Prevent and Channel Panel Data Sharing Agreement

Contents

1. Introduction to the Data Sharing Agreement

This Data Sharing Agreement [DSA] documents how the parties to this agreement will share personal data about people at risk from radicalisation under the Prevent/Channel Panel programmes vulnerable adults and children for safeguarding purposes. The key agencies are listed in Appendix A, and the agreement is to be signed by all relevant parties, including local partners, voluntary sector, and any specialist organisations.

By signing this Agreement, the named agencies agree to accept the conditions set out in this document, according to their statutory and professional responsibilities, and agree to adhere to the procedures described.

This Agreement has been developed to:

- Define the specific purposes for which the signatory agencies have agreed to share information.
- Outline the Personal, Special Category and Criminal Data to be shared.
- Set out the lawful basis conditions under UK GDPR and Data Protection Act 2018 through which the information is shared, including reference to the Human Rights Act 1998 and the Common Law Duty of Confidentiality.
- Stipulate the roles and procedures that will support the processing/sharing of information between agencies.
- Describe how the rights of the data subject(s) will be protected as stipulated under the data protection legislation.
- Describe the security procedures necessary to ensure that compliance with responsibilities under data protection legislation and agency-specific security requirements.
- Describe how this arrangement will be monitored and reviewed.
- To illustrate the flow of information from referral through processing and outcome.

Parties to this agreement cannot amend or add appendices unless agreed as part of a formal review. It is expected that each party will have procedures, processes and policies sitting underneath this agreement, for their respective organisations. These will, for example, describe the specific processes for secure transfer of data.

1.1. Ownership of this agreement

This agreement was drafted by a working group of representatives of the Metropolitan Police, Probation, and local authorities. These professionals were specialists in safeguarding, Prevent and Channel, police procedures, Probation, information governance and law. The local authority representatives worked under the banner of the Information Governance for London Group (IGfL), to draft one agreement that would work for all boroughs, the Probation Service, the City of London Police, British Transport Police, and all Metropolitan Police BCUs across London. The aim is to reduce the number of versions of sharing agreements that historically differed between boroughs, partly to reduce the burden on pan-London organisations that must have agreements with multiple boroughs. For ease of use throughout the document the term “Police” will refer to the Metropolitan Police Service, British Transport Police, and the City of London Police.

IGfL, a group of information and security professionals at London boroughs, assisted with coordination of this agreement, but the responsibilities within it, and compliance with data protection legislation, remain with the listed data controllers.

1.2. Responsibilities of parties involved

The parties are registered Data Controllers under the Data Protection Act. A list of expected types of signatories is at Appendix A. Signatories are identified as those who have signed this agreement. Sign up will either be via the Information Sharing Gateway (councils, police, probation, some other signatories) or via soft copy agreement. Local agencies may be signed up by local processes with lists of signatories provided to IGfL as a central store.

All parties confirm that they comply with data protection legislation by:

- having a lawful basis for processing and sharing personal data.
- ensuring data quality.
- storing and sharing information securely, with access management controls.
- having policies and procedures for compliance with data protection legislation including for managing data subject rights & complaints, identifying and managing data breaches/incidents and retention & disposal.
- ensuring that mandatory training is undertaken regularly by their employees to ensure they are clear and up to date on their responsibilities. Every individual must uphold the principles of this agreement and overarching confidentiality, and seek advice from the relevant Data Protection Officer when necessary.
- undertaking appropriate data protection due diligence checks with any contractors/data processors they employ, and ensuring that a written agreement is in place with each data processor, and that all data processors will be bound by this agreement.
- having written processes for the processing of data to ensure employees use and share personal data in line with data protection law, the data protection principles, and this agreement.

Organisations and their staff must consult the organisation's Data Protection Officer/Information Governance Manager and/or Caldicott Guardian if they are unsure at any point in the processing and sharing of personal data.

1.3. Confidentiality and vetting

Each Partner must ensure that there are appropriate written contracts or agreements with employees, agency staff, volunteers etc. These must include requirements to ensure compliance with policies which include confidentiality.

Each Partner must ensure that suitable vetting has taken place. This may be through standard employee checks (BPSS or equivalent), DBS, Security Vetting or Counter Terrorist Check [CTC].

Where agencies not party to the DSA attend meetings for example, they may be asked to sign or verbally agree appropriate confidentiality statements. Other measures are covered in 2.7 below.

1.4. Assessment and review

A review of this data sharing agreement will take place after 6 months and then annually, unless otherwise agreed by the organisations' Data Protection Officers. The aim of the review will be to ensure the purposes are still relevant, the scope has not slipped, the benefits to the data subjects and organisations are being realised, and the procedures followed for information security are effective.

Changes in legislation and developments in the areas of public sector data sharing will be considered as and when they arise, as will any changes to the signatory parties.

The working group who drafted this agreement strongly recommends that a working group approach is used for any reviews, as this was a successful way to achieve pan-London and cross-specialism consensus to one sharing agreement.

1.5. Termination of agreement

In the event of termination of this agreement each party may continue to hold information originating from other parties for which they are a Data Controller.

1.6. Outside of this agreement

There are multiple other information sharing arrangements either live or currently in draft, that form part of the duties of the parties and may involve similar data for often similar overall purposes, like safeguarding and preventing crime. A non-exclusive list is below.

Area of work	Description
ASB	The sharing of data regarding anti-social behaviour and related enforcement
MAPPA - Multi-Agency Public Protection Arrangements.	Information sharing between probation, police, councils and other agencies as mandated under MAPPA for the most serious risk posing offenders
YOS	Sharing of data between councils, police and probation for specific Youth offending service purposes
Rescue & Response (County Lines)	The exploitation of persons to sell and move drugs between areas, commonly known as "county lines" is a major element of modern exploitation of young persons and in some cases, modern slavery.
IOM	Integrated Offender Management (IOM) tackles the most prolific reoffenders and those who commit offences deemed to have the most significant impact on the local community.

MAS/MASH	The multi-agency safeguarding DSA covers children's safeguarding, well-being, and MACE sharing.
Licensing	This covers sharing for all licensing including alcohol, gambling, special treatments and sexual entertainment venues, and various other areas such as pet shops and highways licenses
Gangs/Serious Youth Violence (SYV)	The gang and serious youth violence projects are part of specific police-led initiatives. There are 2 agreements: one councils/police, and one council to council.
Residual crime	A local BCU signed DSA to cover lower-level crime not covered in other DSAs such as caution registers, nuisance, persons posing a risk to themselves, and other criminal issues.
Domestic Abuse Multi-Agency Risk Assessment Conference (MARAC)	Domestic abuse and violence against women and girls have complex roots, and as such commonly involve police, social care, health, voluntary and faith organisations in case management.
Adult Safeguarding	Safeguarding of adults vulnerable to physical, emotional, sexual, psychological, or financial abuse, and at risk of becoming victims of scams, cuckooing and such like
Troubled Families/Supporting Families	Troubled families was an early intervention programme created by central government to support families to reduce anti-social and criminal behaviour.
CCTV	The sharing between councils and police of CCTV footage, whether live feed or recorded, and from any type of device including cameras, drones and vehicle CCTV
Environmental Crime	There are two agreements, one between councils and the Environment Agency covering crime that the EA handles, the other is between councils for a wider range of environmental related crime such as fly-tipping, dog fouling etc
Trading Standards	This covers information sharing between the police and National Trading Standards London Region, and between the police and local councils for the whole range of trading

	standards related activity such as scams, rogue traders etc

2. Purpose and Benefits

Research and experience have demonstrated the importance of information sharing across professional boundaries, effective information sharing is key to the delivery of Prevent and Channel panels, so that partners are able to take appropriately informed action.

Information viewed alone or in silos may not give the full picture or identify the true risk.

All the information from various agencies needs to be available and accessible in one place; to keep vulnerable adults and children safe and assist signatories to this Agreement in discharging their legal obligations and public duties. However, the information sharing must be assessed on a case-by-case basis and is governed by legislation.

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.

Some information sharing does not use personal data and is under the duties outlined in the Crime and Disorder Prescribed Descriptions Regulations 2007 (to have in place arrangements for the sharing of information between responsible authorities).

Channel Panel

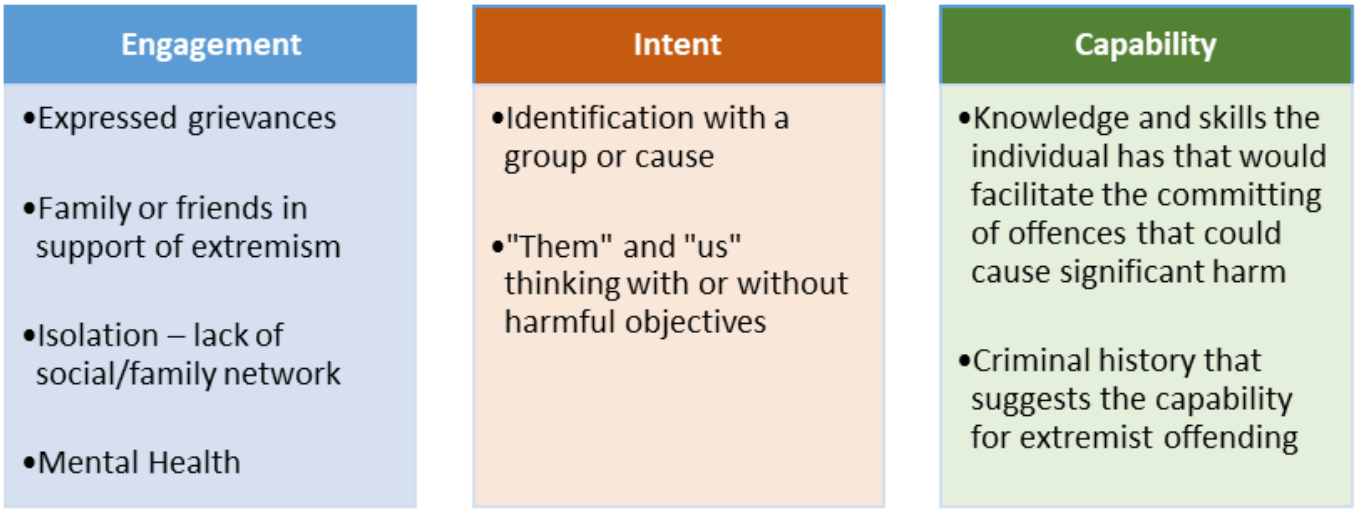
The Channel Panel is a multi-agency safeguarding board in respect of Prevent. The potential partners to Channel are local authority safeguarding services and counter-terrorism police. Channel is about ensuring that children and vulnerable adults of any faith, ethnicity or background receive support before 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 list of potential partners at Channel is Local Authorities services such as:

- Prevent
- Children's Social care
- Adult's Social care
- Early Help
- Multi Agency Safeguarding Hub (MASH)
- Education
- Housing
- Family Justice Centre (FJC)

- Metropolitan Police Service, British Transport Police, City of London Police
  - Frontline Policing (eg local Police)
  - Counter Terrorism Command (eg SO15)

- Probation Service
- Immigration
- Clinical Commissioning Group (NHS)
- Mental Health Trust Safeguarding lead
- NHS Acute Trust Safeguarding lead
- Home Office
- Intervention Providers (commissioned by the Home Office)
- HM Courts and Tribunals Service
- Children and Family Court Advisory and Support Service (CaFCASS)
- Children and Adolescent Mental Health Services (CAMHS)
- Education providers.

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.

For example, understanding a data subject's ethnic origin, political opinions and religious / philosophical beliefs will enable the panel to assess whether the ideas, beliefs and language used by a data subject are extremist in nature and where their influences may have occurred. Similarly the sharing of data including health and sex life / orientation will support the panel in making informed decisions about the best approach to safeguard the individual (e.g. the impact of substance misuse on their vulnerability).

2.1. Supporting vulnerable individuals

Prevent requires a multi-agency approach to protect people at risk from radicalisation. When vulnerable individuals are identified the police will undertake the following:

- In partnership with other agencies including the local authority, consider appropriate interventions, including the Channel programme, to support vulnerable individuals;
- Work in partnership with and support Channel Panels chaired by local authorities to coordinate Channel partners and Channel actions;
- Support existing and identify potential new intervention providers.

2.2. Wider Community Safety work

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.

2.3. Benefits

The benefits of this DSA are to:

- Allow the agencies to better comply with their duties around Prevent And Channel Panels

- Cover the sharing of information about those at risk of radicalisation
- Remove barriers to effective information sharing.
- Sets parameters for sharing personal data and clearly identifies the responsibilities of organisations.
- Identify the correct lawful basis to share personal information.
- Ensure information is shared whenever there is a requirement to do so.
- Enables authorities to share data on performance, quality assurance, learning and impact analysis.
- Raises awareness amongst all agencies of the key issues relating to information sharing and gives confidence in the process of sharing information with others.
- More effective multidisciplinary working between the Channel and Prevent.
- Enable the Channel Panel and Prevent to provide a more holistic support package for individuals at risk of radicalisation.
- Enable the Channel Panel and Prevent to better risk assess subjects who are at risk of being radicalised.

2.4. Principles of information sharing

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.

To share information, a lawful basis for doing so must be identified. This may come from legislation or from statutory guidance such Counter-Terrorism and Security Act 2015

The sharing of personal data must comply with both the GDPR Principles and the Caldicott Principles, listed at Appendix B. Together, those principles lead to a series of questions and considerations to be answered before sharing takes place. These are listed as an Information Sharing Checklist in Appendix D: Information Sharing Checklist.

2.5. Lawful Basis

The sharing of information must comply with the law relating to confidentiality, data protection and human rights. Having a legitimate purpose for sharing information is an important part of meeting those legal requirements. This is a complex area and each Partner must take their own decisions and seek advice from their organisation's Data Protection Officer/Information Governance Manager and/or Caldicott Guardian.

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 the lawful basis for processing set out in 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. The laws given at Appendix C – Applicable legislation provide for each party a legal basis under section 8 – the specifics are noted in the appendix. 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.

Article 9 (2) – Special Category Personal 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

(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 – Criminal Offence Data Processing

Use of Article 10 GDPR 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 (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 this agreement 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 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.

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.*

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.

2.6. Consent

The parties will often work collaboratively with data subjects and aim for agreement with them on the actions to be taken. However, it is recognised that this is different to using consent (Article 6 (a)) or explicit consent (Article 9 (a)) as the lawful basis conditions used for processing under this agreement.

Consent is not the lawful basis public sector organisations use for sharing information with each other under this agreement. Information shared between organisations under this data sharing agreement will use the lawful basis set out in 2.5 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.

2.7. Proportionality and necessity

Proportionality and necessity are factors to be taken into consideration when deciding whether to share personal information. In making the decision, employees must weigh up what might happen as a result of the information being shared against what might happen if it is not and apply their professional judgement. The relevant legal duties and powers of the agencies need to be considered. Factors will include those relevant to individual data subjects but also to society more generally.

Data Controllers are expected to justify that they believed sharing was necessary for one of the following criteria:

- necessary for the purposes of preventing or detecting crime
- required or authorised by an enactment, by a rule of law or by the order of a court or tribunal
- in the particular circumstances, was justified as being in the public interest.

Or that they acted in the reasonable belief that:

- the person had a legal right to do the obtaining, disclosing, procuring or retaining
- the person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it

Measures to assist proportionality include:

- All panel attendees have to sign a confidentiality agreement
- Panel attendees only attend with the panel chair's permission.
- Cases are time managed throughout the Channel panel meeting. Referring agencies (e.g. schools) only attend for their specific case to answer panel questions and receive actions and then leave the meeting.
- Channel panel meeting minutes and notes can be pseudonymised although it should be noted that pseudonymised records may still contain Personal Data or data that is re-identifiable when combined with other data sources.
- Limited electronic and hard copy are circulated to members to minimise the risk of data breaches.
- Channel notes and minutes are held securely on the relevant Council system with Role Based Access Control.

2.8. Other relevant legislation

The actual disclosure of any personal data to achieve these objectives must also be conducted within the framework of the Human Rights Act 1998 (HRA) and the Common Law Duty of Confidence. Caldicott

Principles also apply to all information sharing and they are listed in Appendix B: Data Protection & Caldicott Principles.

2.9. Common Law Duty of Confidence

Much of the police information to be shared will not have been obtained under a duty of confidence as it is legitimately assumed that data subjects will understand that police will act appropriately with regards to the information for the purposes of preventing harm to or promoting the welfare of children.

However, for the police, as a safeguard before any information is passed on, it will undergo an assessment check against criteria (included in relevant Standard Operating Procedures) by the Public Protection Desk (PPD). Whilst still applying proportionality and necessity to the decision, the protection of persons at risk would clearly fulfil a public interest test when passing the information to a partner agency whose work with the police would facilitate this aim.

Information held by other agencies that will be shared in the Prevent process may have been gathered where a duty of confidence is owed. Duty of confidence is not an absolute bar to disclosure as information can be shared where consent has been provided or where there is a strong enough public interest to do so. When overriding the duty of confidentiality, the parties may seek the views of the organisation who hold the duty of confidentiality and consider their views in relation to breaching confidentiality. The organisation may wish to seek legal advice if time permits.

2.10. Freedom of Information

The Freedom of Information Act 2000 gives all individuals the right to access official information held by a public authority (the Environmental Information Regulations 2004 also allow access to data. For ease of drafting, FOI is used to cover both legislation). Limited exemptions may apply and all public authorities must ensure they have recognised procedures in place for administering requests of this nature.

It is encouraged that all parties proactively publish this document. It may also be disclosed to the public under FOI. All requests for FOI will be directed through the relevant organisations' FOI processes. Each party will seek advice/opinion from the other parties where there is concern about that information being released and any impact it is likely to have. The final decision to disclose or not will lie with the party who holds the information (Data Controller). In order to ensure that the authority in receipt of the FOIA request is able to respond within the statutory deadline, any request for assistance or information made to partner authorities should be made and processed within two working days, and any data exchange completed within seven working days.

3. Individuals

Organisations processing personal data are required to begin with the ethos of Data Protection by Design and Default (also known as Privacy by Design (PbD)). This means that we must consider and uphold the privacy of an individual's data before we begin and throughout the processing taking place.

Each party agrees that they have undertaken a DPIA (Data Protection Impact Assessment), where they feel the processing meets the legislative criteria for a DPIA.

3.1. Right to be informed – Privacy notices

Where personal data is created or received by one of the parties, they are responsible, as required by law, for making the data subject(s) aware within a reasonable time frame that the organisation holds the data, what they will do with it, how long they will keep it, and who they will share it with (such as under this DSA). This is normally done through a privacy notice, whether written or verbal. Organisations agree that they will adhere to the transparency requirements of the UK GDPR and will issue appropriate privacy notices which inform the data subject that the information will be shared with the parties under this agreement.

In some cases, it may not be appropriate to let a person know that information about them is being processed and shared. Consideration should be given to whether notifying the individual may place someone at risk or prejudice a police or counter terrorism investigation. In these circumstances, the parties need not inform individuals that the information is being processed/shared; but should record their reasons for sharing information without making the individual aware.

3.2. Data subject rights requests and complaints

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 where relevant and appropriate. In each case each party is responsible for securely disposing of such information or limiting its processing.

Each party must have clear, fair and objective complaint procedures. Any complaints from individuals how their data is being processed or shared will be handled under the policy and processes of the organisation concerned.

All parties accept that data should not be disclosed that would compromise an investigation or proceedings. If a SAR is received that covers information shared under this Agreement then the party receiving the SAR will consult with the partner who provided the data to avoid inappropriate disclosure.

3.3. Data subjects

There is a breadth of data subjects whose data is shared under this agreement. The data subjects are all individuals who may be vulnerable to being radicalised.

People who have been referred to the Channel/Prevent programme which can be individuals of any sex, gender identity, religion, ethnic origin, or race and can be children or adults. It is however,

- unusual to receive a referral in isolation about children under the age of 7 due to the lack of mental capacity of the child to form an ideological perspective.

- However, children under the age of 7 are unlikely to be able to critically think which may result in them to being more susceptible to extremist views of those around them.The majority of referrals to Channel are for vulnerable individuals (both children and adults)

Parties to this agreement are in positions of power over data subjects and data subjects have little or no control over why and how their data is processed.

4. Data

The personal data and its processing involved in these workstreams is extensive, highly sensitive and at times intrusive. There is a high volume of data and data subjects.

Anonymisation or pseudonymisation will rarely be possible because of the way the work focuses on individuals, although any statutory returns, workforce planning and management reports should be anonymised if possible.

Information will include:

- **Personal, special category and criminal data**
- **Personal, special category and criminal data** for law enforcement purposes, including data defined as **sensitive data** for the competent authorities for law enforcement purposes
- **Aggregated (anonymised or pseudonymised) data** reporting
- **Personal and anonymised data** required for statutory returns.

4.1. The data to be shared

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.

- 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;
- youth offending information: offences (including alleged offences), criminal proceedings, convictions and sentences;
- medical history;

- mental health history
- 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 category information can include:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs, and 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
- data concerning health,
- sex life / sexual orientation

The MPS Process for gathering the relevant information

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

The MPS shared information will be sent to the Prevent lead via either secure email or at Channel Panel meetings where the recipients of the MPS data will be the Prevent lead and the Channel Panel Chair. The Chair will become the secondary point of contact, in the absence of the Prevent Lead.

A record of the personal information disclosed to a partner agency will be created on CRIMINT PLUS by the MPS disclosing officer at the time the information is supplied (or as soon as possible thereafter) unless this disclosure record has already been made on another MPS systems (e.g. ViSOR, MERLIN or CRIS) relating to that system. For clarity, where personal information has been shared that is only held on CRIMINT PLUS the disclosure record must be made on CRIMINT PLUS. Such records should include what was shared or not, and the reason for the decision.

The City of London Police and British Transport Police have equivalent processes and procedures using their own case management systems.

4.2. Deceased persons

It is noted that the sharing may involve data of deceased persons. This data will not be covered by data protection legislation but will still require due regard to the common law duty of confidentiality and the Human Rights Act.

4.3. Confidential information

In this agreement, we refer to personal data, as defined by data protection legislation. However, the word 'confidential' may be used by individuals and practitioners to describe information and can mean different things to different people.

Confidential can mean:

- Personal and special category data as defined by data protection legislation
- Patient Identifiable Information (PII) or 'personal confidential information'; both terms most commonly used in health settings
- Information which is not already lawfully in the public domain or readily available from another public source

- Information that has been provided in circumstances where the person giving the information could reasonably expect that it would not be shared with others.

4.4. Storing and handling information securely

Information must be stored and shared lawfully and securely. Special category data may need a higher level of security. The employee/organisation sharing the information must choose the most appropriate secure method of transfer and be responsible for its safe delivery.

Electronic records:

Organisations may have different electronic methods for storing and sharing information securely. Some have local restrictions which block access to information shared using specific tools.

Parties must make sure the chosen method is suitably secure and that access is only provided to those who need it, and only to the data needed.

Unencrypted email (i.e. sent in plain text over the public internet) must not be used to share information under this DSA.

Sharing methods that may be appropriate include:

- **Email encryption tools** where the email and attachments are encrypted from named sender to named recipient (e.g. Microsoft 365 Message Encryption; Egress Protect)
- **Encryption via Transport Layer Security** (TLS) where the email and attachments are encrypted in transit over the internet. Both the sender and recipient email domains must have TLS enabled. This can be checked using https://www.checktls.com/
- **Secure corporately managed data repository and sharing platforms** (e.g. MS Teams; Google Docs)
- **Secure group email services** (e.g. CJSM: https://cjsm.justice.gov.uk/index.html)
- **Secure File Transfer Protocols**
- **Virtual Private Networks**

The above are examples, get advice from your organisation's information security or IT teams on secure methods of sharing available at your organisation and document these in the organisation's process documents.

Phone/virtual meetings/face-to-face meetings:

Information may be shared over the phone, in a virtual meeting, or at face to face meetings. Meeting attendance and distribution of content, e.g. meeting minutes or recordings, must be limited to those with a need to know.

Sharing by telephone should be avoided unless the requirement is urgent and email is not practicable.

Individuals should be aware of their surroundings and the presence of other individuals or voice recognition or 'Internet of Things' devices (e.g. virtual assistant apps like Alexa, Cortana, SIRI) to ensure they aren't overheard by those that should not have access to the information discussed.

Paper records:

Printed paper records must always be kept to a minimum and kept secure whether in the office, home or during transit. Organisations must adopt an appropriate policy surrounding the use and transfer of paper records. Appropriate security methods must be applied when storing or disposing of paper records.

4.5. Access controls and security

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.

4.6. Outside UK processing

Parties are responsible for ensuring that if information is processed or shared outside the UK, that suitable written agreements are in place, and that appropriate due diligence has been completed for the transfer of data, that appropriate safeguards are in place and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. These are for example, a legally binding and enforceable instrument between public authorities or bodies, binding corporate rules, and/or standard data protection contractual clauses. Due to sensitivities surrounding Prevent/Channel, if it is proposed that information will be processed outside the UK then the originating Data Controller will be informed in advance and appropriate arrangements agreed before any such outside UK processing commences.

4.7. Data quality

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.

4.8. Data breaches/incidents

All parties must have a clear policy and procedure regarding the reporting and handling of data protection breaches or data loss incidents. This must include assessing the level of risk to the data subject(s), as well as to make a decision on notifying the ICO within the statutory time frame of 72 hours. This complies with Articles 33 and 34 of UK GDPR, and Section 67 and 68 of the DPA 2018 for personal data processed for law enforcement purposes.

If the incident may impact the processing of another party to this agreement, all relevant parties should be informed, usually within 24 hours of the breach being identified, and appropriate coordination of the incident must take place. The decision to report the incident will lie with the Data Controller(s) of the information concerned. The parties agree to provide all reasonable and necessary assistance at their own expense to each other to facilitate the handling of any personal data breach in an expeditious and compliant manner.

It is confirmed that security breaches (including misuse or unauthorised disclosure) are covered by the partner's internal disciplinary procedures. If misuse is found there should be a mechanism to facilitate an investigation, including initiating criminal proceedings where necessary.

4.9. Retention & Disposal

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.

5. Signatures

For the Metropolitan Police:

Name

Rank

Date

All other parties will sign electronically on the Information Sharing Gateway

Version control	
Document production date	March 2022
Document currency	1.0

6. Appendix A: Key parties to this agreement

Organisation	Duties
London Borough Councils	● Co-ordinates, gathers, processes and shares local authority information relevant to Public Protection and shares this information with the Police. ● Supports assessments of risk and vulnerability. ● Assists in the implementation of agreed interventions.
Metropolitan Police Service, British Transport Police, and City of London Police	● Co-ordinates, gathers, processes, risk assesses and shares police information relevant to Public Protection. ● Supports assessments of risk and vulnerability
The Home Office	● The Home Office oversees Prevent activity in all local authorities – everyone is subject to the Prevent duty, though the 'priority areas' receive funding for actual roles, i.e. the Prevent Coordinator and occasionally additional staff. In other local authorities there is a 'Prevent lead', which is only one part of their role and they are normally a safeguarding professional. ● Section 36 of the CT&S Act places a duty on local authorities to ensure that a Channel panel is in place for their area. The local authority should ensure these meetings are serviced and administrated appropriately. ● Section 37(5) of the CT&S Act requires Channel panels to be chaired by the responsible local authority (that is, the authority responsible for ensuring a panel is in place). Members of the panel must include the responsible local authority and the police for the relevant local authority area under section 37(1) of the CT&S Act, and they have principal responsibility for Channel in their areas.
Probation Service	● Co-ordinates, gathers, processes, risk assesses and shares Probation information relevant to adult offenders. ● Supports assessments of risk & vulnerability
Local health partner	● Co-ordinates, gathers, processes, risk assesses and shares health information relevant to the child or young person ● Supports assessment of risk and vulnerability ● Identifies opportunities for early help, joint assessments and interventions
Local CCG	Co-ordinates, gathers, processes, risk assesses and shares health information relevant to midwifery, ante-natal, health visiting, school nursing, specialist health services, GPs Supports assessments of risk & vulnerability

Department for Work & Pensions (inc Job Centre Plus)	Co-ordinates, gathers, processes, risk assesses and shares information regarding families in receipt of benefits Advises on eligibility for accessing benefits Supports assessments of risk and vulnerability.
London Ambulance Service	Gathers and shares information relating to the treatment, transportation and relevant medical information of individuals. Provides emergency transportation, urgent care and support to the health service Supports assessments of risk and vulnerability
Local substance misuse partner	Co-ordinates, gathers, processes, risk assesses and shares drug and alcohol service information relevant to adults and young people Supports assessment of risk and vulnerability Identifies opportunities for early help, joint assessments and interventions
Local housing partner if ALMO	Co-ordinates, gathers, processes, risk assesses and shares housing applicants, tenant and leaseholder's information relevant to children and adults Advises on eligibility for accessing accommodation under the homeless legislation and Housing Allocation Scheme
Local voluntary groups	Co-ordinates, gathers, processes, risk assesses and shares information relevant to adults and young people service users Supports assessment of risk and vulnerability Identifies opportunities for early help, joint assessments and interventions

7. Appendix B: Data Protection & Caldicott Principles

The Principles as described in Article 5 of the General Data Protection Regulation – Accountability is an overarching principle of the legislation.

1) Fair & Lawful
processed lawfully, fairly and in a transparent manner in relation to the data subject

2) Purpose limitation
collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

3) Data minimisation
adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4) Accuracy
accurate and, where necessary, kept up to date; Inaccurate data must be erased or rectified without delay

5) Storage limitation
kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

6) Integrity & Confidentiality
secured through appropriate technical or organisational measures, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

7) Accountability
processed by organisations that take responsibility for the personal data, with appropriate measures and records in place to demonstrate compliance.

The Caldicott Principles

Principle 1
Justify the purpose(s) for using confidential information
Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2
Use confidential information only when it is necessary
Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3
Use the minimum necessary confidential information
Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4
Access to confidential information should be on a strict need -to-know basis
Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5
Everyone with access to confidential information should be aware of their responsibilities
Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6
Comply with the law
Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7
The duty to share information for individual care is as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8
Inform patients and service users about how their confidential information is used
A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. As a minimum, this should include providing accessible, relevant and appropriate information. In some cases, greater engagement will be required.

8. Appendix C: Applicable legislation

Note that all legislation can be found at www.legislation.gov.uk

Legislation	Main purpose of Legislation
Counter-Terrorism and Security Act 2015 and Counter Terrorism and Border Security Act 2019	Section 26 of the Counter-Terrorism and Security Act 2015 (the Act) places a duty on certain bodies ("specified authorities" listed in Schedule 6 to the Act), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". (Prevent Duty Guidance for England and Wales 2015). Section 36 provides for processing of personal data necessary for the purposes of the various Channel duties set out in the Act, the purpose being to put in place a local panel to carry out assessments and provide support for persons vulnerable to being drawn into terrorism. Section 38 (amended by CTBSA2019) 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. Section 20 CTBSA 2019 amends the 2015 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.
The Localism Act 2011	General powers for Local Government to act as in any manner they believe suitable for the purposes of promoting economic, social and environmental well-being within their boundaries. Gives a legal basis under Section 8 of the DPA for this use. However, as a general power it can be challenged, and an additional legal basis is preferred.
The Education Act 2002	The Education Act 2002 puts a duty on schools to exercise their functions with a view to safeguarding and promoting the welfare of children. Prevent is covered by the Education Act 2002, even though schools and colleges are subject to the Prevent duty under Section 26 of the Counter-Terrorism and Security Act 2015. 'Keeping Children Safe in Education' (KCSIE) which is statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002. KCSIE clearly states: protecting children from the risk of radicalisation 'should be a part of a schools' or colleges' safeguarding approach'. It also says: 'The Prevent duty should be seen as part of schools' and colleges'

Legislation	Main purpose of Legislation
	wider safeguarding obligations'. Gives a legal basis under Section 8 of the DPA for this use.
The Children Act 2004	The Children Act 2004, as amended places duties on the police, clinical commissioning groups and the local authority to make arrangements to work together, and with other partners locally, to safeguard and promote the welfare of all children in their area. Provides a general safeguarding and welfare power giving a legal basis under Section 8 of the DPA.
The Criminal Justice Act 2003	This act amended a wide range of provisions in the PACE act and provided new regulations on offence management, disclosure and trials. The regulation clarifies the process and procedure for police and their legal basis for use.
The Police and Criminal Evidence Act 1984	This act makes the specific provision for the secretary of state to issue codes of practice to police with statutory effects. It provides the basis for many of the police actions in respect of matters relating to safeguarding and other matters, and as such provides their legal basis for use.
The Children & Social Work Act 2017	Safeguarding partners, as defined under the Children Act 2004 (and amended by the Children and Social Work Act, 2017), have a statutory duty to work with relevant appropriate agencies within their locality to safeguard and protect children.
The Mental Capacity Act 2005	Where the capacity of an individual to make a specific decision is brought into question, the Mental Capacity Act 2005 provides safeguards within a statutory framework to protect the rights of those who may not be able to make their own decisions.
The Crime and Disorder Act 1998	s115 provides agencies and professionals with a permissive power (but not a legal duty) to disclose personal information lawfully 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 a power to do so. Also places a duty on councils to formulate a strategy to reduce crime and disorder in their area and to work with police authorities to do this.

Legislation	Main purpose of Legislation
Section 14 Offender Management Act 2007 (Disclosure for Offender Management Purposes	Disclosure for Offender Management Purposes, Section 14 sets out the powers of certain bodies to share data for specified purposes which include • The probation purposes • The performance of the functions relating to prisons or prisoners (inc young offender institutions and secure training centres, together with those persons detained within them); • Any other purpose connected with the management of offenders (including the development or assessment of policies relating to matters connected with the management of offenders).

The Care Act 2014	The Care Act 2014 is covered under the Channel Duty Guidance and stipulates local authorities are required to have Safeguarding Adults Boards in their area. These boards provide strategic leadership to the work of the local authority and partner agencies on the development of policy and practice in relation to safeguarding adults at risk.

Guidance	Main Purpose
Department for Education Information Sharing for Practitioners 2018	Non-statutory advice to support practitioners in the decisions they take to share information, which reduces the risk of harm to children and young people and promotes their well-being.
NHSE Safeguarding Vulnerable People in the NHS – Accountability and Assurance Framework 2015	Sets out the safeguarding roles, duties and responsibilities of all organisations commissioning NHS healthcare. Aims to aims to: • Identify and clarify how relationships between health and other systems work at both strategic and operational levels to safeguard children, young people and adults at risk of abuse or neglect. • Clearly set out the legal framework for safeguarding as it relates to the various NHS organisations in order to support them in discharging their statutory requirements to safeguard children and adults. This provides the policy document required for the safeguarding purposes under Schedule 1 Part 2, para 18 of the DPA for the NHS bodies.

London Child Protection Procedures 2022	Sets out the procedures which all London agencies, groups and individuals must follow in identifying, raising and responding to welfare concerns when coming into contact with or receiving information about children unborn to 18th birthday. This provides the policy document required for the safeguarding purposes under Schedule 1 Part 2, para 18 of the DPA for various London bodies.
Working Together to Safeguard Children 2018	Practical implementation guidance for councils, partner organisations and agencies of their safeguarding and welfare promotion duties for children in their area under . Children Acts 1989 and 2004. This provides the policy document required for the safeguarding purposes under Schedule 1 Part 2, para 18 of the DPA for national bodies

9. Appendix D: Information Sharing Checklist

The following questions must be considered when deciding whether to share information.

- Whose information is this?
- Is there a lawful basis to share the information? Justify the purpose and identify relevant legislation that applies.
- Can information be pseudonymised or anonymised ahead of sharing?
- How have individuals been informed that the information will be shared eg via a privacy notice? Will they have the expectation that their information will be shared? **Consider whether notifying the individual of the sharing may place someone at risk or prejudice a police or safeguarding investigation.**
- Have any requests not to share been received and considered?
- How much information is it necessary to share in this situation?
- Is the information accurate and up to date? Has the difference between fact and opinion been stated?
- Is access to the information limited to only those who need it? Is it being given to the right person?
- Is the information being shared in a secure way?
- Has the decision to share or not share, and the rationale for the decision, been recorded?