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**	**16/3/22**	**Sarah Laws**
1.0	**Revised draft, agreed**	**22/3/22**	**Sarah Laws, Janice Boucher, Rukshana Hussain**

Project / Work Stream Name	**Youth Offending Service Pan-London Data Sharing Agreement**
Overview: (Summary of the project/work stream)	This DPIA covers the Data Sharing Agreement (DSA) between all London local authorities including City of London Corporation, the Metropolitan Police, the City of London Police, and the London Probation Service, which explains what information they will share about the full range of Youth Offending Services [YOS] to allow each party to undertake their roles in YOS matters. It should be noted that the DSA does not include sharing with the Youth Justice Liaison and Diversion service which is subject to separate arrangements. It does not cover sharing between individual councils, or councils and local bodies, which will be subject to local arrangements. The DSA 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.

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.	YOS work is carried out across London and is a legal obligation. This is a renewal of previous fragmented agreements, and for councils with no existing DSAs, a new DSA, intended to cover all-London. It has been produced with the input of representatives from: ● London Boroughs' YOS teams ● the Metropolitan Police, ● the Information Governance for London forum (a group of IG professionals from across all London Boroughs) ● Probation Services

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?	No
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.**

Step 2: Identify the need for a DPIA										
2.1	**Is this a new or changed use of personal data/special categories of personal data and/or business sensitive data that is already processed/shared?**								New/Changed	
									Changed	
2.2	**What data will be processed/shared/viewed?**									
	Personal Data									
	Forename	yes	Surname	yes	Date of Birth	yes	Age	yes	Gender	yes
	Address	yes	Postal address	yes	Employment records	yes	Email address	yes	Postcode	yes
	Other unique identifier (*please specify*)	yes eg case management system ref number	Telephone number	yes	Driving licence number		NHS No		Hospital ID no	
	Other data *(Please state):*	• details regarding personal life, habits and lifestyle • family and close contacts information • location information • people with whom the young person may be in conflict with or at risk from • any other relevant information that needs to be shared in real-time to protect the general public from crime and disorder								
	Special Categories of Personal Data									
	Racial or ethnic origin			yes	Political opinion		yes	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 • criminal information on relevant allegations, criminal justice proceedings and convictions, relevant police information and intelligence									**yes**
	Other data *(Please state):*	• health and wellbeing information								

		• vulnerability information • danger and exploitation indicator	

Will the dataset include clinical data? (please include)	**Yes/No**
	NO
Will the dataset include financial data?	Only 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			

<table>
<tr><th colspan="4">Step 3: Describe the sharing/processing</th></tr>
<tr><td rowspan="5">3.1</td><td colspan="2">List of organisations/partners involved in sharing or processing personal/special categories personal data? If yes, list below</td><td>Yes/No</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td>Name</td><td>Controller or Processor?</td><td>Completed and compliant with the IG Toolkit or Data Security and Protection (DSP) Toolkit
Yes / No</td></tr>
<tr><td>London Local Authorities</td><td>Controller</td><td>Yes</td></tr>
<tr><td>Metropolitan Police Service, and City of London Police</td><td>Controller</td><td>Yes</td></tr>
<tr><td>3.2</td><td>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?</td><td colspan="2">Yes/No
Yes - This DPIA covers the single DSA that will be put in place to cover sharing with the partners. Each Local Authority will be responsible for ensuring that they have Data Processing Contracts in place with any local Processors.</td></tr>
<tr><td>3.3.</td><td>Has a data flow mapping exercise been undertaken?
If yes, please provide a copy, if no, please undertake</td><td colspan="2">The flows will vary case by case according to specific circumstances and case requirements</td></tr>
<tr><td rowspan="2">3.4</td><td colspan="2" rowspan="2">Does the project involve employing contractors external to the Organisation who would have access to personal or special categories of personal data?</td><td>Yes / No</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">3.5</td><td colspan="3">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)</td></tr>
<tr><td colspan="3">The DSA covers information sharing between councils, the Metropolitan Police, the City of London Police, and London Probation Services for YOS- Youth Offending Services. The scope described in sections 1 and 1.6 of the DSA explain the information sharing that is covered by this agreement - that is information shared between councils’ YOS, the Metropolitan Police, the City of London Police, and London Probation Services in respect of Youth Offending Services. This includes preventative measures, interventions, referrals, transfer to Adult Probation Service, and assessments.
Research and experience have demonstrated the importance of information sharing across professional boundaries to ensure effective delivery of YOS, better outcomes for young people and protection of the public. Lack of data sharing results in poor outcomes, including greater exposure of young people to danger and exploitation, increased crime, more victims and less</td></tr>
</table>

public safety. 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 to relevant agencies in one place; to keep young people and members of the public safe and assist signatories to this Agreement in discharging their obligations under the relevant legislation that covers delivering YOS.

To deliver the best decisions that ensure timely, necessary and proportionate interventions, local authority decision makers need the full information picture concerning a young person, other relevant individuals and their circumstances to be available to them. The police who provide intelligence to the local authority on YOS matters need appropriate information in order to make fully informed and evidenced representations, and to fulfil their law and order responsibilities effectively. Police who may be called to deal with urgent issues regarding youth offending may need timely and up-to-date information to effectively handle such matters.

Young offenders often find themselves in complex situations, causing them to be vulnerable to external influences. In order to provide a comprehensive service, YOS professionals need to respond in real-time with up-to-date information. The Police share intelligence with local authorities on criminal behaviour and activities, e.g. carrying weapons and key information needs to be shared by various YOS professionals to take appropriate action.

In order to act collectively and work effectively with young offenders, sharing information is crucial to piecing together the whole picture and providing the right support, protection and justice outcomes.

Benefits

The benefits of this DSA are to achieve a more comprehensive, joined up and efficient method for both police and councils to deliver their YOS work using up-to-date, relevant and timely information. It will also:

- Cover the sharing of information for welfare and criminal justice purposes.
- 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 the signing partners of the key issues relating to information sharing and gives confidence in the process of sharing information with others.
- Provide better understanding between professionals.
- Greater efficiencies in processes and resources.
- Preventing and detecting crime.
- Effectively dealing with public safety concerning YOS related matters
- Ensuring the most appropriate outcome is achieved.

Step 4: Assess necessity and proportionality	
4.1	**Lawfulness for Processing/sharing personal data/special categories of personal data?** **Councils sharing information under this DSA with the Metropolitan Police and or Probation Services do so under the Crime and Disorder Act 1998 and therefore operate under Part 3 of the Data Protection Act 2018.** Where councils share information with other organisations for YOS purposes such as safeguarding they will operate under Part 2 of the Data Protection Act 2018. That sharing is outside this DSA and is covered in for example the MAS, Adults Safeguarding, Gangs, and or ASB DSAs. References should be made to those DSAs for the relevant lawful basis and terms and conditions for sharing under those agreements. **For the purposes of law enforcement by competent authorities - ie councils under this DSA** The "competent authorities" are defined in Section 30 of the DPA which refers to Schedule 7. The competent authorities under this agreement are police, probation services and youth offending teams. 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".* The processing under this DSA is for law enforcement purposes. s35(2) DPA says that the processing of personal data for any of the law enforcement purposes is only lawful where it is based on law and either the data subject has given consent to the processing for that purpose, or the processing is necessary for the performance of a task carried out for that purpose by a competent authority. The law is provided in Appendix C. Data subjects do not provide consent for this processing. However the processing is necessary to perform the tasks of the parties in respect to their roles as set out in this DSA. 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 data processed under this DSA will include sensitive processing. The additional alternative 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. That is not applicable in this case. 35(5) requires that the processing be strictly necessary for the law enforcement purposes, and meets a condition in Schedule 8. **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). **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 remit of YOS. The terms of this agreement address the requirements for data sharing pursuant to Part 3 of the DPA 2018. To note that there is a separate regime for intelligence service processing, which falls outside the remit of this DSA.		
4.2	**Will the information be processed/shared electronically, on paper or both?**	Electronic	Yes
		Paper	No
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 relevant 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.		
4.5	**How will you help to support the rights of individuals?**		
	Note that for this DSA the rights are those under Part 3 DPA 18 not Part 2. 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)?**		
	Note that for this DSA the rights are those under Part 3 DPA 18 not Part 2.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. All storage is EEA 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
	It may be shared with externally instructed lawyers/counsel, the CPS, the court service etc as necessary in individual cases.	Possibly
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.	Yes
5.2	**How will access to information be controlled?**	
	This varies between Partners, 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)	
	Relevant professionals in the Partners	
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		key to locked filing cabinet/room	
	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

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. The YOS information is sensitive and about young people who are afforded special protections under the law and who by virtue of being under YOS are vulnerable. Compliance risk: Appropriate technical and organisational measures shall be taken. Corporate risk: Reputational risk. Loss of trust. Legal implications.	Medium	Very High	Very High
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. The YOS information is sensitive and about young people who are afforded special protections under the law and who by virtue of being under YOS are vulnerable. 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	High	High	High

people. The YOS information is sensitive and about young people who are afforded special protections under the law and who by virtue of being under YOS are vulnerable. Compliance risk: dasta minimization, privacy intrusion Appropriate technical and organisational measures shall be taken. Corporate risk; Reputational risk. Loss of trust. Legal implications			

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 all Partner 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. The Partners 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	Reduced	Low	Yes

	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.			
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 Partners **not** the existing processing for YOS which are covered by other DPIAs. 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. There are laws requiring the sharing and sharing of information required by law is considered to be proportionate	Reduced	Medium	Yes

Residual Risk Level	**Medium**

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by:	Sarah Laws, Janice Boucher, Rukshana Hussain	Each council IAO to check they agree from their own perspective
Residual risks approved by:	Sarah Laws, Janice Boucher, Rukshana Hussain	Each council IAO to check they agree from their own perspective
DPO advice provided:	Sarah Laws, Janice Boucher, Rukshana Hussain	LB Camden (and LOTI) LB RBKC LB Hillingdon
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 remaining risk that is medium rather than low is the privacy intrusion. This is 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: Accepted as drafted Andrew Maughan Data Protection Officer March 2022		
This DPIA will kept under review by: Eugene Griffin	The DPIA will be reviewed by the respective DPOs of each organisation when required	The DPO should also review ongoing compliance with DPIA