory partners agree the appropriate level of support to an individual at risk of being drawn into terrorism or committing terrorist acts. It is about early intervention to protect and divert vulnerable people away from the risk they face before illegality occurs.
- 11.4 If an individual is assessed to be vulnerable to radicalisation, they may be offered support through the local Channel multi agency panel which meet monthly and operates in every local authority area in England and Wales.
- 11.5 Channel Panels are chaired by the local authority and partners will discuss each case individually and carefully assess the extent to which an individual may be vulnerable to

radicalisation. If required, the panel will offer the individual a package tailored to their specific identified needs.

- 11.6 Support could include assistance with education or employment, health support or ideological mentoring to provide vulnerable individuals with the skills to protect themselves from being drawn any further into terrorism-related activity or supporting terrorism.
- 11.7 The vulnerable individual and or their parent or guardians must be aware that they are receiving support through Channel, what the aims of the programme are and what to expect. They must also consent to participating in the process and for their personal sensitive information to be shared with multi-agency partners.
- 11.8 The Channel Duty through Section 38 of the Counter Terrorism & Security Act 2015 places a Duty on all partners – to support and attend Channel multi agency panels and provide advice and interventions as required.
- 11.9 The Home office have produced a bespoke eLearning training product which explains how the Channel process works. This training package is available to anyone who may contribute to, sit on, or even run a Channel Panel. It is aimed at all levels, from a professional asked to input and attend for the first time, to a member of staff new to their role and organising a panel meeting Home Office eLearning: Channel Awareness. This does not replace the training available through eLFH at levels 1 to 3.
- 11.10 The Prevent Mental Health Guidance issued by NHS England in November 2017, established a number of clear expectations for mental health trusts to support Prevent. These included senior clinical representation at all Channel panel meetings and the expedited offer of assessment (within 7 days) for individuals within the Channel process where diagnosed or suspected mental health vulnerability has been identified. The Guidance complements the bespoke Prevent Mental Health eLearning Level 3 training resource, and it is good practice to ensure all mental health clinical staff undertake this module.

## **12.0 Contributing to the Counter Terrorism Local Profile (CTLP)**

- 12.1 CTLPs are produced annually and provide a strategic overview of the threat and vulnerability from terrorism related activity within the local area at a given time. This enables BSW ICB in its locality areas as well as strategically to plan activity to address threats.
- 12.2 CTLPs provide partners with a practical and consistent approach to sharing Counter-Terrorism related information to help them target activities and resources as effectively as possible.
- 12.3 Health providers are a key partner in countering terrorism at a local level and, it is imperative that all NHS funded services as well as the ICB are able to contribute to it.
- 12.4 NHS England Regional Prevent Co-ordinators play a central role in ensuring that commissioners and service providers are able to contribute relevant information and data for the CTLP through completion of an annual questionnaire.

- 12.5 Information provided in the CTLP questionnaire by the ICB should also highlight any current and emerging themes or vulnerabilities across the health system, and indicate whether the threats, risks and vulnerabilities have changed or remained the same.
- 12.6 The BSW ICB Safeguarding Locality Leads should attend annual CTLP risk and threat briefings delivered by the NHS England Regional Prevent Co-ordinator and cascade any relevant information to staff within the organisation to enable them to better understand the local context.

### **13.0 Confidentiality, Information Sharing and Disclosure**

- 13.1 Timely and effective information sharing has been identified as a key element within the Prevent Duty. It is therefore vital that healthcare organisations are familiar with their organisational policies and procedures on information sharing and have arrangements in place so that information can be shared with partners when necessary for Prevent purposes. This should include clear guidance as to how Prevent concerns are noted on patient records and handed over when patients are transferred.
- 13.2 Staff or other workers providing services on behalf of BSW ICB must ensure that they share information appropriately both professionally and legally when there is a safeguarding concern. This should be in line with HM Governments Information Sharing Guidance June 2018: Department of Health NHS Confidentiality Code of Practice 2003 (as amended), GMC Confidentiality: good practice in handling patient information Guidance May 2018 and the relevant local BSW ICB information sharing protocols.
- 13.3 Prevent is based on the active engagement of the vulnerable individual and is at a pre-criminal stage, therefore appropriate consent should be obtained from the individual involved (or their parents or guardian if aged under 18 years) prior to a referral to Prevent. This is both to comply with *NHS the Code of Practice on Confidentiality* and to establish an open relationship with the vulnerable individual at the start of the process.
- 13.4 However, if you consider that failure to disclose the information would leave individuals or society exposed to a risk or harm so serious that it outweighs the patient's and the public interest in maintaining confidentiality, you should disclose relevant information promptly to an appropriate person or authority (See Appendix 4: Information Sharing).
- 13.5 In cases where the vulnerable person lacks capacity as described in the Mental Capacity Act 2005 to give consent, a referral may be made without consent if it is determined to be in their Best Interests.
- 13.6 The decision and rationale for making a referral without the individual's informed consent should be subject to a case-by-case basis assessment. This should include whether the informed consent of the individual can be obtained and the proposed sharing to be necessary, proportionate and lawful. This should clearly be documented and recorded. This is described in greater details in the GMC Confidentiality: good practice in handling patient information guidance (2018).
- 13.7 Additionally agencies may share limited and proportionate information prior to seeking informed consent when this is urgently required to establish whether the case should be managed under Prevent or as a counter terrorism case. Again, this must be carried out in

line with the principles outlined in the GMC Confidentiality: good practice in handling patient information guidance (See also Appendix 4: Information Sharing).

- 13.8 Where there is concern or evidence that an individual is engaged in the planning or undertaking of terrorist acts, then consent is not required to share any information that may be required to assess and manage the risk of a serious criminal offence occurring. In these cases, and to ensure the safety of others, the individual should not be informed that information is being shared, and the 7<sup>th</sup> Caldicott principle (i.e. that the duty to share information can be as important as the duty to protect patient confidentiality) should be applied.
- 13.9 If BSW ICB staff are not sure regarding information sharing or consent issues, they should seek advice from their organisational Caldicott Guardian or Information Governance Officer. All information sharing of patient personal or sensitive data must comply with all Caldicott Principles and the law (See: Appendix 4: Information Sharing).
- 13.10 Any disclosures or discussions on information sharing or consent must always be documented in the patient record.
- 13.11 In the event of a significant concern or immediate risk to others, which needs a more urgent Prevent response (e.g. if there is a significant concern – particularly if it is out of hours) there are some useful telephone numbers that you can call:

The **101 number** is designed to encourage people to contact the police at an early stage to prevent or detect crime. In terms of Prevent, the earlier authorities can be involved the greater the chance we can intervene with partners and stop someone from being radicalised.

Confidential Anti-Terrorist Hotline - If you are suspicious that someone is being radicalised or that the call is terrorism related you can call the confidential Anti-Terrorist Hotline on **0800 789 321**. A textphone service is available for people with speech or hearing difficulties on **0800 0324539** (text messages from mobiles are not accepted).

**In an emergency where you feel that there is an immediate terrorist threat, call 999.**

#### **14.0 Information Requests about an Individual raised by another organisation**

- 14.1 Generally requests for patient information should be made in writing, justifying the grounds for disclosure and submitted to the Data Controller of the data system from which the information is sought. The seriousness of the potential crime and the risk of harm to the individual or the public may outweigh the need to maintain patient confidentiality. The amount of information shared should be appropriate and responsive to the concern raised.
- 14.2 In situations where disclosures to (or information sharing with) the police or local authority may become routine, it is considered as good practice to have a purpose specific information protocol and agreement between the organisation and the police, so that all staff involved know what to do.
- 14.3 Note that the Crime and Disorder Act 1998 (See Appendix 4: Information Sharing) does not in itself constitute a statutory requirement for NHS organisations to disclose patient information to other agencies. This should be determined on a case by case basis with

the BSW ICB Safeguarding Locality Lead and in consultation with the Caldicott Guardian and/or Information Governance Officer for the organisation.

14.4 If a Safeguarding Locality Lead is asked to share information for the purposes of preventing an individual from being drawn into terrorism the following questions should be considered:

- By sharing the information, is the intention to safeguard the individual from criminal exploitation, grooming (being drawn into terrorism) or self-harm?
- In sharing information, is a serious crime being prevented or detected or a vulnerable person being safeguarded?
- Is the information that has been requested appropriate to the risk of the serious harm of exploitation to the individual who may be being drawn into supporting terrorism?
- In being drawn into terrorism does this individual pose harm to themselves or the wider public?
- Can the public interest justification be clearly stated? (If in doubt, seek advice from your organisations Caldicott Guardian).
- The GMC Confidentiality: good practice in handling patient information guidance (2018) also provides a framework to help you decide when you can share information and helps you to think about why you are sharing the information. This may be for the direct care or protection of the patient, to protect others or for another reason. It also has a handy flowchart which you can use to help you decide whether to share the information.

14.5 Information Governance policies should outline guidelines on areas of information management risk for the organisation including:

- An IT policy that identifies inappropriate use by either patients or staff
- Room hire by external organisations
- Appropriate use of notice boards
- The distribution of inappropriate materials or leaflets

## **15.0 Monitoring Compliance**

15.1 Prevent data collection demonstrates how BSW ICB monitors delivery by NHS funded services on the key elements of the Prevent duty. These include, delivery of awareness training, the level of referrals made and the engagement with relevant partnership forums that co-ordinate the Prevent Strategy at local and regional levels. It assists the ICB in identifying potential areas for development and provides the ICB with an assurance framework on which our Health partners delivery of the Prevent Strategy can be assured.

15.2 BSW ICB Prevent training data will be maintained by BSW ICB People Team.

15.3 A record of all Prevent concerns raised by BSW ICB will be held as highly confidential by the ICB Safeguarding Locality Leads.

## **16.0 Legislation Compliance & References**

16.1 The following legislation, regulation and guidance has been used to inform this Policy:



- NHS Standard Contract (See SC 32 specifically)
- NHS England Prevent Training and Competencies Framework 2022
- General Data Protection Regulations/Data Protection Act 2018
- Information Commissioners Office Guidance
- Human Rights Act 1998
- European Convention on Human Rights 1953
- Equality Act 2010
- Common Law Duty of Confidentiality (CLDC)
- Caldicott principles as defined in 'The Information Governance Review'
- Information sharing advice for safeguarding practitioners (HM Govt:2018)
- GMC 'confidentiality: good practice in handling patient information guidance' (May 2018)
- Crime and Disorder Act 1998
- CONTEST Strategy 3.0
- Counter Terrorism and Security Act 2015
- Counter Terrorism and Border Security Act 2019
- Revised Prevent Duty Guidance 2015
- Channel Duty Guidance 2020
- Guidance for mental health services in exercising duties to safeguard people from the risk of radicalisation:2017
- Care Act 2014
- Safeguarding children and young people: roles and competencies for health care staff intercollegiate Document: Jan 2019.
- Working Together to Safeguard Children 2018
- Adult Safeguarding: Roles and Competencies for Health Care Staff 2018
- Looked After Children: Roles and Competencies of Healthcare Staff 2020

16.2 The Champion of this Policy is the Associate Director for Strategic Safeguarding. The Policy has been personalised for BSW ICB from the Generic Policy Template provided by NHS England (2019).


## 17 – Review History

Version	Review Date	Reviewed By	Changes Required? (If yes, please summarise)	Changes Approved By	Approval Date
1.1	03/02/23	Colette O'Neill	CCG changed to ICB.  BSW ICB Quality and Performance Assurance Committee changed to Quality, Outcomes & Governance Committee.  'Whilst employed' added to policy aim at 1.1.		

			<p>'Extremist action' changed to 'National Action' at 3.3</p> <p>Executive Director of Nursing changed to Chief Nurse at 4.6.2</p> <p>Date of the Prevent Training and Competency Framework changed to September 2022 at 5.1.</p> <p>Looked after children: roles and competencies for healthcare staff (2020) added at 5.1.</p> <p>'The organisation' changed to 'The NHS funded service along with the ICB' at 5.2.</p> <p>Additional resource to report material promoting terrorism added at 8.6.</p> <p>Weblink for reporting terrorist activity updated at 8.6.</p> <p>"In the event that BSW ICB staff have concerns that a patient, service user or their carer may be at risk of being drawn into terrorism or may be vulnerable to grooming or exploitation by others, the primary point of contact will be their line manager" removed at 9.2 and replaced with additional information at 9.1.</p>		
--	--	--	---	--	--

			<p>Additional wording          'This does not replace the e-LFH training at levels 1 – 3' and the hyperlinks removed at 9.5 and 11.9.</p> <p>The term 'provider' replaced by NHS commissioned services and health partners at 15.1.</p> <p>Legislation and guidance updated at 16.1.</p>		

# APPENDIX 1 – COPY OF THE EQUALITY IMPACT ASSESSMENT

 <b>Bath and North East Somerset, Swindon and Wiltshire</b> <small>Clinical Commissioning Group</small>		
<b>Equality Impact Assessment (EIA) Summary for:</b>		
Prevent Policy		
<b>Date of Assessment:</b>		
11/12/2020		
<b>Document/Policy/Strategy/Project Aims:</b>		
To provide advice, guidance and information should staff need to raise concerns about an individual who may be at risk of being drawn into terrorism or committing terrorist attacks.		
<b>EIA: Summary Table:</b>		
9 Protected Characteristics	Impact Considered (√/x)	Equality risk identified: Yes/No/Expand
Race	✓	No
Gender	✓	No
Disability	✓	No
Age	✓	No
Maternity & Pregnancy	✓	No
Religion or Belief	✓	No
Gender Identity	✓	No
Marriage & Civil Partnerships	✓	No
Sexual Orientation	✓	No
<b>Groups/Individuals considered and engaged with during the EIA Process:</b>		
Safeguarding Transformation and Assurance Group		
<b>Actions Summary (timescales and action overview and review):</b>		
<p>The policy is inclusive in its principles with no individual where there are concerns about them being at risk of radicalisation being treated differently on the basis of any of the protected characteristics. The policy is designed to establish a mandatory, formal process to follow by all CCG staff. Safeguarding is an accountable process which supports, assures and develops the knowledge, skills and values of an individual, group or team. Safeguarding and promoting the welfare of children and vulnerable adults must be an integral part of the care offered to all children, adults and their families by all health care professionals working within BSW CCG. There is no perceived difference (advantage or disadvantage wise) in the benefits those supported by this Policy will receive as a result of their having protected characteristics. However, in order to monitor the impact, it is important that Equality Impact data is collected and subsequently analysed as a result of any requests for</p>		
<b>EIA Completed by:</b>	<b>Executive approval:</b>	
Colette O'Neill		

## **APPENDIX 2 – VULNERABILITY FACTORS**

Radicalisation is a process and not an event, and there is no single route or pathway to radicalisation. Evidence indicates that those targeted by radicalisers may sometimes have doubts or call into question about what they are doing and there may therefore be opportunities to intervene and safeguard them or others from harm. It is because of this doubt that frontline health and social care workers need to have mechanisms and interventions in place to support a person being exploited and to help safeguard them from being drawn into criminal activity and terrorism.

### **Use of extremist rational (often referred to as ‘narrative’)**

Radicalisers usually attract people to their cause through a persuasive rationale contained within a storyline or narrative that has the potential to influence views. Inspiring new recruits, embedding the beliefs of those with established extreme view and/or persuading others of the legitimacy of their cause is the primary objective of those who seek to radicalise vulnerable individuals.

### **What factors might make someone vulnerable?**

In terms of personal vulnerability, the following factors may make individuals susceptible to exploitation. None of these are conclusive in themselves and therefore should not be considered in isolation but should be contextualised and considered in conjunction with the circumstances of the case and any other signs of radicalisation. Remember Prevent does not require you to do anything in addition to your normal duties. What is important is that if you have a concern that you raise these in line with the BSW ICB policies and procedures.

#### **Identity Crisis:**

Adolescents/adults at risk of harm who are exploring issues of identity can feel both distant from their parents/family and cultural and religious heritage, and uncomfortable with their place in society around them. Radicalisers can exploit this by providing a sense of purpose or feelings of belonging. Where this occurs, it can often manifest itself in a change in a person’s behaviour, their circle of friends, and the way in which they interact with others and spend their time.

#### **Criminality:**

In some cases, a vulnerable individual may have been involved in a group that engages in criminal activity or, on occasion, a group that has links to organised crime and be further drawn to engagement in terrorist-related activity.

#### **Personal Grievances:**

The following are examples of grievances which may play an important role in the early indoctrination of vulnerable individuals into the acceptance of a radical view and extremist ideology:

- A misconception and/or rejection of UK foreign policy

- A distrust of Western media reporting
- Perceptions that UK government policy is discriminatory (e.g. counter-terrorism legislation)
- Ideology and politics
- Provocation and anger (grievance)
- Need for protection
- A distrust of Western media reporting
- Seeking excitement and action
- Fascination with violence, weapons and uniforms
- Youth rebellion
- Seeking family and father substitutes
- Seeking friends and community
- Seeking status and identity

### **Personal Crisis:**

This may, for example, include significant tensions within the family that produce a sense of isolation of the vulnerable individual from the traditional certainties of family life.

### **Personal Circumstances:**

The experience of migration, local tensions or events affecting families in countries of origin may contribute to alienation from UK values and a decision to cause harm to symbols of the community or state.

### **Unemployment or under-employment**

Individuals may perceive their aspirations for career and lifestyle to be undermined by limited achievements or employment prospects. This can translate to a generalised rejection of civic life and adoption of violence as a symbolic act.

## APPENDIX 3 – National Prevent Referral Form

This form is to be used by the BSW ICB Safeguarding Designated Nurse only for making referrals in order to safeguard someone from being drawn into radicalisation or supporting terrorism. Prevent is intended to deal with all kinds of terrorist threats to the UK, arising from issues including among others Islamist extremism, Right Wing Extremism, and mixed or unclear ideologies. Identification and referral should therefore arise from concerns about behaviour and the risk of harm they may pose to themselves or others. **PLEASE NOTE THAT IT SHOULD BE PROTECTIVELY AT OFFICIAL SENSITIVE WHEN COMPLETE.**

### REFERRAL PROCESS

By sending this form you consent for it to arrive with both your dedicated Local Authority safeguarding team & Prevent policing team for a joint assessment. Wherever possible we aim to give you feedback on your referral, please be aware, however, that this is not always possible due to data-protection & other case sensitivities.

Once you have completed this form, please email it to: **[Insert name of relevant LA MASH or police lead here]**

### INDIVIDUAL'S BIOGRAPHICAL & CONTACT DETAILS

<b>Forename(s):</b>	First Name(s)
<b>Surname:</b>	Last Name
<b>Date of Birth (DD/MM/YYYY):</b>	D.O.B.
<b>Approx. Age (if DoB unknown):</b>	Please Enter
<b>Gender:</b>	Please Describe
<b>Known Address(es):</b>	Identify which address is the Individual's current residence
<b>Nationality / Citizenship:</b>	Stated nationality / citizenship documentation (if any)
<b>Immigration / Asylum Status:</b>	Immigration status? Refugee status? Asylum claimant? Please describe.
<b>Primary Language:</b>	Does the Individual speak / understand English? What is the Individual's first language?
<b>Contact Number(s):</b>	Telephone Number(s)
<b>Email Address(es):</b>	Email Address(es)
<b>Any Other Family Details:</b>	Family makeup? Who lives with the Individual? Anything relevant.

### DESCRIBE CONCERNS

**In as much detail as possible, please describe the specific concern(s) relevant to Prevent.**

Please Describe

PERSON WHO FIRST IDENTIFIED THE CONCERNS	
Do they wish to remain anonymous?	Yes / No
Forename:	Referrers First Name(s)
Surname:	Referrers Last Name
Professional Role & Organisation:	Referrers Role / Organisation
Relationship to Individual:	Referrers Relationship To The Individual
Contact Telephone Number:	Referrers Telephone Number
Email Address:	Referrers Email Address
PERSON MAKING THIS REFERRAL (if different from above)	
Forename:	Contact First Name(s)

<b>FOR EXAMPLE:</b>	
<ul style="list-style-type: none"> <li>• How / why did the Individual come to your organisation's notice in this instance?</li> <li>• Does it involve a specific event? What happened? Is it a combination of factors? Describe them.</li> <li>• Has the Individual discussed personal travel plans to a warzone or countries with similar concerns? Where? When? How?</li> <li>• Does the Individual have contact with groups or individuals that cause you concern? Who? Why are they concerning? How frequent is this contact?</li> <li>• Is there something about the Individual's mobile phone, internet or social media use that is worrying to you? What exactly? How do you have access to this information?</li> <li>• Has the Individual expressed a desire to cause physical harm, or threatened anyone with violence? Who? When? Can you remember what was said / expressed exactly?</li> <li>• Has the Individual shown a concerning interest in hate crimes, or extremists, or terrorism? Consider <i>any</i> extremist ideology, group or cause, as well as support for "school-shooters" or public-massacres, or murders of public figures.</li> <li>• Please describe any other concerns you may have that are not mentioned here.</li> </ul>	
<b>COMPLEX NEEDS</b>	<b>Is there anything in the Individual's life that you think might be affecting their wellbeing or that might be making them vulnerable in any sense?</b>
Please Describe	
<b>FOR EXAMPLE:</b>	
<ul style="list-style-type: none"> <li>• Victim of crime, abuse or bullying.</li> <li>• Work, financial or housing problems.</li> <li>• Citizenship, asylum or immigration issues.</li> <li>• Personal problems, emotional difficulties, relationship problems, family issues, ongoing court proceedings.</li> <li>• On probation; any erratic, violent, self-destructive or risky behaviours, or alcohol / drug misuse or dependency.</li> <li>• Expressed feelings of injustice or grievance involving any racial, religious or political issue, or even conspiracy theories.</li> <li>• Educational issues, developmental or behavioural difficulties, mental ill health (see <b>Safeguarding Considerations</b> below).</li> <li>• Please describe any other need or potential vulnerability you think may be present but which is not mentioned here.</li> </ul>	
<b>OTHER INFORMATION</b>	<b>Please provide any further information you think may be relevant, e.g. social media details, military service number, other agencies or professionals working with the Individual, etc..</b>
Please Describe	



<b>Surname:</b>	Contact Last Name
<b>Professional Role &amp; Organisation:</b>	Contact Role & Organisation
<b>Relationship to Individual:</b>	Contact Relationship to the Individual
<b>Contact Telephone Number:</b>	Contact Telephone Number
<b>Email Address:</b>	Contact Email Address

### REFERRER'S ORGANISATIONAL PREVENT CONTACT (if different from above)

<b>Forename:</b>	Referrers First Name(s)
<b>Surname:</b>	Referrers Last Name
<b>Professional Role &amp; Organisation:</b>	Referrers Role / Organisation
<b>Relationship to Individual:</b>	Referrers Relationship To The Individual
<b>Contact Telephone Number:</b>	Referrers Telephone Number
<b>Email Address:</b>	Referrers Email Address

### SAFEGUARDING CONSIDERATIONS

<b>Does the Individual have any stated or diagnosed disabilities, disorders or mental health issues?</b>	Yes / No
Please describe, stating whether the concern has been diagnosed.	
<b>Have you discussed this Individual with your organisations Safeguarding / Prevent lead?</b>	Yes / No
What was the result of the discussion?	
<b>Have you informed the Individual that you are making this referral?</b>	Yes / No
What was the response?	
<b>Have you taken any direct action with the Individual since receiving this information?</b>	Yes / No
What was the action & the result?	
<b>Have you discussed your concerns around the Individual with any other agencies?</b>	Yes / No

### RELEVANT DATES

<b>Date the concern first came to light:</b>	When were the concerns first identified?
<b>Date referral made to Prevent:</b>	Date this form was completed & sent off?
What was the result of the discussion?	

### INDIVIDUAL'S EMPLOYMENT / EDUCATION DETAILS

<b>Current Occupation &amp; Employer:</b>	Current Occupation(s) & Employer(s)
<b>Previous Occupation(s) &amp; Employer(s):</b>	Previous Occupation(s) & Employer(s)
<b>Current School / College / University:</b>	Current Educational Establishment(s)
<b>Previous School / College / University:</b>	Previous Educational Establishment(s)

### THANK YOU

Thank you for taking the time to make this referral. Information you provide is valuable and will always be assessed. If there is no Prevent concern but other safeguarding issues are present, this information will be sent to the relevant team or agency to provide the correct support for the individual(s) concerned.

### GUIDANCE NOTES

Prevent aims to safeguard people and communities by stopping people becoming terrorists or supporting terrorism and this form must be used if you have concerns that this may be a risk for a staff member patient or service user. Completing and submitting this form will enable professionals working in Prevent to ensure that the individual you are concerned about is safeguarded from further harm and has the opportunity to access appropriate support to prevent their involvement in terrorism.

## NOTICE/CHECK/SHARE

**NOTICE** – are you worried about a patient/staff member, someone acting or saying things which concerns you? Use your professional judgement, if something doesn't feel right, it may not be!

**CHECK** – Speak with your manager, or organisational Safeguarding Locality Lead. Check your concern with them – does your concern also worry your Safeguarding Lead?

**SHARE** – when a decision is made by the Safeguarding Team, they should share the information with appropriate partners (this differs according to local authorities) or have a confidential conversation with the Police or Local Authority Prevent Lead.

When the Locality Safeguarding Leads have completed the form please email it securely to:

[Insert name of MASH] and your local authority Prevent Lead [Insert name] who will have a secure mail account.

If you have concerns relating to other vulnerabilities, then you should also make appropriate referrals at the same time.

However, in some cases by the time you are made aware of the risk the situation may already be well advanced – if this is the case:

- If there is an urgent safeguarding issue, then the Safeguarding Locality Lead should immediately contact Children's Social Care First Response or Adult Safeguarding Team.
- If there is an imminent danger that a crime is about to be committed dial 999.

If you feel that a call needs a more urgent Prevent response (e.g. if there is a significant concern – particularly if it is out of hours) there are some useful telephone numbers, you can call.

The **101 number** is designed to encourage people to make contact with the police at an early stage to prevent or detect crime. In terms of Prevent, the earlier authorities can be involved the greater the chance we can intervene with partners and stop someone from being radicalised.



### **Confidential Anti-Terrorist Hotline**

If you are suspicious that someone is being radicalised or that the call is terrorism related you can call the confidential **Anti-Terrorist Hotline on 0800 789 321**



**In an emergency where you feel that there is an immediate terrorist threat please call 999**

### **Run Hide Tell “Stay Safe” Campaign**

Is a short public information film which sets out practical steps that can be taken to stay safe in the unlikely event of a firearms or weapons attack. It is worth watching this to gain an understanding of the advice that should be provided to callers in such circumstances and the advice which should be provided. in the unlikely event of a weapons attack police urge you to follow the [Run, Hide, Tell message](#)

### **APPENDIX 4 – INFORMATION SHARING (General)**

All information sharing for Prevent purposes must comply with the relevant legislation i.e. *Data Protection Act 2018*, *Human Rights* legislation and the *Common-law Duty of Confidentiality* (amongst others) and meet the same rigour required for sharing information in respect of any other safeguarding concern.

The *General Data Protection Regulations GDPR* underpins the *Data Protection Act 2018* (DPA 2018): *Chapter 2/Part 3 of the Data Protections Act 2018* is based around six key data protection principles and provides a range of rights for individuals which are applicable to the processing or sharing of personal and sensitive data.

The principles state that personal data must:

- Be processed lawfully, fairly and in a transparent manner
- Be processed for specified, explicit and legitimate purposes and not in any manner incompatible with those purposes
- Be adequate, relevant and limited to what is necessary in relation to the purposes
- Be accurate and up to date
- Not be kept for longer than is necessary
- Be secure

#### **Lawful basis for sharing personal data:**

To disclose data into the programme and the lawfulness of the processing of the personal data must, one of the conditions found in *Article 6* of the GDPR must be met. If any special category data is to be disclosed, then one of the conditions of *Article 9* must be met.

The primary conditions for disclosing information for the purposes of Prevent *should be consent*, however this may not always be appropriate or achievable. If consent is not appropriate or achievable then a different lawful basis must be met (see Schedule 2 of the

DPA 2018 below) in order to share personal data. If another lawful basis is not met, then data cannot be shared.

### Consent:

The *General Data Protection Regulations (GDPR)* has strengthened the need to demonstrate consent is given freely – the GDPR has also strengthened the need to have a clarity of purpose for sharing /processing data whilst ensuring that criminal justice agencies and others can continue to use and share personal data to prevent and investigate crime, bring offenders to justice, to safeguard the vulnerable and keep communities safe from harm.

Potential lawful conditions to share information where consent of the individual or patient is inappropriate or unachievable are described below:

#### [Schedule 2 Part 1 of the Data Protection Act 2018:](#)

[Schedule 2, Part 1, Para 2 of the DPA 2018](#)) allows for the processing of personal data for the purposes of (but not limited to):

- *the prevention or detection of crime*
- *the apprehension or prosecution of offenders,*

[\(Schedule 2, Part 1, Para 5 of the DPA 2018\)](#) allows for the processing of personal data for the purposes of (generally) legal proceedings.

[Part 3 of the DPA 2018](#) allows for the processing of personal data by a competent authority for the purposes of the detection and/or prevention of crime.

This provides a legitimate basis upon which a competent authority is permitted to share information for the prevention of crime and disorder, because it will be exercising a statutory function for law enforcement purposes. [Part 3 \(Schedule 8\)](#) allows for the processing of sensitive data to safeguard children and adults at risk from harm.

A competent authority means:

- a 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.

It should be added that if the sharing is to any organisation other than the Police, if the disclosure is for the purposes of the prevention and detection of crime, that receiving organisation must be a *competent authority* as defined by the DPA 2018 otherwise the disclosure cannot be made for this purpose/reason.

### Section 115 of the Crime and Disorder Act 1998

The sharing of data by public sector bodies requires the existence of a power to do so, in addition to satisfying the requirements of the DPA 2018, the HRA 1998 and the Common Law duty of Confidentiality. Section 115 of the C & D Act 1998 provides agencies and professionals with the power (but not a legal duty) to disclose personal information. It provides that any person can lawfully disclose information, where necessary or expedient for any provision of the Act, to a Chief Officer of Police, a Police Authority, Local Authorities, Probation Provider or Health Authority (or to a person acting on behalf of any of these bodies), even if they do not otherwise have this.

This legislation satisfies the lawful basis for processing/disclosing information mentioned earlier under Schedule 2 Part 1 of the Data Protection Act 2018 and [Part 3 of the DPA 2018](#).

If the sharing of information with partner agencies is for preventing crime and disorder and the requirements of the DPA 2018/CLDC/HRA are satisfied, then that sharing by or on behalf of **[Insert name of organisation]** will have a lawful basis.

### European Convention on Human Rights (ECHR)

[Article 8 of the ECHR](#) states that everyone has the right to respect for private and family life, home and correspondence.

A public authority cannot interfere with an individual's Article 8 rights 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.

This is a qualified right that may therefore be interfered with *if the interference is necessary and proportionate for a legitimate aim*.

The legitimate aims of the information sharing are as set out in *Chapter 2 of Part 3 of the Act* (see above) and only information that is assessed as being necessary and proportionate for one of those aims will be shared between parties.

### Case by case judgement

Each instance where personal or sensitive information need to be shared for safeguarding purposes should be decided through a case-by-case assessment which considers whether the informed consent of the individual can be obtained and the proposed sharing being necessary, proportionate and lawful.

This should clearly be documented and recorded with the rationale given for your decision. This is described in greater detail in [GMC 'Confidentiality: good practice in handling patient information guidance'](#) (May 2018): -

- Best interest disclosure where the person lacks capacity to consent (see Page 16: para 16).
- Disclosure required or permitted by law (see Page 16: para(s) 17-19)
- The disclosure can by law be justified in the public interest (see Page 18 para(s) 22 - 23)

The GMC website also has a useful [Confidentiality decision tool](#)

If a data subject has not consented to the sharing of personal information in relation to them and no other legitimate conditions apply, then data should NOT be shared/disclosed.

If BSW ICB staff are not sure regarding information sharing or consent issues, they should seek advice from their organisational Caldicott Guardian and Information Governance Team.

### Common Law Duty of Confidentiality

The [Common Law Duty of Confidentiality \(CLDC\)](#) is built up from case law and its basis is that information that has the necessary quality of confidence should not be used or disclosed further, except as originally understood by the discloser, or with their subsequent permission. Some situations and relationships (such as Doctor/Patient relationship) also add a level of quality to the information imparted, which can help to achieve the necessary threshold for CLDC.

Case law has been established that exceptions can exist “in the public interest”; and confidentiality can also be set aside, by legislation (see above <https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality> Schedule 2 Part 1 DPA Act 2018 and GMC ‘Confidentiality: good practice in handling patient information guidance’).

The Department of Health & Social Care has also produced a code of practice concerning confidentiality, which is required practice for those working within or under contract to NHS organisations. [DH – Code of Practice on protecting the Confidentiality of service user information](#) (see 19.0 Legislation Compliance & References).

### The Caldicott Principles

Confidentiality is an important ethical and legal duty, but it is not an absolute. You may disclose personal information without breaching duties of confidentiality in certain circumstances and these are described in greater detail in the [GMC ‘Confidentiality: good practice in handling patient information guidance’](#) (May 2018)

Principle 7 of the Caldicott explains that duty to share information can be as important as the duty to protect patient confidentiality. Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

**Please remember** that if in doubt you should always consult with the Caldicott Guardian and/or Information Governance Officer for the organisation for further advice and guidance before sharing personal or sensitive information for Prevent purposes.

## **APPENDIX 4a - PRACTICAL INFORMATION SHARING FOR PREVENT PURPOSES**

Please consider all the following when making a Prevent referral or when responding to a request for personal or sensitive information relating to a Prevent inquiry.

### **1. Consent:**

The primary conditions for disclosing personal sensitive information about staff members, patients or service users for the purposes of Prevent should always be based on informed consent, however this may not always be appropriate or achievable.

If consent is not appropriate or achievable then a different lawful basis must be met (see 2: Legal gateways and exemptions) in order to share personal data. If another lawful basis is not met, then data cannot be shared.

Legal gateways and exemptions exist to facilitate the sharing of personal data without consent and for public interest reasons. Exemptions should not routinely be relied upon or applied in a blanket fashion. You must consider each exemption on a case-by-case basis

### **2. Legal gateways and exemptions**

Data Protection Act 2018 (DPA 2018)

[Schedule 2, Part 1, Para 2 of the DPA 2018](#) (Potential Exemption)

Allows for the processing of personal data for the purposes of (but not limited to):

- *the prevention or detection of crime*  
*the apprehension or prosecution of offenders*

[Section 115 of the Crime and Disorder Act 1998](#) (Permissible power)

The sharing of data by public sector bodies requires the existence of a power to do so, in addition to satisfying the legal requirements of the DPA 2018, the Human Rights Act 1998 (HRA 1998) and the [Common Law Duty of Confidentiality \(CLDC\)](#) Section 115 of the C&D Act 1998 provides agencies and professionals with the power (but not a legal duty) to disclose personal information.

### **3. Case by case decisions**

Each instance where personal or sensitive information need to be shared for safeguarding purposes should be decided through a case-by-case assessment by the safeguarding professional, which considers whether the informed consent of the individual can be obtained; any exemptions which are being relied upon as described above (Section 2 Legal gateways and exemptions), and that the proposed information sharing is necessary, proportionate and lawful.

### **4. Prevent referrals**

When making a Prevent referral please consider all the following: -

- You should use the standard National Prevent Referral form (attached) to make the referral to your SO15 contact and the relevant Local Authority Prevent Coordinator using secure email i.e. via your NHS.net account.

- You should include contact details detailing in the National Prevent Referral form (see above) where possible, the original source of person who made the initial referral within your organisation). This will ensure that that the referral source can be contacted where necessary by the Requesting agency.
- The email should always be protectively marked at OFFICIAL SENSITIVE
- If it has been decided that seeking consent from the patient/service user/staff member to refer is not appropriate you should always clearly document your decision and rationale in the record i.e. explain which public interest/best interest considerations have been applied to set aside their rights under the CLDC the DPA 2018/HRA1998.
- If consent has not been sought from the individual, you should also include wording in your email to explain the basis on which you are sharing their information.

Example: -

"This referral is being made without seeking the prior consent of the patient/service user /staff member, (~~\*\*delete where applicable~~), and I am applying the legal exemptions (contained in the 'Data Protection Act 2018 –'Schedule 2 Part 1 para i.e. the prevention or detection of crime and to protect wider members of the public from harm") and in accordance with permissible powers contained in Section 115 of the Crime and Disorder Act 1998. I believe this is reasonable and justified, appropriate, proportionate and necessary action which is in the wider *public interest*."



## 5. Important points to consider

Any information sharing for Prevent purposes with partners must be undertaken within the existing statutory framework(s) as defined in the DPA Act 2018/HRA 1998 and the [Common Law Duty of Confidentiality \(CLDC\)](#) (the CLDC is an additional legal requirement for health and must be satisfied in addition to the DPA 2018/HRA 1998).

Consent must always be considered on a case by basis taking into account if there are tangible public interest or best interest considerations (i.e. if in your professional opinion the individual may be of harm to themselves or others, and patient consent should therefore legitimately be overridden in this instance). Without this, there is no legal basis to share personal or sensitive information between statutory agencies.

When external partners i.e. police local authority request patient/staff information from health providers for Prevent purposes, it is advisable that you always consider the following: -

- Has the Requestor used an appropriate official information sharing request proforma sanctioned by their organisation? Different organisations have different forms for sharing personal data, and they should always be sent by secure protectively marked email.
- Has the Requestor included/cited the permissible powers and legal exemptions which are being relied upon in cases where the individual's consent has not been sought to share their personal or sensitive information (as described in Legal gateways and exemptions)? i.e. [Section 115 Crime & Disorder](#) and legal gateways such as [Section 2 /Pt1Para2 of the Data Protection Act 2018](#) (i.e. for the purposes of prevention and detection of crime etc.).

### Providing a 'form of words'

- Has the Requester i.e. police or local authority provided a legitimate reason for you to share patient/service user/staff member's personal or sensitive information with them?

In other words, has the Requester explained in broad terms why informed consent has not been sought to share their personal or sensitive information? i.e. that there are tangible public interest/best interest considerations where the individual is at risk of being drawn into terrorism and by informing them, we may prejudice the intended outcome'

This basic information will then enable the health provider to in turn satisfy themselves that:

- there are tangible public interest/best interest considerations for providing the information being requested;
- the relevant public interest/best interest exemption will therefore override your duty to protect patient information;
- it is legitimate to provide information specific to the safeguarding concern which has been identified by the Requestor

By way of context; there are occasional instances where this level of information has not initially been provided by the Requestor/local authority/police, and this failure to adhere to these requirements has caused blockages in release of information by health providers to Prevent leads.

### Being specific

- Requestors should explain to you what specific/relevant information is required from the patient/service user/staff member record to assist with the case management of the individual in question. Health providers should only release information, which is relevant, necessary and proportionate to the public interest described in the request. This will always come down to your own professional judgement and based on the nature of the inquiry and the information provided by the Requestor.

## 6. Summary

Confidentiality is an important ethical and legal duty, but it is not an absolute. You may disclose personal information without breaching duties of confidentiality in certain circumstances and these are described in greater detail in the in the [GMC 'Confidentiality: good practice in handling patient information guidance'](#) (May 2018).

7. If all the conditions as described above in '*5. Important points to consider*' are met, the health provider should share the information as requested under the aforementioned 'Public Interest' exemptions or if a Best Interest decision has been taken (for a person who lacks capacity) which can exempt patient confidentiality.
  - Principle 7 of the Caldicott explains that duty to share information can be as important as the duty to protect patient confidentiality. Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by their employers, regulators and professional bodies.
  - However there have been instances where health providers have refused to release information to the Requestor citing patient confidentiality - even where a public interest has been clearly defined and articulated by the Requestor. This can cause unnecessary delays in partner agencies initiating important safeguarding measures to protect the individual and others.
  - **Please remember** that if in doubt you should always consult with your organisational Caldicott Guardian and or Information Governance Officer for your organisation for further advice and guidance if you have any concerns about sharing personal or sensitive information for Prevent purposes.

**Don't forget to write it down-always document your decision-making and rationale at the time.**

## APPENDIX 5- DEFINITION OF TERMS

<b>Terrorism</b>	Actions of individuals or groups who seek to bring about social or political change through actions intended to cause serious harm, loss of life or raise attention through fear and/or damage to property to cause loss of life, disruption or raise attention by fear and/or damage to property
<b>Radicalisation</b>	The process of grooming an individual to support, encourage or condone violence to advance terrorist ideology
<b>Extremism</b>	Vocal or active opposition to fundamental values including democracy, the rule of the law, individual liberty, and mutual respect and tolerance of different beliefs and faiths. We also include in the definition of extremism calls for the death of members of our armed forces, weather in this country or overseas.
<b>CONTEST Strategy</b>	Sits under the Home Office and is a national strategy or long-term plan of action designed to reduce the risk of terrorism, by stopping people becoming terrorists, preventing terrorist attacks, strengthening the UK's resilience to terrorism and facilitating emergency preparedness procedures in the event of attack.
<b>Prevent duty</b>	<p>Safeguarding and support for those at most risk of radicalisation through early intervention, identifying them and offering support.</p> <p>Enabling those who have already engaged in terrorism to disengage and rehabilitate.</p> <p>Tackling the causes of radicalisation and responding to the ideological challenge of terrorism.</p>
<b>Vulnerability</b>	In the context of <i>Prevent</i> is a person who is susceptible to extremists' messages and is at risk of being drawn into terrorism or supporting terrorism at a point in time.
<b>Channel</b>	<p>Multi-agency approach to protect people at risk from radicalisation. It is entirely voluntary and requires the consent of the individual and or their parent or guardian (if aged under 18 years) to participate.</p> <p>Channel uses existing collaboration between local authorities, statutory partners (such as education and health sectors, social services, children's and youth services and offender management services, the police and the local community) to:</p> <ul style="list-style-type: none"> <li>• identify individuals at risk of being drawn into terrorism;</li> <li>• assess the nature and extent of that risk; and</li> <li>• develop the most appropriate support plan for the individual concerned.</li> </ul> <p>Channel is about safeguarding children and adults at risk from being drawn into committing terrorist-related activity. It is about early intervention to protect and divert away from the risk they face before illegality occurs.</p>

APPENDIX 6 - Reporting flow chart for Raising Concerns

**Action to take if you suspect an individual is being radicalised or self-radicalised into extremist activities**

