DATA PROTECTION IMPACT ASSESSMENT

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

Version Control

Version	Reason	Date	Author(s)
1.0	**New**	**25/3/2021**	[redacted]

Project / Work Stream Name	**London Boroughs and Metropolitan Police BCU Sharing Agreement for Anti-Social Behaviour ("ASB"), disorder and wider community safety**	
Project / Work Stream Lead	Name	[redacted]
	Designation	Information Rights Team Leader, LB Camden/ Information Governance Lead, LB Islington
	Email	[redacted]@camden.gov.uk [redacted]@islington.gov.uk
Overview: **(Summary of the project/work stream)**	The DPIA covers the Data/Information Sharing Agreement (DSA/ISA) between each London Borough and the Metropolitan Police covering information about **anti-social behaviour (ASB)** and disorder and wider community safety. Anti-social behaviour (ASB) is defined in the Crime and Disorder Act (1998) as acting 'in a manner that caused or was likely to cause harassment, alarm or distress to one or more persons not of the same household as the perpetrator.' ASB can be targeted to a specific individual or group or community. Environmental antisocial behaviour is when a person's actions affect the wider environment, such as public spaces or buildings. Antisocial behaviour can have a lasting impact on neighbourhoods and communities as it often leads to an increase in crime, particularly violence and criminal damage. Wider community safety covers all areas regarding Community Protection Notices, Criminal Behaviour Orders, ASB Injunctions and other areas that require joint working for the prevention and detection of crime related to anti-social behaviour, and the reduction of anti-social behaviour. It includes information sharing where this will help agencies understand the root causes of ASB and assist them in identifying the most appropriate action to take.	

	Research and experience have demonstrated the importance of information sharing across professional boundaries to ensure effective delivery of public services. Many of the areas covered in the DSA/ISA are areas where the police and councils frequency work closely and liaise over common matters. To deliver the best most effective decisions in any case, that ensure timely, necessary and proportionate interventions, decision makers and action takers need the full information picture and the wider circumstances to be available to them. Information viewed alone or in silos may not give the full picture or identify the true risk.
Implementation Date:	1/4/2021
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.** *Please provide any supporting documents such as benefit study, fact sheets, white papers, reports or refereed articles published by industry associations, technology providers, and research centres.*	The areas covered by this DSA/ISA is undertaken pan London and nationally and is covered by a number of Acts. There has been no previous comprehensive DSA/ISA for this information leading to ad hoc local arrangements with varying degrees of success. The DSA/ISA was drafted and agreed by a working group comprising Data Protection specialists, council community safety and similar officers, the Metropolitan Police Information Sharing Unit, a police safeguarding Detective Chief Inspector and a crime Detective Superintendent .

Step 1: Complete the Screening Questions

Q 1	Category	Screening question	Yes/No
1.1	Technology	Does the project introduce new or additional information technologies that can substantially reveal an individual's identity and has the potential to affect that person's privacy?	No
1.2	Technology	Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business?	No
1.3	Identity	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Local Gov. Identifier, Hospital ID no. or, will use intrusive identification or identity management processes or, electronic linkage of personal data?	Yes

1.4	Identity	Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	No
1.5	Multiple organisations	Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners?	Yes
Q	**Category**	**Screening question**	
1.6	Data	Does the project involve new process or significantly change the way in which personal data/special categories of personal data and/or business sensitive data is handled? *See glossary of terms*	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 U.K?	No
1.11	Exemptions and Exceptions	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	Yes
1.12	Exemptions and Exceptions	Does the project's justification include significant contributions to public security and measures?	Yes
1.13	Exemptions and Exceptions	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	No

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

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

Step 2: Identify the need for a DPIA

2.1	**Is this a new or changed use of personal data/special categories of personal data and/or business sensitive data that is already processed/shared??**	New/Changed Changed

2.2 **What data will be processed/shared/viewed?**

Personal Data

Forename	**X**	Surname	**X**	Date of Birth	**X**	Age	**X**	Gender	**X**	
Address	X	Postal address	X	Employment records	x	Email address	x	Postcode	X	
Other unique identifier (*please specify*)		Telephone number	X	Driving licence number		NHS No		Hospital ID no		

Other data *(Please state)*:

- information as to whether a victim is a repeat victim
- school and educational information
- housing information
- social services information, referrals and assessments, which may include physical and mental health needs where relevant,
- financial information
- images in photographs, film or CCTV
- employment information
- next of kin and carer contact details

Special Categories of Personal Data							
Racial or ethnic origin	x	Political opinion		Religious or philosophical beliefs			
Trade Union membership		Physical or mental health or condition	X where relevant				
Sexual life or sexual orientation		Social service records	X where relevant	Child protection records	X where relevant		
Sickness forms		Housing records	X where relevant	Tax, benefit or pension records		Adoption records	
DNA profile		Fingerprints		Biometrics		Genetic data	
Proceedings for any offence committed or alleged, or criminal offence record	X						
Other data *(Please state):*							
Will the dataset include clinical data? (please include)	**no**						
Will the dataset include financial data?	Yes where relevant						
Description of other data processed/shared/viewed?							
social services information, referrals and assessments, which may include physical and mental health needs where relevant.							

2.3	**Business sensitive data**		
	Financial	No	
	Local Contract conditions	No	
	Operational data	No	
	Notes associated with patentable inventions	No	
	procurement/tendering information	No	
	Customer/supplier information	No	

	Decisions impacting:	One or more business function	**Yes/No** No
		Across the organisation	No
	Description of other data processed/shared/viewed (if any).		
	N/A		

Step 3: Describe the sharing/processing			
3.1	**List of organisations/partners involved in sharing or processing personal/special categories personal data?** *If yes, list below*		Yes/No
			Yes
	Name	Controller or Processor?	Completed and compliant with the IG Toolkit or Data Security and Protection (DSP) Toolkit
			Yes / No
	London Local Authorities	Controller	Yes
	Metropolitan Police Service	Controller	Yes
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
3.3.	**Has a data flow mapping exercise been undertaken?** *If yes, please provide a copy, if no, please undertake*		The DSA/ISA includes statements on flows, but in general data is shared from councils to the police, and from police to councils.
3.4	**Does the project involve employing contractors external to the Organisation who would have access to personal or special categories of personal data?** *If yes, provide a copy of the confidentiality agreement or contract?*		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)
	See overview above. Police and councils roles are hampered without proper information, and enhanced by timely appropriate sharing.

Step 4: Assess necessity and proportionality

4.1	**Lawfulness for Processing/sharing personal data/special categories of personal data?**

UK GDPR		**DPA 2018**		**Other Lawful Basis**	
Personal data sharing					
Article 6 1(c) processing is necessary for compliance with a **legal obligation** to which the controller is subject Article 6 1(e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller		Data Protection Act section 8. The applicable laws are given at Appendix C of the DSA/ISA and are in the next column. The police legal basis is 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".*		Crime and Disorder Act 1998 Public Order Act 1986 Antisocial behaviour crime and policing act 2014 The Health Protection (Coronavirus) Regulations 2020 The Mental Health Act 1983 and the Mental Health Act Code of Practice Police and Criminal Evidence Act 1984 Human Rights Act 1998 Common Law	
Special Category Personal Data Sharing					
Article 9 2(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 Article 9 2(g) 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)***			

	Article 9 2(g) **substantial public interest** - processing is necessary for reasons of substantial public interest, on the basis of 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		***Preventing and detecting unlawful acts under Para 10(1)(2)(3)*** ***Safeguarding children and individuals at risk under Para 18(1)(2)(3)(4)***			

4.2	**Will the information be processed/shared electronically, on paper or both?**	Electronic	X
		Paper	X

4.3	**How will you ensure data quality and data minimisation?**	
Each partner is responsible for ensuring the accuracy and relevance of the personal data that it processes and shares and must have clear processes in place for managing data quality. Any party learning of the inaccuracy of personal data is responsible for informing the parties with whom that data has been shared.		
4.4	**Have individuals been informed about the proposed use of their personal or special categories of personal data?** *For example, do the organisations/partners listed in section 3.1 have updated Fair Processing Notice available to patients on their websites?*	NO
	Privacy notices for all organisation note law purposes, and specific privacy notices for particular areas will include provisions for sharing for law enforcement and associated uses. However law enforcement is excluded from many of the requirements to notify hence some, but not all, use will be without notice.	
4.5	**How will you help to support the rights of individuals?**	
	Full details are provided in the DSA/ISA – some rights are restricted in this area due to the legal basis.	
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.	

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
4.8	**Will individuals be asked for consent for their information to be processed/shared?** *If no, list the reason for not gaining consent e.g. relying on other lawful basis, consent is implied where it is informed.*	NO
	Consent is not the lawful basis for sharing.	
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 system.
4.10	**Where will the data will 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?*	
	The retention period will vary by organisation and subject matter, and will be set out in the relevant retention schedule for each organisation. 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
	Where legal action is undertaken there will be sharing with courts and CPS as necessary. Depending on the nature of the matter and action required, information may be shared with eg the NHS, the probation service, or safeguarding organisations. This is covered by the legal basis.	Yes

Step 5: Information Security Process		
5.1	**Is there an ability to audit access to the information?**	Yes/No
	All DSPT certified provider systems have audit built in	Yes
5.2	**How will access to information be controlled?**	
	This varies between providers, but Role Based Access Control (RBAC) is required with password access as minimum.	
5.3	**What roles will have access to the information?** (list individuals or staff groups)	
Police, council staff, those involved in relevant activities in other council areas such as safeguarding, community safety, and legal.		
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	X	Smartcard	**X**	key to locked filing cabinet/room	**X**
Secure 1x Token Access		Restricted access to Network Files			x
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	Dates
	- Data Collection:	Yes	Continuous

	• Use of the System or Service:	Yes	Continuous
	• Information Governance:	Yes	Continuous
5.8	**Are there any new or additional reporting requirements for this project?**	No	
	• What roles will be able to run reports?		
	N/A		
	• What roles will receive the report or where will it be published?		
	N/a		
	• Will the reports be in person-identifiable, pseudonymised or anonymised format?		
	N/A		
	• Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format?		
	N/A		
5.9	**Have any Information Governance risks been identified relating to this project?** (if Yes the final section will need to be completed)	**Yes/No**	
		Yes	

Step 6: Identify and Assess 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.			
Wider sharing increases risk of disclosure to inappropriate persons	Medium	Medium	Medium
Inherent privacy intrusion from sharing information with a third party. Whilst much of the information to be shared will not be very intrusive, for some cases the information will be sensitive for example relating to vulnerabilities.	Medium	Medium	Medium
Inappropriate secondary processing by recipients of the data	Medium	High	Medium

Step 7: Identify Measures to reduce risk

Identify likely additional measures 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
Wider sharing increases risk of disclosure to inappropriate persons	Training and appropriate policy. Data minimisation, sharing only what is needed. Knowledge of DSA/ISA and its limits.	Reduced	Low	Yes
Inherent privacy intrusion from sharing information with a third party	Data minimisation will be followed. Information only shared where necessary. In the vast majority of cases there will be no damaging intrusion. In many cases the intrusion will have a beneficial outcome.	Reduced	Low	Yes
Inappropriate secondary processing by recipients of the data	Each organisation has appropriate policies in place, staff are trained, aware of the limits of secondary processing and the need for all processing to be compliant with Data Protection legislation.	Reduced	Low	Yes

Step 8: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		
Residual risks approved by:		
DPO advice provided:	[redacted]	

Summary of DPO advice: Note that local DPOs for each organisation need to produce their own DPIAs, or consciously adopt this suggested DPIA		
DPO advice accepted or overruled by:	N/A	If overruled, you must explain your reasons
Comments: N/A		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	The DPIA will be reviewed by the respective DPOs of each organisation when required	The DPO should also review ongoing compliance with DPIA

Glossary of terms

1. ‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
2. ‘Special Categories of Personal Data’ mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.
3. ‘Controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, ‘
4. ‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
5. ‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
6. ‘Data Subject’ – an individual who is the subject of personal information.
7. Data Flow Mapping (DFM) means the process of documenting the flows/transfers of Personal Data, Sensitive Personal Data (known as special categories personal data under GDPR) and Commercially Confidential Information from one location to another and the method by which they flow.
8. ‘Pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
9. ‘Anonymised Data’ - means data in a form where the identity of the individual cannot be recognised i.e. when:
    - Reference to any data item that could lead to an individual being identified has been removed;
    - The data cannot be combined with any data sources held by a Partner with access to it to produce personal data.