

Data Sharing Agreement between Counter Terrorism Policing South East, HMPPS/ OSCT Joint Extremism Unit (JEXU), Hampshire Constabulary, Thames Valley Police, Hampshire Fire and Rescue Service, West Hampshire Clinical Commissioning Group, Fareham and Gosport Clinical Commissioning Group, South Hampshire Clinical Commissioning Group, North Hampshire Clinical Commissioning Group, North East Hampshire and Farnham Clinical Commissioning Group, Hampshire and IOW Community Rehabilitation Company, Army Training Regiment (Winchester), University of Portsmouth, University of Southampton, University of Winchester, Home Group, HM Prison and Probation Service, Southampton Football Club, South Central Ambulance Service, Basingstoke & Deane Borough Council, East Hampshire District Council, Eastleigh Borough Council, Fareham Borough Council, Gosport Borough Council, Hart District Council, Havant Borough Council, New Forest District Council, Portsmouth City Council, Rushmoor Borough Council, Southampton City Council, Test Valley Borough Council, Winchester City Council, Test Valley Partnership and Hampshire County Council.

Prevent Board

Version 1.0

1. Introduction

1.1 The Prevent strategy, published by the Government in 2011, is part of our overall counter-terrorism strategy, CONTEST. The aim of the Prevent strategy is to reduce the threat to the UK from terrorism by stopping people becoming terrorists or supporting terrorism. In the Act this has simply been expressed as the need to “prevent people from being drawn into terrorism”.

The 2011 Prevent strategy has three specific strategic objectives:

- respond to the ideological challenge of terrorism and the threat we face from those who promote it
- prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support
- work with sectors and institutions where there are risks of radicalisation that we need to address.

1.2 Prevent work depends on effective partnership. To demonstrate effective compliance with the duty, specified authorities must demonstrate evidence of productive co-operation, in particular with local Prevent co-ordinators, the police and local authorities, and co-ordination through existing multi-agency forums, for example Community Safety Partnerships.

1.3 The Prevent programme must not involve any covert activity against people or communities. But specified authorities may need to share personal information to ensure, for example, that a person at risk of radicalisation is given appropriate support (for example on the Channel programme). Information sharing must be assessed on a case-by-case basis and is governed by legislation. To ensure the rights of individuals are fully protected, it is important that information sharing agreements are in place at a local level.

1.4 Sections 36 to 41 of the Counter-Terrorism and Security Act 2015 place a legal obligation on specified organisations to provide support for people vulnerable to being drawn into terrorism.

1.5 The Channel Panel programme involves a multi-agency approach to identify and provide support to individuals who are at risk of being drawn into terrorism. Partners of a Panel may be requested to provide information about an individual to the Channel Panel during the information gathering stage. There is a data sharing agreement for the Channel Panel.

2. Objectives and purpose of the Information sharing

- To prevent people from being drawn into terrorism.
- To identify and provide support for people vulnerable to being drawn into terrorism.

- To address risks of radicalisation.

The parties to this agreement (the Partner Organisations) agree that Information shared under this arrangement between Hampshire County Council and Counter Terrorism Policing South East, HMPPS/ OSCT Joint Extremism Unit (JEXU), Hampshire Constabulary, Thames Valley Police, Hampshire Fire and Rescue Service, West Hampshire Clinical Commissioning Group, Fareham and Gosport Clinical Commissioning Group, South Hampshire Clinical Commissioning Group, North Hampshire Clinical Commissioning Group, North East Hampshire and Farnham Clinical Commissioning Group, Hampshire and IOW Community Rehabilitation Company, Army Training Regiment (Winchester), University of Portsmouth, University of Southampton, University of Winchester, Home Group, HM Prison and Probation Service, Southampton Football Club, South Central Ambulance Service, Basingstoke & Deane Borough Council, East Hampshire District Council, Eastleigh Borough Council, Fareham Borough Council, Gosport Borough Council, Hart District Council, Havant Borough Council, New Forest District Council, Portsmouth City Council, Rushmoor Borough Council, Southampton City Council, Test Valley Borough Council, Winchester City Council and Test Valley Partnership will only be used for the purposes set out in section 2 of this agreement and will not be used for any other purpose including commercial or marketing purposes.

3. What data will be shared and how long will it be kept?

3.1 Hampshire County Council to Counter Terrorism Policing South East, HMPPS/ OSCT Joint Extremism Unit (JEXU), Hampshire Constabulary, Thames Valley Police, Hampshire Fire and Rescue Service, West Hampshire Clinical Commissioning Group, Fareham and Gosport Clinical Commissioning Group, South Hampshire Clinical Commissioning Group, North Hampshire Clinical Commissioning Group, North East Hampshire and Farnham Clinical Commissioning Group, Hampshire and IOW Community Rehabilitation Company, Army Training Regiment (Winchester), University of Portsmouth, University of Southampton, University of Winchester, Home Group, HM Prison and Probation Service, Southampton Football Club, South Central Ambulance Service, Basingstoke & Deane Borough Council, East Hampshire District Council, Eastleigh Borough Council, Fareham Borough Council, Gosport Borough Council, Hart District Council, Havant Borough Council, New Forest District Council, Portsmouth City Council, Rushmoor Borough Council, Southampton City Council, Test Valley Borough Council, Winchester City Council and Test Valley Partnership.

- Names and contact information for the people may need support
- Allegations and details of behaviour, including online activity
- Family situation and details of associates
- Sensitive personal information such as details of vulnerabilities and risks to health and wellbeing
- Information about previous cautions and convictions
- Background information, such as education or housing, if relevant.

Each Party will securely retain and dispose of personal data in line with their own organisation's retention schedule.

3.2 Counter Terrorism Policing South East, HMPPS/ OSCT Joint Extremism Unit (JEXU), Hampshire Constabulary, Thames Valley Police, Hampshire Fire and Rescue Service, West Hampshire Clinical Commissioning Group, Fareham and Gosport Clinical Commissioning Group, South Hampshire Clinical Commissioning Group, North Hampshire Clinical Commissioning Group, North East Hampshire and Farnham Clinical Commissioning Group, Hampshire and IOW Community Rehabilitation Company, Army Training Regiment (Winchester), University of Portsmouth, University of Southampton, University of Winchester, Home Group, HM Prison and Probation Service, Southampton Football Club, South Central Ambulance Service, Basingstoke & Deane Borough Council, East Hampshire District Council, Eastleigh Borough Council, Fareham Borough Council, Gosport Borough Council, Hart District Council, Havant Borough Council, New Forest District Council, Portsmouth City Council, Rushmoor Borough Council, Southampton City Council, Test Valley Borough Council, Winchester City Council and Test Valley Partnership to Hampshire County Council

- Names and contact information for the people who may need support
- Allegations and details of behaviour, including online activity
- Family situation and details of associates
- Sensitive personal information such as details of vulnerabilities and risks to health and wellbeing
- Information about previous cautions and convictions
- Background information, such as education or housing, if relevant.

The data will be stored and disposed of in accordance with Hampshire County Council's data retention policy.

4. Data Controller

4.1 Each Partner Organisation will continue to be the data controller as defined by the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA2018) (and any successor legislation) for the personal data it holds and retain the responsibilities held with this position.

4.2 Each Partner confirms that it is registered with the Information Commissioner's Office as a Data Controller.

4.3 Each Partner Organisation will become a separate data controller for the data received for the purposes defined in paragraph 2 of this agreement.

4.4 Each Partner Organisation will ensure that any personal data received under this agreement will only be used for the purposes defined in paragraph 2.

4.5 Each Partner as a Data Controller acknowledges its obligations under the GDPR and DPA2018 when processing personal data, which can include collecting, storing, amending and disclosing data.

4.6 Each Partner Organisation agrees that they will only process personal data shared under this agreement within the EU. Should they wish to process personal data outside the EU they will obtain the prior written consent from the signatory of the Partner organisation.

5. Arrangements for the safe transmission of data

5.1 The personal data shared between the Partner Organisations will be shared using secure methods of transfer. Information may also be shared verbally between the Partner Organisations by telephone and at meetings.

5.2 Referrals and further information will be sent by secure email. Information sent over the telephone will not include personal data or will only be sent when a member is confident that they will not be overheard by anyone who should not be party to the information.

5.3 Once the personal data is shared between the Partner Organisations it will be necessary for it to be stored securely to ensure that it is protected and is not easily accessible. All approved officers within Hampshire County Council and Counter Terrorism Policing South East, HMPPS/ OSCT Joint Extremism Unit (JEXU), Hampshire Constabulary, Thames Valley Police, Hampshire Fire and Rescue Service, West Hampshire Clinical Commissioning Group, Fareham and Gosport Clinical Commissioning Group, South Hampshire Clinical Commissioning Group, North Hampshire Clinical Commissioning Group, North East Hampshire and Farnham Clinical Commissioning Group, Hampshire and IOW Community Rehabilitation Company, Army Training Regiment (Winchester), University of Portsmouth, University of Southampton, University of Winchester, Home Group, HM Prison and Probation Service, Southampton Football Club, South Central Ambulance Service, Basingstoke & Deane Borough Council, East Hampshire District Council, Eastleigh Borough Council, Fareham Borough Council, Gosport Borough Council, Hart District Council, Havant Borough Council, New Forest District Council, Portsmouth City Council, Rushmoor Borough Council, Southampton City Council, Test Valley Borough Council, Winchester City Council and Test Valley Partnership must ensure that they take appropriate measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.

5.4 Information received by Hampshire County Council will be stored in a secure and confidential folder in Sharepoint or in confidential folders.

5.5 If a Partner wants to share any information outside of the meeting they must seek permission from the Chair.

6. Legal Justification for Sharing the Data

6.1 Where Personal data may be processed according to in GDPR Article 6, the lawful basis will likely be:

- Art 6 (1)(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

6.2 The statutory duties that may apply include:

For Prevent:

- Section 26 of the Counter-Terrorism and Security Act 2015 to reduce the risk of radicalisation and offer support to those who are at risk

When a Channel Panel referral is received:

- Sections 36 to 41 of the Counter-Terrorism and Security Act 2015 to provide support for people vulnerable to being drawn into terrorism.

6.3 Where Special category data will be processed, in addition to an Article 6 condition, The relevant Article 9 conditions for Special Category will likely be:

- Art 9(2)(g) Processing is necessary for reasons of substantial public interest on the basis of Union or Member State Law.

6.4 The Data Protection Act includes additional requirements (conditions) where a Data Controller is relying on Article 9 (2)(g) for Processing Special Category Data (necessary for reasons of substantial public interest on the basis of Union or Member State Law). These are set out in DPA18 Schedule 1 Part 2, they require an appropriate policy document. Relevant conditions to this Agreement include:

- Statutory and government purposes: where the processing is necessary for reasons of substantial public interest and where the purpose is the exercise of a function conferred on a person by an enactment or rule of law
- 'preventing or detecting unlawful acts' enables processing of relevant special category (sensitive and personal) data where processing is necessary for the purposes of the prevention or detection of an unlawful act and is necessary for reasons of substantial public interests, and sharing without consent is necessary so not as to prejudice the prevention or detection of a crime.
- 'safeguarding of children and individuals at risk' enables processing relevant special category (sensitive and personal) data without consent if it is to keep a child or individual at risk safe from neglect or physical, emotional or mental harm, or if it is protecting their physical, mental, or emotional well-being AND the individual cannot consent, or it cannot be reasonably expected to gain consent from the individual, or if the act of gaining consent could place a child or adult at risk.

7. Fair Processing/ Privacy Notices

7.1 The partners to this agreement recognise their duty under the GDPR to provide information proactively and on request to individuals about how their information is processed.

7.2 Each Partner will ensure that their privacy notices give details of the processing of personal data and will be provided when:

- the data is collected from a data subject; or
- they receive personal data from another organisation.

7.3 The sharing of information under this agreement is covered by the privacy notices published by the individual partners to this agreement:

8. Responsibilities when Sharing Information

General

8.1 Each Partner Organisation shall be responsible for ensuring that they have technical, organisational and security measures in place to protect the personal data and to ensure the lawful use of such information shared under this Agreement.

8.2 Each Partner Organisation accepts responsibility for independently or jointly auditing compliance.

8.3 Each Partner Organisation shall ensure that their staff comply with their rules and policies in relation to the protection and use of shared data and that staff have received sufficient training and are aware of their individual responsibilities in relation to data protection and the confidentiality, integrity and availability of personal data. Each organisation will ensure that appropriate sanctions and disciplinary procedures are in place to deal with noncompliance.

8.4 Each Partner Organisation shall have a written policy for the retention and disposal of the personal data shared under this Agreement.

8.5 Each Partner Organisation shall be aware that consent should only be relied on as the basis for processing and sharing the data where there are no other legal basis under the GDPR. Partners shall be aware that a data subject may withdraw consent without detriment at any time to the processing of their personal data

Personal Data

8.6 Personal data may only be shared where there is a specific lawful purpose under Article 6 GDPR and Article 9 GDPR (when the sharing includes Special Category Data)

8.7 Staff of Partner Organisations may only be permitted access to the personal data shared under this Agreement when necessary in order for them to perform their duties in connection with the services they are required to deliver.

8.8 This Agreement does not permit unrestricted access to the personal information held by the other Partner Organisation. It sets out the parameters for the safe and secure sharing of information for a justifiable need to know purpose.

8.9 Each Partner Organisation shall be responsible for ensuring every member of its staff with access to the personal data shared under this Agreement is aware of and complies with their obligation under the GDPR, DPA 2018,, their common law duty of confidentiality and the responsibility to disclose information only to those who have a right to see it.

8.10 Each Partner Organisation shall ensure that any of its staff accessing information follow the principles and standards that have been agreed and incorporated within this Agreement.

9. Restrictions on use of Information Shared

All information must only be used for the purpose(s) specified in this agreement unless required under statute or regulation, or by court order.

10. Security

The Partner Organisations shall have appropriate technical and organisational measures in place to protect the security, confidentiality, integrity and availability of the personal information (both electronic and hard copy) during all stages of processing. (e.g. transfer, storage, access and deletion)

11. Training

All Partner Organisations will ensure that any staff processing information shared under this Protocol are trained in data protection and are fully aware of their responsibilities to maintain the accuracy, security and confidentiality of personal information in an efficient and lawful manner. Staff will also be made aware of the requirements to provide privacy notices when sharing or receiving personal data.

12. Individual Responsibilities

12.1 Every individual working for the Partner Organisations is responsible for the safekeeping of any information they obtain, handle, use and disclose.

12.2 Every individual should know how to obtain, use and share information they legitimately need to do their job.

12.3 Every individual should follow the guidelines set out in this Agreement and seek advice when necessary.

13. Data Accuracy, Rectification, Erasure and Portability

13.1 Each partner will ensure that the personal data they process and share under this agreement is accurate and up to date.

13.2 Where data is rectified (corrected) or erased or restricted under Articles 16, 17 or 18 GDPR the controller shall inform the other recipients to the extent required by Articles 19 and 4 of the GDPR and should the data subject request the identity of the recipients the controller shall provide the relevant information to the data subject.

14. Data Subject Rights

Each partner will process Data Subject Rights Requests in line with their own existing policies and practices, directing requestors under existing procedures, when the request is for data not held by that partner.

15. Freedom of Information Act considerations

Participating partner organisations acknowledge a duty to assist one another in meeting their individual responsibilities under the Freedom of Information Act 2000 to provide information subject to this agreement in response to formal requests.

16. Data Protection Incidents

16.1 Members of partner organisations working on Prevent Board shall be responsible for reporting all potential breaches of the Data Protection Act 2018, including unauthorised access to records, loss of personally identifiable information and unauthorised disclosures in line with the procedure used by the partner organisation employing the member of staff involved in the breach.

16.2 All potential breaches will be investigated and dealt with by the partner organisation where the breach occurs.

16.3 Each partner agrees to adhere to the required standards of security. If there is a potential data breach in which information received from another party under this agreement is compromised, the originating organisation will be notified immediately through an agreed process.

16.4 Decisions relating to the notification to data subjects or the Information Commissioners Office will be taken by the partner investigating the breach, who will also deal with correspondence with the Information Commissioner's Office.

16.5 The Partner Organisations will ensure that they implement any changes to processes or procedures required as a result of a data incident.

17. Commencement of this Agreement

Data will be shared under this Agreement between Hampshire County Council and Counter Terrorism Policing South East, HMPPS/ OSCT Joint Extremism Unit (JEXU), Hampshire Constabulary, Thames Valley Police, Hampshire Fire and Rescue Service, West Hampshire Clinical Commissioning Group, Fareham and Gosport Clinical Commissioning Group, South Hampshire Clinical Commissioning Group, North Hampshire Clinical Commissioning Group, North East Hampshire and Farnham Clinical Commissioning Group, Hampshire and IOW Community Rehabilitation Company, Army Training Regiment (Winchester), University of Portsmouth, University of Southampton, University of Winchester, Home Group, HM Prison and Probation Service, Southampton Football Club, South Central Ambulance Service, Basingstoke & Deane Borough Council, East Hampshire District Council, Eastleigh Borough Council, Fareham Borough Council, Gosport Borough Council, Hart District Council, Havant Borough Council, New Forest District Council, Portsmouth City Council, Rushmoor Borough Council, Southampton City Council, Test Valley Borough Council, Winchester City Council and Test Valley Partnership from the date when a named individual of each organisation signs the Declaration of Acceptance and Participation (below).

18. Review Arrangements

18.1 This Agreement will be reviewed every two years.

18.2 Any of the signatories can request an extraordinary review at any time where a joint discussion or decision is necessary to address developments or issues.

19. Agreement to abide by this Data Sharing Agreement

We the undersigned agree that each Partner Organisation that we represent will adopt and adhere to this Data Sharing Agreement:

Please sign the 'Declaration of Acceptance and Participation' form below and return to:
 Department Data Protection Lead

DECLARATION OF ACCEPTANCE AND PARTICIPATION
 (All sections of this form must be completed)

Your organisation:	
Your Name:	
Your Position:	
Signature:	
Date:	

Name(s) and email address(es) of individual(s) acting as main contact(s):	
Name(s) of additional individual(s) who will process received data:	

Your organisation:	Hampshire County Council
Your Name:	Sarah Snowdon
Your Position:	SIRO
Signature:	
Date:	

Names and email addresses of individuals acting as main contacts:	Primary Contact: Sarah Snowdon sarah.snowdon@hants.gov.uk Secondary Contact: Rob Vernon rob.vernon@hants.gov.uk
--	---

Names of additional individuals who will process received data:

--