Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project.

Version Control

Version	Reason	Date	Author(s)
1.0	New	15/03/2021	[redacted]
2.0	Amended drafts	Jan and March 2022	[redacted]
3.0	Reviewed and amended	March 2022	[redacted]
4.0	Reviewed	March 2022	[redacted]

Project / Work Stream Name	**London PREVENT/ChannelPanel Information Sharing**
Overview: **(Summary of the project/work stream)**	A legal requirement to ensure that persons are not drawn into terrorism was created by the Counter-Terrorism and Security Act 2015. To do this successfully, organisations need to share data about persons who may be at risk of radicalisation and being drawn into terrorism (PREVENT) , and run Channel Panels which assist in ensuring the legislative requirements are met. There are also Police-led Partnership Panels and Multi-Agency Assessment Centres (both run by police), This DPIA covers the Data Sharing Agreement (DSA) which is a multi-agency agreement for Prevent and Channel Panel. **Prevent** Prevent is one of four strands of the government's counter-terrorism strategy. It aims to stop people becoming terrorists or supporting terrorism. The Prevent Strategy was last revised in 2011, but a number of other advice documents have been published since for each sector. The three areas of focus are to: - respond to the ideological challenge of terrorism and the threat from those who promote it

	- prevent people from being drawn into terrorism and ensure they are given the right advice and support - work with institutions where there are risks of radicalisation that need to be addressed. Prevent work depends on effective partnership. To demonstrate effective compliance with the duty, specified authorities must demonstrate evidence of productive engagement, with local Prevent services, the police and local authorities, and co-ordination through existing multi-agency such as the Community Safety Partnerships. The Prevent Duty will sometimes require the sharing of personal and sensitive information between partners; this is particularly the case where sharing of information will be central to providing the best support to vulnerable individuals and meets the duties outlined in section 26 of the Counter-Terrorism and Security Act 2015 to have in place arrangements for the sharing of information between responsible authorities: Local government; Criminal justice; Education, child care, Health and social care; Police. Channel Panel The Channel Panel (the Prevent equivalent of MARAC) is a multi-agency safeguarding board in respect of Prevent. The potential partners to Channel, which are local authority safeguarding services and counter-terrorism police. Channel is about ensuring that children and vulnerable adults of any faith, ethnicity or background receive support before their vulnerabilities are exploited by those that would want them to embrace terrorism and before they become involved in criminal terrorist activity. Participating in this process means that partners are fulfilling their statutory duty to cooperate and protect vulnerable residents from being drawn into activities that could place themselves and others at risk of extreme harm. The information shared will be used to support the panel's assessment of the vulnerability of the subject, extent and vulnerability of radicalisation and the capacity and will of the person to be drawn into terrorism. The statutory Channel guidance issued by the Home Office categories these vulnerability factors as: Engagement, Intent, and Capability. The information will also be used to plan and put in place appropriate safeguarding measures. Information gathered will be used to inform the decisions of the panel and to complete the Vulnerability Assessment Framework (VAF) on the relevant Home Office and police case management systems. Information will also be provided to the Intervention Provider (IP) to inform the interaction.

Implementation Date:	1/4/22 although note that the sharing is ongoing this DPIA covers the new pan-London DSA
<u>Environmental Scan</u> **Describe the consultation/checks that have been carried out regarding this initiative or, project of similar nature, whether conducted within your organisation or by other organisations.**	PREVENT work is carried out In England, Wales and Scotland and is a legal obligation. This is a renewal of previous fragmented agreements, intended to cover all London.

Step 1: Complete the Screening Questions			
Q 1	**Category**	**Screening question**	**Yes/No**
1.1	Technology	Does the project introduce new or additional information technologies that can substantially reveal an individual's identity and has the potential to affect that person's privacy?	No
1.2	Technology	Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business?	No
1.3	Identity	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Local Gov. Identifier, Hospital ID no. or, will use intrusive identification or identity management processes or, electronic linkage of personal data?	Yes
1.4	Identity	Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	No
1.5	Multiple organisations	Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners?	Yes
Q	**Category**	**Screening question**	

1.6	Data	Does the project involve new process or significantly change the way in which personal data/special categories of personal data and/or business sensitive data is handled?	No
1.7	Data	Does the project involve new or significantly changed handling of a considerable amount of personal data/special categories of personal data and/or business sensitive data about each individual in a database?	No
1.8	Data	Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	No
1.9	Data	Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special categories of personal data and/or business sensitive data from multiple sources?	Yes
1.10	Data	Will the personal data be processed out of the U.K?	No
1.11	Exemptions and Exceptions	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	Yes
1.12	Exemptions and Exceptions	Does the project's justification include significant contributions to public security and measures?	Yes
1.13	Exemptions and Exceptions	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	No

The purpose of the screening questions is to confirm that the data protection laws are being complied with, or highlights problems that need to be addressed. It also aims to prevent problems arising at a later stage which might impede the progress or success of the project.

Answering "Yes" to any of the screening questions above represents a potential Information Governance (IG) risk factor, please proceed and complete the next section.

Step 2: Identify the need for a DPIA		
2.1	**Is this a new or changed use of personal data/special categories of personal data and/or business sensitive data that is already processed/shared??**	New/Changed Changed
2.2	**What data will be processed/shared/viewed?**	

	Personal Data									
	Forename	yes	Surname	yes	Date of Birth	yes	Age	yes	Gender	yes
	Address	yes	Postal address	yes	Employment records	yes	Email address	yes	Postcode	yes
	Other unique identifier (*please specify*)		Telephone number	yes	Driving licence number	No	NHS No	yes	Hospital ID no	yes
	Other data (Please state):		Due to the complexity of the Prevent referral process, providing a prescriptive list of data fields to be shared is difficult. Not all the information below will be shared in every case; only relevant information will be shared on a case-by-case basis where an organisation has a 'need-to-know' the information. Data that can be shared includes: ● personal information (name, DOB, ethnicity, address, telephone, email, NHS number, proof of identity, unique pupil number); ● parents'/carers' personal information; ● personal information about other members of household; ● personal information about close relatives; ● details of family relationships in and outside of the household; ● data subject and family's legal status; ● accommodation; ● employment status; ● details about physical and emotional well-being and parenting; ● details of any risk issues; ● health, social care or other services provided; ● information about situation given to us by family/carers and/or other organisations (e.g. GP, school nurse, Police);								

		● reports relating to situation (e.g. safeguarding and other assessments, Child Protection Plans and Looked After Children reviews); ● educational progress and attainment information; ● school attendance, exclusions and behavioural information; and ● information such as court orders and professional involvement; ● The data subject and immediate families' immigration history if relevant to the case (e.g. intelligence suggesting radicalisation / affiliation with foreign or transnational extremist or terrorist organisations); ● police audio and video recording, although this will only be shared with individual panel members where it will enable them to more effectively assess vulnerability and plan appropriate safeguarding measures. It will not be routinely shared with all panel members. ● any documents sent to us relating to the data subject (e.g. referrals received from other agencies and professionals);

Special Categories of Personal Data

Racial or ethnic origin			yes	Political opinion		yes	Religious or philosophical beliefs				yes
Trade Union membership			yes	Physical or mental health or condition							yes
Sexual life or sexual orientation		yes	Social service records		yes	Child protection records					yes
Sickness forms	yes	Housing records	yes	Tax, benefit or pension records		yes	Adoption records				yes
DNA profile	No	Fingerprints	No	Biometrics	No	Genetic data					No
Proceedings for any offence committed or alleged, or criminal offence record											yes

Other data *(Please state):*	Sensitive information (both special categories of personal data and criminal offences data) that can be shared may include: ● youth offending information: offences (including alleged offences), criminal proceedings, convictions and sentences;	

		● medical history; ● mental health history ● religious or philosophical beliefs in this context may include (this is an indicative not an exhaustive list): ○ The extreme far- right ○ Al Qaeda inspired or Daesh inspired extremist ideology ○ Animal rights extremism ○ Environmental extremism ○ Dissident Irish extremism ○ Any kind of ideology that encourages violence as an outlet This may be information relating to the individual or to others.	

	Yes
Will the dataset include clinical data? (please include)	Yes where health records are shared by NHS partners
Will the dataset include financial data?	Yes where relevant

Description of other data processed/shared/viewed?

Information shared by the Counter Terrorism Case Officer (CTCO) and the Prevent lead is likely to include personal information including:

- name
- date of birth
- recent offending history, arrests and charges,
- Crimint+ information
- court appearances
- sentencing
- prison data
- any other relevant information held on MPS systems as appropriate for a risk assessment to be made on an individual.

Information will be taken from the following MPS systems by the CTCO.

- CRIS
- PNC
- Crimint+
- Merlin

	● Stops Database ● CAD

2.3	Business sensitive data			
	Financial	No		
	Local Contract conditions	No		
	Operational data	No		
	Notes associated with patentable inventions	No		
	procurement/tendering information	No		
	Customer/supplier information	No		
	Decisions impacting:	One or more business function	**Yes/No**	
			No	
		Across the organisation	No	
	Description of other data processed/shared/viewed (if any).			
	N/A			

Step 3: Describe the sharing/processing			
3.1	**List of organisations/partners involved in sharing or processing personal/special categories personal data?** *If yes, list below*		Yes/No
			Yes
	Name	Controller or Processor?	Completed and compliant with the IG Toolkit or Data Security and Protection (DSP) Toolkit
			Yes / No
	London Local Authorities	Controller	Yes

	Metropolitan Police Service, British Transport Police & City of London Police	Controller	Yes
	National Probation Service	Controller	Yes
	Local health partner (including GPs, clinics etc.)	Controller	Yes
	London CCGs	Processor	Yes
	Department for Work & Pensions (inc Job Centre Plus)	Controller	Yes
	London Ambulance Service	Controller	Yes
	Local substance misuse partner	Controller	Depends on how constituted; mixed
	Local housing partner if ALMO	Controller	Depends on how constituted; mixed
	Local voluntary groups	Controller	Depends on how constituted; mixed
	Home Office	Controller	Not necessary
3.2			Yes/No
	If you have answered 'yes' to 3.1 is there an existing ' Data Processing Contract' or 'Data Sharing Agreement' between the Controller and the Processor?		Yes - A single DSA will be put in place to cover sharing with the listed partners where they are Controllers. Each Local Authority will be responsible for ensuring that they have Data Processing Contracts in place with any local Processors.
3.3.	**Has a data flow mapping exercise been undertaken?** **If yes, please provide a copy, if no, please undertake**		The DSA includes statements on flows, but in general data is shared within the Channel Panel

		process, and a few other police-managed risk management processes; actual flows are based on need.
3.4	**Does the project involve employing contractors external to the Organisation who would have access to personal or special categories of personal data?**	Yes / No
		No
3.5	**Describe in as much detail why this information is being processed/shared/viewed?** Section 26 of the Counter Terrorism and Security Act 2015 placed a duty on specified agencies in the exercise of their functions to have "due regard to the need to prevent people from being drawn into terrorism". Local authorities have a multi-agency Prevent Coordination, which ensures that the specified agencies are compliant with the duty. Section 36 of the Counter Terrorism and Security Act 2015 sets out the duty on local authorities and partners of local panels to provide support for people vulnerable to being drawn into terrorism. In England and Wales, this duty is met through Channel panels. Prevent requires a multi-agency approach to protect people at risk from radicalisation. Effective information sharing is a vital element of the agencies' roles in effective management of Prevent and Channel. Organisations can hold different pieces of information which need to be placed together to enable a thorough assessment and plan to be made. For further details, see the Overview on page 1 of this DPIA; Section 2 (Purpose and Benefits) in the DSA; and the Channel Duty Guidance published on HMG website: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/964567/6.6271_HO_HMG_Channel_Duty_Guidance_v14_Web.pdf	

Step 4: Assess necessity and proportionality	
4.1	**Lawfulness for Processing/sharing personal data/special categories of personal data?**
	For purposes other than law enforcement by competent authorities Articles 6 (1), 9 and 10 of the UK GDPR, and section 8 of the DPA 2018 set out the acceptable conditions for the processing and sharing of personal, special category, and criminal data. The conditions relevant in the UK GDPR to data processed under this agreement are below. **Article 6 (1) - Personal Data Processing** ● **(c)** processing is necessary for compliance with a **legal obligation** to which the controller is subject. This applies to non-local authority signatories to the DSA. Section 38 of the CT&S Act (amended by the Counter-Terrorism and Border Security Act 2019), requires Channel partners to co-operate with the local authority and the police in providing any relevant information to the panel so that they can effectively carry out their functions to determine whether an individual is vulnerable to being drawn into terrorism ● **(e)** processing for the purposes of Channel relies on Article 6(1)(e) GDPR: the 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. Also includes (a) processing of personal data that is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and (b) processing of personal data that is necessary for the exercise of a function of the Crown, a Minister of the Crown or a government department. Use of this article requires that the Data Protection Act section 8 be satisfied. In particular processing of personal data for Channel is necessary for the purposes of the various Channel duties set out in section 36 of the Counter-Terrorism and Security Act 2015 (CTSA). The purpose for the function is to put in place a local panel to carry out assessments and provide support for persons vulnerable to being drawn into terrorism; and Section 20 of Counter Terrorism and Border Security Act 2019 amends the act to enable Police and Local authority to refer individuals for assessment by the panel if there are reasonable grounds to believe that the individual is vulnerable to being drawn into terrorism. Deidentified or pseudonymised data may also be used for strategic purposes under the duties in the The Crime and Disorder (Prescribed Information) Regulations 2007 See Appendix C of the DSA for further details of the applicable legislation. **Article 9(2) - Special Category Data Processing** ● (b) **social protection law** - processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law. Use of this article requires DPA18 S 10(2) be satisfied which needs a condition Schedule 1, Part 1 to be met. For this agreement these are: ○ Employment, social security and social protection under Para 1(1)(2)(3). This requires an appropriate policy document, and this document will form part of the policy for such processing, although competent authorities will need to satisfy

themselves that their own internal policy documents fully cover such use. The underpinning laws are set out in Appendix C of the DSA

(g) **substantial public interest** - processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

Use of this article requires that the Data Protection Act Section 10(3) be satisfied. This requires that a condition within Schedule 1, Part 2 is met. For this agreement these are:

- Statutory etc., and government purposes under Para 6(1)(2)
- Preventing and detecting unlawful acts under Para 10(1)(2)(3)
- Safeguarding children and individuals at risk under Para 18(1)(2)(3)(4)

Article 10 - Processing of personal data relating to Criminal Convictions and Offences data

This requires that DPA 2018 Section 10(5) be satisfied. This requires that the processing meets a condition is Schedule 1 Parts 1,2 or 3. For this agreement these are:

- Statutory etc., and government purposes under Para 6(1)(2)
- Preventing and detecting unlawful acts under Para 10(1)(2)(3)
- Safeguarding children and individuals at risk under Para 18(1)(2)(3)(4)
- Suspicion of terrorist financing or money laundering Para 15

  Use of DPA Schedule 1 Paragraph 15 - This condition is met if the processing is necessary for the purposes of making a disclosure in good faith under either of the following—

  (a)(a) (a) section 21CA of the Terrorism Act 2000 (disclosures between certain entities within regulated sector in relation to suspicion of commission of terrorist financing offence or for purposes of identifying terrorist property).;

For the purposes of law enforcement by competent authorities

The “competent authorities” are defined in Section 30 of the DPA which refers to Schedule 7. The competent authorities under the DSA are generally (but not exclusively) police, probation services, youth offending teams and government departments.

The “law enforcement” purposes are defined in Section 31 of the DPA as “*prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”.*

There are additional safeguards required for “sensitive processing”. This is defined in Section 35(8) as:

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation.

The additional requirements are given in Section 35(4) and (5). Both require an appropriate policy document, and the DSA will form part of the policy for such processing, although competent authorities will need to satisfy themselves that their own internal policy documents fully cover such use.

Section 35(4) requires the consent of the data subject, 35(5) requires that the processing be strictly necessary for the law enforcement purposes, and meets a condition in Schedule 8.

For the processing in relation to the purposes here, the following conditions in Schedule 8 are met:

- Statutory etc. purposes Para 1(a)(b);
- Administration of justice Para 2;
- Protecting individual's vital interests Para 3;
- Safeguarding of children and of individuals at risk Para 4(1)(2)(3)(4);

The applicable legislation that provides the lawful basis is listed in more detail in *Appendix C – Applicable legislation* of the DSA.

In order for competent authorities to carry out and share sensitive personal data with partners:

- that processing must be strictly necessary; and
- at least one condition specific in Schedule 8 of the DPA be satisfied. An analysis of three relevant conditions is set out below:

Strict necessity

Although it is difficult to anticipate all the circumstances in which sharing under this agreement may be necessary, in general competent authorities do not consider that there are any other less intrusive means of obtaining personal data held by partners.

The reasons for the necessity of sharing personal data is set out in Sections 2 and 2.1 (above) and 2.6 (below).

Schedule 8 conditions

The following conditions set out in Schedule 8 of the DPA 2018 are likely to be satisfied, depending on the precise context of the data processing:

Paragraph 1: Statutory etc purposes

This condition is met if the processing—

	(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and (b) is necessary for reasons of substantial public interest. The processing of the data is carried out in the exercise of the legal powers and duties of the MPS. It is plainly in the substantial public interest that for example witness, victims and potential suspects are located as soon as reasonably practicable by the police. Paragraph 3: Protecting individual's vital interests This condition is met if the processing is necessary to protect the vital interests of the data subject or of another individual. This condition is met in cases where there is a risk to the life of the of the data subject or where the data subject poses a threat to the life of either his or herself or the life of others. This may be the case where the police consider that a victim faces an ongoing risk of harm. Paragraph 4: Safeguarding of children and of individuals at risk (1) This condition is met if— (a) the processing is necessary for the purposes of— (i) protecting an individual from neglect or physical, mental or emotional harm, or (ii) protecting the physical, mental or emotional well-being of an individual, (b) the individual is— (i) aged under 18, or (ii) aged 18 or over and at risk, (c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and (d) the processing is necessary for reasons of substantial public interest. (2) The reasons mentioned in sub-paragraph (1)(c) are— (a) in the circumstances, consent to the processing cannot be given by the data subject; (b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing; (c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a). (3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual— (a) has needs for care and support (b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

	(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it. (4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual. This condition is met where the child or vulnerable adult is at risk of harm (whether physical or mental), and the police are unable to obtain consent for any of the reasons listed in para 4(2). This condition will be met in most cases given the serious risk of harm posed to missing children or vulnerable adults in the aftermath of a major incident. The terms of this agreement address the requirements for data sharing pursuant to Part 3 of the DPA 2018. To note that there is a separate regime for intelligence service processing, which falls outside the remit of this DSA.		
4.2	**Will the information be processed/shared electronically, on paper or both?**	Electronic	yes
		Paper	yes
4.3	**How will you ensure data quality and data minimisation?**		
Each partner is responsible for ensuring the accuracy and relevance of the personal data that it processes and shares and must have clear processes in place for managing data quality. Any party learning of the inaccuracy of personal data is responsible for informing the parties with whom that data has been shared.			
4.4	**Have individuals been informed about the proposed use of their personal or special categories of personal data?**		Not always
	Privacy notices for all organisations note legal purposes. However, in some cases, data subjects may not be specifically notified about the use of their data where giving them this information would be impossible or involve disproportionate effort. Data subjects may not be specifically notified about the use of their data where doing so would prejudice the prevention or detection of crime, in these cases the DPA exemption under Schedule 2, Part 1, Para 2 (Crime and taxation: general) will apply.		
4.5	**How will you help to support the rights of individuals?**		
	Each organisation must have in place appropriate policies and processes to handle data subject requests made in line with data protection law, to ensure they are responded to within deadline and in an appropriate manner. Requests include; right of access, right to rectification, right to erasure, right to restrict processing, right to data portability, right to object and rights related to automated decision making including profiling.		

	If an individual successfully requests the erasure or limitation of use of their data (right to erasure, right to rectification, right to restrict processing, right to object), the party that has been informed by the data subject will communicate this to the other parties.	
4.6	**Are arrangements in place for recognising and responding to Subject Access Requests (SARs)?**	
	Each controller remains responsible for their own data subject requests and see 4.5 above.	
4.7	**Will the processing of data include automated individual decision-making, including profiling?**	NO
4.8	**Will individuals be asked for consent for their information to be processed/shared?** *If no, list the reason for not gaining consent e.g. relying on other lawful basis, consent is implied where it is informed.*	NO
	Consent is not the lawful basis for sharing under the data sharing agreement. The lawful basis is covered in detail in section 4.1 above. It is noted that when there is engagement with individuals, by support or other services, **after** the referral has been made, then this engagement is undertaken with the individual's consent. However this later stage processing is outside the scope of this agreement. Each party is responsible for managing consent where they use consent as the lawful basis condition.	
4.9	**As part of this work is the use of Cloud technology being considered either by your own organisation or a 3rd party supplier? If so please complete the embedded questionnaire.**	Existing technologies are used, no new systems.
4.10	**Where will the data will be stored?**	
	Provider systems are used. Paper storage is minimised; all storage is UK only. All parties will ensure that they have appropriate technical and organisational security measures in place to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. All personal data held by partner organisations electronically will be stored in a secure network area with password protected entry and appropriate back-up functionality. The systems will be auditable so that it is possible for any auditor to establish who has accessed the system. All laptops, computers, and any other portable devices will be encrypted. Any individual no longer required to have access will promptly have such access revoked by the line manager and Human Resources related to the relevant employer. Partner organisations will either be working toward ISO 27001, the International Standard for Information Security Management, or a similar standard of security.	

4.11	**Data Retention Period** *How long will the data be kept?*	
	Organisations are required by data protection legislation to document processing activities for personal data, such as what personal data is held, where it came from and with whom it has been shared. This Record of Processing Activity (ROPA) must include the retention period for the data. Information must not be retained for longer than necessary for the purpose for which it was obtained. Disposal or deletion of personal data once it is no longer required, must be done securely with appropriate safeguards, in accordance with that organisation's disposal policies.	
4.12	**Will this information be shared/processed outside the organisations listed above in question 3?** *If yes, describe who and why:*	Yes/No
	There will be a need to share with organisations outside London e.g. if a child is moved to a new area. This is covered by the legal basis. There may be a need to share with relevant intelligence agencies in some cases.	Yes

Step 5: Information Security Process

5.1	**Is there an ability to audit access to the information?**	Yes/No
	All DSPT certified provider systems have audit built in. All personal data held by partner organisations electronically will be stored in a secure network area with password protected entry and appropriate back-up functionality. The systems will be auditable so that it is possible for any auditor to establish who has accessed the system.	Yes
5.2	**How will access to information be controlled?**	
	This varies between providers, but RBAC control is required with password access as minimum.	
5.3	**What roles will have access to the information?** (list individuals or staff groups)	
Local authority staff with a business need (safeguarding professionals, Prevent staff, family services), health staff, counter-terrorism police, probation officers etc. Home Office officials can have access to the Prevent data too. Voluntary or third sector providers only very occasionally receive Prevent data, for example if it is relevant to the support they are providing to an individual.		
5.4	**What security and audit measures have been implemented to secure access to and limit use of personal data/special categories of personal data and/or business sensitive data?**	

Username and password	yes	Smartcard	**yes for**	key to locked filing cabinet/room	**yes**

				N H S		
	Secure 1x Token Access		Restricted access to Network Files			
	Other: *Provide a Description Below*:					
	All parties will ensure that they have appropriate technical and organisational security measures in place to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. All personal data held by partner organisations electronically will be stored in a secure network area with password protected entry and appropriate back-up functionality. The systems will be auditable so that it is possible for any auditor to establish who has accessed the system. All laptops, computers, and any other portable devices will be encrypted. Any individual no longer required to have access will promptly have such access revoked by the line manager and Human Resources related to the relevant employer. There is an expectation that partner organisations will either be working toward ISO 27001, the International Standard for Information Security Management, or a similar standard of security.					

5.5	**Is there a documented System Level Security Policy (SLSP) (**required for new systems**) or equivalent for the particular council for this project? If yes, please provide a link.**	Yes/No	Not required, no new system.
5.6	**Are there Business Continuity Plans (BCP) and Disaster Recovery Protocol for the proposed/existing system or process?**	Yes/No	Yes

5.7	**Is Mandatory Staff Training in place for the following?**	Yes/No	Dates
	● Data Collection:	Yes	Continuous
	● Use of the System or Service:	Yes	Continuous
	● Information Governance:	Yes	Continuous
5.8	**Are there any new or additional reporting requirements for this project?**	No	
	● What roles will be able to run reports?		
	N/A		
	● What roles will receive the report or where will it be published?		
	N/A		

	● Will the reports be in person-identifiable, pseudonymised or anonymised format?	
	N/A	
	● Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format?	
	N/A	
5.9	**Have any Information Governance risks been identified relating to this project?** (if Yes the final section will need to be completed)	**Yes/No** Yes

Step 6: Identify and Assess the Data Privacy Risks			
Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Note: risks here are data protection and privacy risks of this sharing ONLY. Signatories should have DPIAs for their own individual systems and methods, covering their local risks.			
Inherent privacy intrusion: The sharing of a large volume of personal, SCD and criminal data which may include details of 3rd party data subjects is intrinsically highly privacy intrusive. In some cases the data subject will be unaware of the sharing or the contents of what is being shared. There have been concerns that the referrals may in some cases have been overzealous and unwarranted leading to unnecessary intrusion. Compliance risk: data minimization, privacy intrusion Appropriate technical and organisational measures shall be taken. Corporate risk: Reputational risk. Loss of trust. Legal implications.	High	High	High
Lack of notice to data subjects: Decisions may be taken by partners to not notify data subjects about specific sharing of their personal data in situations where the data subjects should have been notified (i.e. where notifying them would not prejudice the purposes of the sharing or put someone at risk of harm). Compliance risk: fairness and transparency, right to be informed. Corporate risk: Reputational risk. Loss of trust.	High	Medium	Medium
Inaccuracy of data: Wider sharing of a large volume of sensitive personal data (both SCD and criminal offences data) increases the impact to the data subject if the data shared is inaccurate and may unfairly affect the data	High	High	High

subject's reputation, access to services or other economic or social opportunities. Compliance risk: data accuracy Corporate risk: Reputational risk. Loss of trust. Legal implications.			
Misuse of data: Wider sharing of a large volume of sensitive personal data (both SCD and criminal offences data) increases risk of disclosure to inappropriate persons or use of data in a manner incompatible with the data sharing agreement. Compliance risk: Appropriate technical and organisational measures shall be taken. Corporate risk: Reputational risk. Loss of trust. Legal implications.	Medium	High	Medium
Lack of controls: Voluntary sector organisation not having DSPT certification in some cases may lead to risks as full assurance is not in place	Medium	High	Medium
Loss of data in transfer: Personal data could be obtained and misused by third parties due to either poor information security or malicious acts. Compliance risk: Appropriate technical and organisational measures shall be taken. Corporate risk: Reputational risk. Loss of trust. Legal implications.	Medium	High	High
Further transfer of data: Inappropriate onward usage by third parties. The risks that recipients of information will reuse information provided under Prevent/Channel in inappropriate ways. Compliance risk: Personal data shall be obtained for one or more specified lawful purposes. Appropriate technical and organisational measures shall be taken. Personal data shall not be transferred outside the European Economic Area Corporate risk: Reputational risk. Loss of trust.	Medium	High	High

Step 7: Identify Measures to reduce risk				
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 6				
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
Privacy intrusion	Referrals are made under a defined framework and under particular conditions and where thresholds are met. Only relevant information is shared, although it is noted that only when a complete picture is known what is relevant may be ascertained. The sharing is undertaken to comply with legal duties- there are legal obligations which oblige sharing by the parties.	Reduced	Medium	Yes
Inaccuracy of data	The sharing is undertaken to comply with legal duties- there are legal obligations which oblige sharing by the parties. Only data which is necessary will be shared. Recipients must have clear processes in place for managing data quality and ensure that onward use of the data is lawful and in compliance with data protection requirements. Privacy and confidentiality around Prevent/Channel mean that reputational loss will be unlikely. Loss of access to services and opportunities is likely to be the result of the risks posed by the person to the public or a section of the public rather than by the sharing itself. Any restriction of service access must be based on law and be	Reduced	Medium	Yes

	proportionate. Partners will have policies and procedures to cover this and to ensure that service decisions are based on accurate, verified data.			
Lack of notice to data subjects	All Privacy notices cover this potential sharing, and where notice is not given this will be covered by one of the exemptions in data protection law that allows notice not to be given.	Reduced	Low	Yes
Misuse of data	Training and appropriate policy. Data minimisation, sharing only what is needed. Parties will only share relevant and necessary information, however it is known that what is relevant may only become apparent when viewed in conjunction with other information. In other words information which may not be obviously relevant may be shared as it may provide context to other information and thus become relevant to other parties. All receiving parties must comply with data protection law and have appropriate technical and organisational measures to guard against accidental or eliminate disclosures or other misuse	Reduced	Low	Yes
Lack of controls	Data minimisation, ensure only needed sharing is done. Appropriate policy document. Storage to be minimised	Reduced	Low	Yes

Loss of data in transfer	Appropriate technical and organisational measures in place and staff trained to follow their organisational policies and procedures for transfer and transport of personal data, with encrypted electronic documents expected to be used in most cases.	Reduced	Low	Yes
Further transfer of data	All agencies have an obligation to use the data shared in accordance with UK GDPR. Other uses may be undertaken if these are not incompatible with the original usage however there are exemptions which may apply for example for crime prevention and public safety. The risks here are of agencies using the shared information outwith those exemptions and purposes. Such uses would constitute a data breach. The agencies are all responsible bodies with DPOs and strong cultures of information governance and in light of that the risks are lowered.	Reduced	Low	Yes

Residual Risk	**Medium**

Step 8: Sign off and record outcomes		
Item	Name/date	Notes
Measures approved by:	[redacted], London Borough of Enfield; [redacted] LOTI and London Borough of Camden, [redacted] of London Borough Hammersmith and Fulham January 2022 and March 2022	Each Data Controller's DPO will need to assess these for their own organisation and ensure they accept them

Residual risks approved by:	[redacted], London Borough of Enfield; [redacted] LOTI and London Borough of Camden, [redacted] of London Borough Hammersmith and Fulham January 2022 and March 2022	Each Data Controller's DPO will need to assess these for their own organisation and ensure they accept them
DPO advice provided:	[redacted], London Borough of Enfield; [redacted] LOTI and London Borough of Camden, [redacted] of London Borough Hammersmith and Fulham January 2022 and March 2022	Each Data Controller's DPO will need to assess these for their own organisation and ensure they accept them
Summary of DPO advice: Whilst there are privacy intrusions to this sharing, they are considered to be proportionate to the aims of the statutory programme. Parties have policies and procedures in place to guard against unwarranted intrusion. The risks overall are classed as medium All DPO advice was incorporated and accepted. Note that local DPOs for each organisation need to produce their own DPIAs, this is a template.		
DPO advice accepted or overruled by:	N/A	If overruled, you must explain your reasons
Comments: N/A		
Comments:		
This DPIA will kept under review by:	The DPIA will be reviewed by the respective DPOs of each organisation when required	The DPO should also review ongoing compliance with DPIA