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)
0.1	**Draft - initial draft**	**10/05/2021**	**Anthea Ferguson**
0.2	**Draft – incorporated work from LB Hillingdon**	**13/05/2021**	**Anthea Ferguson**
0.3	**Draft- review and update**	**15/3/22**	**Sarah Laws**
0.4	**Draft- review and finalise**	**23/3/22**	**Anthea Ferguson and Sarah Laws**

Project / Work Stream Name	**Adults Safeguarding pan-London Data Sharing Agreement**
Overview: **(Summary of the project/work stream)**	Research and experience has demonstrated the importance of information sharing across professional boundaries to safeguard adults at risk of abuse, harm or neglect. The Care Act 2014 (Section 6) places duties on the local authority and its partners to cooperate in the exercise of their functions relevant to care and support including those to protect adults. This is reinforced by the statutory guidance for Care Act 2014 The London Adult Safeguarding Data/Information Sharing Agreement (DSA/ISA) will formalise the information sharing arrangements between the organisations involved in adult safeguarding to ensure that all parties are clear on the processes and principles for sharing information between each other, with other professionals, and the local Safeguarding Adults Board (SAB). This will enable decision makers to: ● have a full information picture of an individual and their circumstances so they can take the best safeguarding decisions to ensure timely, necessary, and proportionate interventions to safeguard those at risk. ● discharge their obligations under the Care Act 2014 and other legislation. The DSA/ISA covers the sharing of information in a wide range of adult safeguarding areas including cuckooing, financial abuse, domestic abuse not covered by other DSAs/ISAs, cases of hoarding, modern slavery, servitude and other areas of adult safeguarding concern. It includes adults aged 18-25 who, when aged under 18, were at risk from or receiving support for reasons related to MACE - Multi-Agency Child Exploitation, issues concerning the sexual and/or criminal exploitation of children, including 'County Lines' and missing children. It is noted that some areas of adult safeguarding that may appear to be omitted from this DSA/ISA will already be covered already in other DSAs such as ASB and MAPPA and reference should be made to them where appropriate

Implementation Date:	sharing ongoing, DSA from 1/4/22
Environmental Scan 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.	Adults Safeguarding work is carried out nationally and is a legal obligation. This is a renewal of previous fragmented agreements, intended to cover all-London. It has been produced with the input of representatives from: - London Boroughs' Safeguarding, Adult Social Care and Community Safety teams, - the Metropolitan Police, - the Probation service, - the Information Governance for London forum (a group of IG professionals from across all London Boroughs)

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 organisatio ns	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
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 EEA?	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.**

<table>
<tr><th colspan="11">Step 2: Identify the need for a DPIA</th></tr>
<tr><td>2.1</td><td colspan="8">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?</td><td colspan="2">New/Changed
Changed</td></tr>
<tr><td>2.2</td><td colspan="10">What data will be processed/shared/viewed?</td></tr>
<tr><td></td><td colspan="10"><u>Personal Data</u></td></tr>
<tr><td></td><td>Forename</td><td>yes</td><td>Surname</td><td>yes</td><td>Date of Birth</td><td>yes</td><td>Age</td><td>yes</td><td>Gender</td><td>yes</td></tr>
<tr><td></td><td>Address</td><td>yes</td><td>Postal address</td><td>yes</td><td>Employment records</td><td>yes</td><td>Email address</td><td>yes</td><td>Postcode</td><td>yes</td></tr>
<tr><td></td><td>Other unique identifier (please specify)</td><td>yes eg case management system ref number</td><td>Telephone number</td><td>yes</td><td>Driving licence number</td><td></td><td>NHS No</td><td>yes</td><td>Hospital ID no</td><td></td></tr>
<tr><td></td><td>Other data (Please state):</td><td colspan="9">● details of safeguarding concerns that may include:
o how safeguarding concerns re potential/actual abuse/neglect came to light
o impact on the data subject
o setting/occasion(s) where/when it took place
o immediate action taken in response to the concern being raised (any use of emergency services, Crime number, any immediate safeguarding plan)
● name and contact details (including address, telephone number, email address)
● age/date of birth
● language
● school and educational information
● housing information
● social services information, referrals and assessments, including child protection and adoption records where appropriate
● financial information, including benefits records and housing rent records
● images in photographs, film or CCTV, noting that the CCTV DSA comprehensively covers the sharing of CCTV footage and should be referred to
● employment information
● relationship of data subject/s to subject of the safeguarding (if not the subject themselves)
● Details of current ongoing criminal investigation against a staff member and relevant information to aid organisation investigation whilst not jeopardising the criminal investigation</td></tr>
<tr><td></td><td colspan="10">Special Categories of Personal Data</td></tr>
</table>

Racial or ethnic origin				**yes**	Political opinion				Religious or philosophical beliefs			**yes**
Trade Union membership					Physical or mental health or condition							**yes**
Sexual life or sexual orientation			**yes**	Social service records			**yes**	Child protection records				**yes**
Sickness forms		Housing records		**yes**	Tax, benefit or pension records				Adoption records			
DNA profile		Fingerprints			Biometrics			Genetic data				
Proceedings for any offence committed or alleged, or criminal offence record ● Details of current ongoing criminal investigation against a staff member and relevant information to aid organisation investigation whilst not jeopardising the criminal investigation												**yes**
Other data *(Please state):*	● details of safeguarding concerns that may include: o how safeguarding concerns re potential/actual abuse/neglect came to light o impact on the data subject o setting/occasion(s) where/when it took place o immediate action taken in response to the concern being raised (any use of emergency services, Crime number, any immediate safeguarding plan) o In respect of adults aged 18-25, details regarding their sexual and/or criminal exploitation, including 'County Lines' and missing children data for when they were under 18 and at risk from or receiving support for reasons related to MACE - Multi-Agency Child Exploitation. ● gender, ethnic origin, religion and other equalities information ● criminal information on allegations and convictions, police information and intelligence, information from the London Fire Brigade, anti-social behaviour (ASB) data ● health records including NHS number, GP, London Ambulance Service, Mental Health services and other health services information, which are not already available to the parties through systems such as Child Health Information System (CHIS), CP-IS, HiE or HealtheIntent and similar. ● information on sex life and sexual orientation ● social services information, referrals and assessments, including child protection and adoption records where appropriate											
Will the dataset include clinical data? (please include)												**Yes/No** Yes where health records are shared by NHS partners

	Will the dataset include financial data?	where relevant
	Description of other data processed/shared/viewed?	

2.3	**<u>Business sensitive data</u>**			
	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
	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	Controller	Yes
	London Probation Service	Controller	Yes
	London Ambulance Service NHS Trust	Controller	Yes
	London Fire Brigade	Controller	Yes
	ALMOs (housing management for council housing)	Controller	Varies
	London Clinical Commissioning Groups (CCGs)	Processor	Yes
	Department for Work & Pensions (inc Job Centre Plus)	Controller	Yes
	Service users'/patients' organisations	Controller	Yes
	Carers' organisations	Controller	Varies
	Advocacy providers inc Healthwatch	Controller	Varies
	Care Home and Domiciliary Care providers/associations	Controller	Varies
	Supporting People providers	Controller	Varies
	Victim support services e.g. Victim Support, Rape Crisis, Women's Aid	Controller	Varies
	Voluntary sector service providers e.g. Age Concern, Help the Aged, MIND, People First, MENCAP, SCOPE	Controller	Varies
	Voluntary sector groups working against abuse of adults e.g. ACT, Action on Elder Abuse, PAVA, POPAN.	Controller	Varies
	Housing Associations/Trusts	Controller	Varies

3.2	**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/No **Yes** - A single DSA will be put in place to cover sharing with the listed adult safeguarding 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 flows will vary case by case according to specific circumstances and case requirements**
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?** *(For example Direct Patient Care, Statistical, Financial, Public Health Analysis, Evaluation. See NHS Confidentiality Code of Practice Annex C for examples of use)*	

This DSA is a means of establishing a standard for sharing sensitive and confidential information for safeguarding purposes and for ensuring those making decisions about adults who may be at risk of abuse or neglect are conducted within statute and regulatory guidance. This may include information about adults who are at risk, service providers or those that may pose a risk to others.

The purpose of the DSA is to provide a framework for the secure and confidential sharing of information between organisations to:

- Ensure there is a consistent and effective response to safeguarding concerns and allegations or disclosures of abuse or neglect.
- Enable early interventions to prevent the escalation of risk.
- Work efficiently together to conduct safeguarding enquiries and support other reviews, such as Safeguarding Adults Reviews (SARs).

Safeguarding means protecting an adult's right to live in safety, free from abuse and neglect. It is about working together to support people to make decisions about the risks they face in their own lives and protecting those who lack the mental capacity to make those decisions. Adults who may be at risk of abuse or neglect include those with care and support needs, for example relating to a person's age, physical or learning disability, mental health needs or other illness. Safeguarding interventions may also be needed in response to people who experience homelessness, domestic abuse, sexual exploitation, anti-social behaviour, modern slavery and cuckooing.

Safeguarding adults at risk is a complex area of work that involves a number of professional organisations working together with the common purpose of preventing or reducing the risk of significant harm to adults at risk from abuse or other types of exploitation, whilst supporting individuals to maintain control over their lives. This includes being able to make choices without coercion. To achieve this, the sharing of information amongst professional organisations who work with vulnerable adults is essential. Early sharing of information is the key to providing an effective response where there are emerging concerns. Sometimes it is only once information from a range of sources is coordinated that an adult is identified as being at risk. It is better that information is shared rather than withheld if this may prevent a vulnerable adult from suffering harm.

To deliver the best safeguarding decisions that ensure timely, necessary and proportionate interventions, decision makers need the full information picture concerning an individual and their circumstances to be available to them. 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 local residents and other stakeholders safe and assist signatories to this Agreement in discharging their obligations under the Act and other legislation.

Information may be shared with and via the Safeguarding Adults Board or other inter-agency groups that focus on specific safeguarding issues as well as on a one-off basis between relevant partners.

Sharing for statutory safeguarding purposes section 42 of the Care Act 2014

Sections 42 to 47 of the Care Act 2014 set out the legal responsibilities in relation to adult safeguarding. The legal framework for the Care Act 2014 is supported by the Care and Support Statutory Guidance which provides information about how the Care Act should operate in practice.

Section 42 of the Care Act 2014 says that the duty to undertake a safeguarding adults enquiry arises where a Council has reasonable cause to suspect that an adult in its area (whether or not ordinarily resident there)

- has needs for care and support (whether or not the authority is meeting any of those needs);
- is experiencing, or is at risk of, abuse or neglect; and
- as a result of those needs is unable to protect himself or herself against the abuse or neglect or the risk of it.

The Care Act 2014 guidance states that early sharing of information is the key to providing an effective response where there are emerging concerns for an Adult at Risk, and no professional should assume that someone else will pass on information which they think may be critical to the safety and wellbeing of the adult. If concerns are raised about the adult's welfare, whether this be the belief that they are suffering or likely to suffer abuse or neglect, and/or are a risk to themselves or another, information should be shared with the local authority and/or the police if the professional/Signatory Organisation believes or suspects that a crime has been committed or that the individual is immediately at risk.

Adults have a legal right to make their own decisions, even if they are unwise, as long as they have the capacity to make those decisions and are free from coercion and control or undue influence. In situations when the individual, about whom the data relates to, does not have capacity to give consent to the sharing of information, in situations where consent is the lawful basis for sharing, then a best interests decision should be made in line with the principles of the Mental Capacity Act 2005.

Sharing for non-statutory safeguarding purposes - purposes of section 1 of the Care Act 2014 and other purposes.

There is no legal obligation on the Local Authority to undertake non-statutory safeguarding enquiries. Ordinarily, such adults would be signposted to sources of support instead. However, there is scope for the local authority to undertake a non-statutory safeguarding enquiry if agreed. An example would be where the adult does not meet the ‘three part test’ but it is agreed that the risks are too high not to continue to take action.

There is no exhaustive list of non-statutory safeguarding purposes under this agreement as every case will have unique features. Whilst the sharing under this section is not statutory under the Care Act 2014, it is noted that in some cases other statutory duties may apply to one or more parties taking action, investigating, and sharing information for those purposes. In some cases, the matters may be criminal offences. Examples of where this could be applicable are when there are high risk issues pertaining to domestic abuse, self-neglect, substance misuse and refusal for health interventions.

Indicative types of purpose would be:

- investigating and resolving individual cases of rough sleeping
- coordinating solutions to cases of entrenched rough sleeping
- homeless persons who are at risk of harm from being homeless
- persons vulnerable due to hoarding by themselves or others
- persons vulnerable due to significant fire risks in their property
- Self-neglect which is having a significant effect on the individual's ability to manage their personal care and hygiene, home environment, activities of daily living, health conditions, finances and similar.
- Adults who are, have been or who are at risk of being victims of cuckooing
- Adults who are, have been, or who are at risk of being victims of physical abuse, sexual abuse, psychological abuse, financial or material abuse, and/or discriminatory abuse (which includes hate crimes)
- Adults aged 18-25 who, when aged under 18, were at risk from or receiving support for reasons related to MACE - Multi-Agency Child Exploitation, issues concerning the sexual and/or criminal exploitation of children, including 'County Lines' and missing children.
- where a staff member has had an allegation made against them of harming or abusing a vulnerable person, often to the police, and a safeguarding or disciplinary investigation is required for the employer or others to take appropriate action

Safeguarding Adults Board

Under the Care Act 2014 all local authorities must establish a Safeguarding Adults Board (SAB). The overarching purpose of a SAB is to help and safeguard adults with care and support needs. It leads adult safeguarding arrangements across its locality and oversees and coordinates the effectiveness of the safeguarding work of its member and partner agencies. One of the Board's core duties under Section 44 of the Care Act is to commission Safeguarding Adult Reviews (SARs) for any cases which meet the relevant criteria, and to ensure learning takes place for such cases in which adults die or are seriously harmed from abuse or neglect.

For such reviews, the Board has the power under s45 of the Care Act 2014 to require any body to provide information that meets the criteria in the section. This reflects that information sharing is essential to improve outcomes for all and to ensure issues for wider public protection as well as risk to individuals are detected.

Benefits

The benefits of this DSA are to:

- Cover the sharing of information for adult safeguarding purposes.
- Enable early intervention and 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.
- Greater efficiencies in processes and resources.
- Preventing and detecting crime.
- Allowing employers to deal effectively when safeguarding related allegations are made about a member of staff particularly in regulated activity when it is important to protect the public

Partner Agencies and Society

- Support increased mutual understanding of safeguarding issues and the use of risk assessment techniques as well as increasing partners' knowledge of the success of different types of intervention strategies.
- Faster, more coordinated and consistent response to safeguarding concerns.
- A more accurate assessment of the risk and need, and the ability to modify plans in the light of information shared.
- A more thorough and focused management of all cases.
- Improving outcomes for adults at risk.
- Better understanding between professionals.
- Avoiding the duplication of effort in respect of service provision and record taking and creating greater efficiencies in processes and use of resources.
- Preventing and detecting crime that impacts individuals and society.
- By sharing their understanding of risk in particular situations, agencies are in a better position to integrate risk assessment into their daily practice.
- Provide reassurance to practitioners on the parameters for sharing and the methods for sharing securely.
- To improve the referral processes around the provision of services for adults at risk.
- To improve the referral processes around interventions to prevent harm by organisations.

Individuals

- Timely action taken to reduce the risk of harm and increase the safety, health and wellbeing of adults at risk.
- A person-centred approach designed to support individuals and deliver comprehensive risk identification and safety planning based on a full account of the facts and circumstances of each individual's situation.
- Adults aged 18-25 who, when aged under 18, were at risk from or receiving support for reasons related to MACE - Multi-Agency Child Exploitation, issues concerning the sexual and/or criminal exploitation of children, including 'County Lines' and missing children.
- The right sort and combination of advice, support and advocacy to be offered at the right time, based on a full and accurate account of the individual's needs and history, including other service contact and use.
- To avoid the added distress for individuals of having to repeat details of their history or experience and other circumstances each time they encounter a different service.
- Safeguard adults in a way that supports them in making choices and having control about how they want to live
- Promote an approach that concentrates on improving life for the adults concerned

	● Ensure that appropriate risk based decisions are made in respect of staff about whom safeguarding allegations have been made,and to safeguard those who may have been or will be in contact with that person

Step 4: Assess necessity and proportionality	
4.1	**Lawfulness for Processing/sharing personal data/special categories of personal data?** **2.4.1 For purposes other than law enforcement by competent authorities** Articles 6, 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. ● **For Local Authorities and the London Ambulance Service** **Article 6 (1) – Personal Data Processing:** (c) processing is necessary for compliance with a **legal obligation** to which the controller is subject. For providing information to the Safeguarding Adults Board for Safeguarding Adult Reviews there is a legal requirement to supply certain information upon request in s45 Care Act 2014. In respect of other sharing, there are a range of laws as specified in appendix C which will apply to different non-law enforcement parties in different circumstances (d) processing is necessary in order to protect the **vital interests** of the data subject or of another natural person (e) processing is necessary for the performance of a **task carried out in the public interest** or in the exercise of official authority vested in the controller. 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. For local authorities the Care Act 2014 may be the most common **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 (c) processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; (h) **provision of health or social care** - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. This requires DPA 10(2) be satisfied which needs a condition in Schedule 1, Part 1 and for this agreement these are: ● Health or Social Care Purposes under Para 2 with appropriate safeguards as required by section 11(1) of the act and Article 9(3) of the UK GDPR

Art. 10 UK GDPR : Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. The article 6 conditions are given above, and the DPA18 Schedule 1, Part 1 conditions met are para 2(1) Health or social care purposes, and Part 2 conditions are paras 6 Statutory etc and government purposes, 10 Preventing or detecting unlawful acts, and 18 Safeguarding children and individuals at risk.

- **For Voluntary sectors:**

It is the responsibility of all data controllers to ensure that their Record Of Processing Activities accurately reflect their exact legal basis for their processing.

Article 6(1):

(a) - Legal duty- Where the voluntary sector is subject to requirements over safeguarding this may apply.

(d) - Vital Interests -may apply in rare cases

(e) - Public task- where the organisation is providing services for a local authority this legal basis may well apply

(a) - Consent- may apply in some cases although it is noted that in many cases consent may be inappropriate even for the voluntary sector

(f)- legitimate interests- the legitimate interests of the voluntary sector organisation, and those of the data controller to whom it will share the data, may apply, although a balance must be undertaken of the data subject's rights and freedoms against the organisation's legitimate interests

Article 9

(b) **health and social protection law** in respect of their employees and volunteers as Local Authorities above

(h) **provision of health or social care** -as Local authorities above

(c) vital interests- in rare cases, as above

Art. 10 UK GDPR : Processing of personal data relating to criminal convictions and offences

Same as for Local Authorities and the London Ambulance Service. It is noted that criminal offence data includes allegations and not just actual convictions. Voluntary agencies are likely to process allegations around safeguarding which may amount to criminal offences.

2.4.2 For the purposes of law enforcement by competent authorities (Metropolitan Police and the Probation Service)

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 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.

Part 3 of the DPA 2018 relates to the processing of personal data by a competent authority (as defined in Section 30(1) and Schedule 7 of the DPA 2018) for law enforcement purposes. “Law enforcement purposes” are defined in Section 31 of the DPA 2018 to mean “the 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”.

The powers to share such information are set out in Section 2.4 above.

This regime will be applicable to processing undertaken by competent authorities (e.g. the police) that are processing data for law enforcement purposes. This will apply where, for example, the police wish to contact a partner body to establish the location of a specific individual who is (or may be) a victim, witness or suspect connected to a criminal act.

It is possible that the police may not have a name for the person or people that they are seeking, but are only able to identify an individual using a description of his/her physical appearance. In such cases the police may provide details of the individual which would amount to sensitive processing within the definition of Section 35(3) of the DPA 2018.

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:

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.

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

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 taking appropriate action to correct it and 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?** *For example, do the organisations/partners listed in section 3.1 have updated Fair Processing Notice available to patients on their websites?*		Yes
	Privacy notices for all organisation note safeguarding 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 controller remains responsible for complying with the applicable data subject rights. Each controller has their own documented policies and procedures which details how they will meet their own obligations in respect of data subject rights.		
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. Where a SAR covers data provided by another party, before responding to the SAR, the Controller will consult with the providing party regarding any disclosure concerns they may have.		
4.7	**Will the processing of data include automated individual decision-making, including profiling?** *If yes, please outline the profiling processes, the legal basis underpinning the process, and the rights of the data subject*		No
	N/A		
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
	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 generally the lawful basis the public sector organisations use for processing information shared under this agreement. It is noted that where consent is not the lawful basis for processing, consent does not need to be sought to share, and thus the concept of "overriding consent" is a misconception. Lawful basis is set out in detail above		

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 be stored** *Examples of Storage include bespoke system (e.g. EPR, Emis & other clinical systems, SharePoint, data repository, Network Drives, Filing cabinet (office and location), storage area/filing room (and location) etc.*	
	Provider systems are used. Paper storage is minimised; all storage is UK only.	
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
	As necessary data may be shared with externally instructed lawyers/counsel, the CPS, the courts and other agencies as required to undertake legal action or provide appropriate care and support to the adults in question.	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 an audit built in. We cannot guarantee for the voluntary sector, however they will be supplying rather than receiving information in most cases.	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)	
	This will vary between partners, but all will have undergone appropriate employee checks, DBS checks where necessary and will be bound by employee codes of conduct. For the voluntary sector it is noted that hey will be supplying rather than receiving information in most cases	
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 N	key to locked filing cabinet/room	yes

				H S		
	Secure 1x Token Access		Restricted access to Network Files			yes
	Other: *Provide a Description Below*:					

5.5	**Is there a documented System Level Security Policy (SLSP) for this project? If yes, please embed a copy below:** SLSP is required for new systems. *SLSP refers to the architecture, policy and processes that ensure data and system security on individual computer systems. It facilitates the security of standalone and/or network computer systems/servers from events and processes that can exploit or violate its security or stature.*	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?** Please explain and give reference to such plan and protocol	Yes/No	Yes

5.7	**Is Mandatory Staff Training in place for the following?**	Yes/No	
	● Data Collection:	Yes	
	● Use of the System or Service:	Yes	
	● Information Governance:	Yes	

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 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 risks of this sharing ONLY. Signatories should have DPIAs for their own individual systems and methods, covering their local risks.			
Misuse of data: Personal data could be used by a recipient in a manner incompatible with the Data Sharing Agreement. This might be unauthorised uses or disclosure to inappropriate persons. Compliance risk: Appropriate technical and organisational measures shall be taken. Corporate risk: Reputational risk. Loss of trust. Legal implications.	Medium	High	Medium
Loss of data in transfer. Personal data could be obtained and misused by third parties. Compliance risk: Appropriate technical and organisational measures shall be taken. Corporate risk: Reputational risk. Loss of trust. Legal implications.	Medium	High	Medium/high
Further transfer of data: Risk to the safety of personal data if transferred elsewhere by a recipient. Concerns may be for sharing with 3rd parties such as insurance companies or the press. Compliance risk: Personal data shall be obtained for one or more specified and 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	Medium/high
Disposal of data: If personal data is not disposed of in an appropriate manner by the party with whom it was shared, it may be possible for third parties to obtain the data. Compliance risk: Personal data shall not be kept for longer than necessary. Appropriate technical and organisational measures shall be taken. Corporate risk: Reputational risk. Loss of trust. Legal implications.	Medium	High	Medium/high
Inherent privacy intrusion: sharing of personal data is inherently privacy intrusive, especially for vulnerable people Compliance risk: data minimization, privacy intrusion Appropriate technical and organisational measures shall be taken.	High	High	High

Corporate risk; Reputational risk. Loss of trust. Legal implications			
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
Lack of notice to data subjects. In some cases 3rd parties may not have appropriate privacy notices in place Compliance risk: data minimization, privacy intrusion Appropriate technical and organisational measures shall be taken. Corporate risk; Reputational risk. Loss of trust. Legal implications	High	Medium	Medium/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**
Misuse of data:	Sharing will be by and to authorised officers only who are subjected to full employment checks. Access to council systems are fully RBAC and auditable. All organisations have full employee policies and codes of conduct. Breaches of those would be a disciplinary offence and may be a criminal act.	Reduced	Low	Yes
Loss of data in transfer.	The DSA specifies the appropriate technical measures in place to ensure the security of the data transfers. Organisations have full policies and procedures in place for the safe transfer of data. Councils routinely share volumes of special category data and have well established protocols to do so safely.	Reduced	Low	Yes

Further transfer of data:	It is noted that where one party receives data from another, the receiving party becomes a Data Controller and therefore takes the liability for the data from that point, and is bound by the requirements of data protection legislation. All parties have full policies and processes in place to ensure data is handled securely. Systems are auditable and RBAC is in force. Employees are subject to robust employment checks. However it is noted that where a Data Controller handles data in a manner not expected this can lead to reputational damage for the supplying party, notwithstanding they have no legal liability data protection wise. For the data in this DSA it is considered these risks are low.	Reduced	Low	Yes
Disposal of data	It is noted that where one party receives data from another, the receiving party becomes a Data Controller and therefore takes the liability for the data from that point, and is bound by the requirements of data protection legislation. All parties have their own data retention policies which they will follow.	Reduced	Low	Yes
Inherent privacy intrusion	The risk is the sharing with and by councils **not** the existing processing for adult safeguarding which are covered by other DPIAs. A degree of privacy intrusion is unavoidable, otherwise the sharing could not be facilitated. The DSA requires that sharing will only be of data necessary in each instance and will be the minimum needed to achieve the lawful purposes.	Reduced	Medium	Yes
Voluntary sector	Data minimisation, ensure only needed sharing is done. Appropriate policy document. Storage to be minimised	Reduced	Low	Yes

Lack of Notice to data subjects	The risk is the sharing with other parties not the underlying data uses. All organisations will be encouraged to have appropriate privacy notices which include this sharing: the major partners already do. In some cases the sharing will fall under exemptions from notification.	Reduced	Low	Yes

Residual Risk Level	**Medium**

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by:	Sarah Laws, Anthea Ferguson	Each Data Controller's IAO to ensure they agree
Residual risks approved by:	Sarah Laws, Anthea Ferguson	Each Data Controller's IAO to ensure they agree
DPO advice provided:	Sarah Laws, Anthea Ferguson	Data Protection Manager LB Camden Information Manager LB Hammersmith and Fulham
Summary of DPO advice: *Please see the FAQs on how councils should adopt/adapt this DPIA or undertake their own.* This is assessed as medium risk. The inherent privacy intrusions are considered proportionate to the aims of the processing and bearing in mind the procedures and processes in place to ensure data minimisation and proportionality, and the legal duties involved.		
Comments: Approved Andrew Maughan Data Protection Officer March 2022		
This DPIA will kept under review by: Sarah Laws	The DPIA will be reviewed by the respective DPOs of each organisation when required	The DPO should also review ongoing compliance with DPIA