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 Data Sharing Agreement	12 August 2021	Kim Starbuck

Project / Work Stream Name	**Integrated Offender Management Data Sharing Agreement**	
Project / Work Stream Lead	Name	Andrew Bessant
	Designation	IG Manager, Richmond and Wandsworth Councils
	Telephone	0208 831 6239
	Email	andrew.bessant@richmondandwandsworth.gov.uk
Overview: **(Summary of the project/work stream)**	IOM is a nationally recognised, multi-agency response to the crime and reoffending threats faced by local communities, with partner agencies working together in the management of offenders, in reducing reoffending by persistent and problematic offenders. IOM is endorsed by the Ministry of Justice (MOJ) as a key effective model to reduce crime and reoffending. IOM helps to improve the quality of life in communities by:	

	● reducing the negative impact of crime and reoffending ● reducing the number of people who become victims of crime ● helping to improve the public's confidence in the criminal justice system In order to achieve a reduction in reoffending, partner agencies need to work together and share relevant and proportionate information, in assessing the needs of individuals and supporting access and engagement with services. Partner agencies with expertise in specific areas work together to manage offenders. These include probation, police, local authorities, drugs and alcohol services and health providers. The benefits of the DSA are to: ● Cover the sharing of information for Integrated Offender Management 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 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. • Reduction in crime, the likelihood of being a victim of crime and the fear of crime • Reduction in the costs of crime • Enhanced public confidence in the Criminal Justice Services through an integrated approach to the management of offenders • Safer communities
Implementation Date:	September 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 IOM Scheme aims to achieve the reduction of offending by the. prolific, priority offenders. National integrated offender management Conference: 2015 The Home Office and the College of Policing held a 2-day national conference, "Integrated Offender Management: meeting the future challenges" on 25 and 26 February 2015. A wide range of speakers spoke about the success of Integrated Offender Management in cutting crime and the potential for the approach to go even further in the future. Themes which emerged during the conference included the role that Integrated Offender Management can play in helping to prevent the onset, or escalation, of problematic criminal careers and how local Integrated Offender Management approaches will need to adapt to changes in the delivery landscape, including the transforming rehabilitation probation reforms. The information shared using this agreement will allow partners to provide the best range of services to IOM clients whilst addressing any continuing offending or anti-social behaviour.

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	No

		personal data and/or business sensitive data about each individual in a database?	
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			
								No			
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		Email address		Postcode	X	
	Other unique identifier (*please specify*)		Telephone number	X	Driving license number		NHS No	X	Hospital ID no		
	Other data *(Please state):*	● Physical descriptions, school and educational information, images in photographs, film or CCTV, employment information									
	Special Categories of Personal Data										
	Racial or ethnic origin	X	Political opinion		Religious or philosophical beliefs	X					
	Trade Union membership		Physical or mental health or condition	X							

	Sexual life or sexual orientation		X		Social service records		X		Child protection records			X
	Sickness forms	X		Housing records	X		Tax, benefit or pension records	X		Adoption records		
	DNA profile			Fingerprints			Biometrics			Genetic data		
	Proceedings for any offence committed or alleged, or criminal offence record											X
	Other data *(Please state):*						• Details of incidents and encounters that relate to criminogenic needs including those that affect safeguarding, risk and vulnerability (redacted if required). • Vulnerable Persons reports (MERLIN in London)					
	Will the dataset include clinical data? (please include)										**Yes**	
											Yes	
	Will the dataset include financial data?										Yes	
	Description of other data processed/shared/viewed?											
	Clinical data may be required for evidence.											

2.3	**Business sensitive data**		
	Financial	No	
	Local Contract conditions	No	
	Operational data	No	

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

Step 3: Describe the sharing/processing			
3.1	**List of organisations/partners involved in sharing or processing personal/special categories personal data?** *If yes, list below*		Yes/No
			Yes
	Name	Controller or Processor?	Completed and compliant with the IG Toolkit or Data Security and Protection (DSP) Toolkit
			Yes / No
	London Local Authorities	Controller	Yes
	Metropolitan Police Service, British Transport Police & City of London Police	Controller	Yes
	National Probation Service	Controller	Yes
	Local health partner (including GPs, clinics etc.)	Controller	Yes
	London CCGs	Processor	Yes
	Department for Work & Pensions (inc Job Centre Plus)	Controller	Yes
	London Ambulance Service	Controller	Yes
	Local substance misuse partner	Controller	Depends on how constituted; mixed
	Local housing partner if ALMO	Controller	Depends on how constituted; mixed
	Local voluntary groups	Controller	Depends on how constituted; mixed
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 ISA includes statements on flows, but in general data is shared with partner representatives; actual flows are based on need.
3.4	**Does the project involve employing contractors external to the Organisation who would have access to personal or special categories of personal data?** *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)*	
	To provide an effective IOM scheme in order to reduce reoffending and protect the public from harm. The information shared using this agreement will allow partners to provide the best range of services to IOM clients whilst addressing	

	any continuing offending or anti-social behaviour.

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(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; Article 6 1(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of		Data Protection Act section 8. The applicable laws are given at Appendix C of the ISA and the legislation provide for each party a legal basis under section 8 Some of the bodies are competent bodies for law enforcement, and their 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		The Mental Health Act 1983[1] and the Mental Health Act Code of Practice[2] The Localism Act 2011[3] The Education Act 2002[4] The Children Act 1989 The Children Act 2004 The Children & Social Work Act 2017[5] The Mental Capacity Act 2005[6] The Health and Social Care Act 2012[7]	

[1] https://www.legislation.gov.uk/ukpga/1983/20/contents
[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435512/MHA_Code_of_Practice.
[3] https://www.legislation.gov.uk/ukpga/2011/20/contents
[4] http://www.legislation.gov.uk/ukpga/2002/32/contents
[5] http://www.legislation.gov.uk/ukpga/2017/16/contents
[6] http://www.legislation.gov.uk/ukpga/2005/9/contents
[7] https://www.legislation.gov.uk/ukpga/2012/7/contents

	official authority vested in the controller		of criminal penalties, including the safeguarding against and the prevention of threats to public security".		FGM Mandatory Guidance[8] Working Together to Safeguard Children 2018 and London Child Protection Procedures 2018[9] (provides the appropriate policy document) NHSE Safeguarding Vulnerable People in the NHS – Accountability and Assurance Framework 2015 [10]	
	Special Category Personal Data Sharing					
	Article 9 2(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; Article 9 2(g) substantial public interest - processing is necessary for reasons of		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			

[8] https://www.gov.uk/government/publications/mandatory-reporting-of-female-genital-mutilation-procedural-information
[9] http://www.londoncp.co.uk/
[10] https://www.england.nhs.uk/wp-content/uploads/2015/07/safeguarding-accountability-assurance-framework.pdf

	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 Article 9 2(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 Article 10: Processing of personal data relating to criminal convictions and offences – Processing of personal data relating to criminal convictions and offences or related security measures		purposes under Para 6(1)(2) • Preventing and detecting unlawful acts under Para 10(1)(2)(3) Safeguarding children and individuals at risk under Para 18(1)(2)(3)(4) Use of Article 9 2(h) requires that the Data Protection Act Section 10(2) be satisfied. This requires that a condition within Schedule 1, Part 1 is met. 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 Data Protection Act 2018 Schedule 1			

	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. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.		PART 1 Health or social care purposes 2(1) This condition is met if the processing is necessary for health or social care purposes. (e)the provision of social care PART 2 Substantial public interest conditions Requirement for an appropriate policy document when relying on conditions in this Part. 5(1)Except as otherwise provided, a condition in this Part of this Schedule is met only if, when the processing is carried out, the controller has an appropriate policy document in place (see paragraph 39 in Part 4 of this Schedule). (2) See also the additional safeguards in Part 4 of this Schedule. Statutory etc and government purposes 6(1) This condition is met if the processing—			

			(a)is necessary for a purpose listed in sub-paragraph (2), and (b)is necessary for reasons of substantial public interest. (2) Those purposes are— (a)the exercise of a function conferred on a person by an enactment or rule of law; Preventing or detecting unlawful acts 10(1) This condition is met if the processing— (a)is necessary for the purposes of the prevention or detection of an unlawful act, (b)must be carried out without the consent of the data subject so as not to prejudice those purposes, and (c)is necessary for reasons of substantial public interest. 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.			

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. Personal information should be shared on a 'need to know' basis only, and only the minimum amount of information required for the task at hand should be shared. 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, in general notify individuals about the processing of their information. However, In some cases, it may not be appropriate to let a person know that information about them is being processed and shared. Consideration should be given to whether notifying the individual may place someone at risk or prejudice a police or safeguarding investigation. In these circumstances, the parties need not inform individuals that the information is being processed/shared; but should record their reasons for sharing information without making the individual aware. The applicable sections of DPA are Schedule 2 Part 3 s.17 and, for law enforcement bodies only, Schedule 8 s.4	
4.5	**How will you help to support the rights of individuals?**	
	Full details are provided in the ISA – 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. See para 4.1 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 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?*	
	Organisations are required by data protection legislation to document processing activities for personal data, such as what personal data is held, where it came from and with whom it has been shared. This Record of Processing Activity (ROPA) must include the retention period for the data. Information must not be retained for longer than necessary for the purpose for which it was obtained. Disposal or deletion of personal data once it is no longer required, must be done securely with appropriate safeguards, in accordance with that organisation's disposal policies.	
4.12	**Will this information be shared/processed outside the organisations listed above in question 3?** *If yes, describe who and why:*	Yes/No
	There may be a need to share information with other 3rd Parties, for example, another Council. This is covered within the lawful 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. 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 (Role-based Access Control) is required with password access as minimum.	
5.3	**What roles will have access to the information?** (list individuals or staff groups)	
Social care and health care professionals; community safety teams; police; probation service; voluntary organisations providing services.		
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			
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	High	Medium
Voluntary sector organisation not having DSPT certification in some cases may lead to risks	Medium	High	Medium
Complexity of system may lead to missed opportunities to protect victims/other 3rd Parties	Medium	High	Medium

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**

Wider sharing increases risk of disclosure to inappropriate persons	Training and appropriate policy. Data minimisation, sharing only what is needed.	Reduced	Low	Yes
Voluntary sector organisation not having DSPT certification in some cases may lead to risks	Data minimisation, ensure only needed sharing is done. Appropriate policy document. Storage to be minimised	Reduced	Low	Yes
Complexity of system may lead to missed opportunities to protect victims/other 3rd Parties?	Training and publicity to all organisations. Ensuring that sharing in each area is closely managed by responsible social care department.	Reduced	Low	Yes

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**

Measures approved by:		
Residual risks approved by:		
DPO advice provided:	Andrew Bessant Richmond and Wandsworth IG Manager	
Summary of DPO advice: The working group IG representatives collaborated on and were happy with this DPIA, with the lead DPO being Richmond and Wandsworth. The DPIA is recommended to all partners. Partners are responsible for their own DPIA and may choose to adopt this DPIA with or without amendment or to produce their own.		
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 shall be prohibited.

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, the controller or the specific criteria for its nomination may be provided for 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. *Direct Care* - means clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals (all activities that directly contribute to the diagnosis, care and treatment of an individual).
8. 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.
9. 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.
10. *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 identifiable data.