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. **You should only complete this full DPIA where you have been told that one is required by the Information Rights Team or the Data Protection Officer.** If you have not been asked to do a full DPIA please do the pre-screen first. Search on essentials for 'DPIA' and download the DPIA pre-screen.

A DPIA is a legal requirement therefore please complete the form in as much detail as you can so the council has the necessary assurances of data protection legal compliance. Avoid technical language and jargon, and assume little prior knowledge of your subject and project by readers.

Ethics screening: If you have been advised to proceed straight to a full DPIA please complete the ethics screening at the end of this document. If you have already completed a DPIA pre-screen then the ethics screening need not be duplicated.

Project Name	MOPAC Safe Accommodation – Domestic Abuse Navigators	
Project Lead and Information Asset Owner/s	Project Lead	[redacted] and [redacted]
	IAO name and asset	Becca Dove, Mosaic
Summary of the project. *Outline what your project is about. Start with a general headline and then go into more detail. Explain any acronyms on first use.*	Through MOPAC, we have been successful for a funding bid through to support domestic abuse victims into safe accommodation. Our successful bid has been focused on domestic abuse navigators, to provide holistic and wrap around support to domestic abuse victims. A team of 6 domestic abuse navigators will work with a small case load of clients to work to provide wrap around and intensive support to them. This could be around their mental health, their child's school or some of the longer-term domestic abuse effects that they are experiencing.	
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	May/June 2022 (TBC on funding conditions as funding announcement has been delayed)	

Initial risk assessment: Screening questions are to do an initial risk assessment and highlight problems that need to be addressed. Answering "Yes" to any of the screening questions above represents a potential privacy/data protection/security risk factor.

If you have already completed a pre-screen, attach it to the DPIA, skip q1 and go to q2 otherwise please answer the questions below.

Q 1	Step 1: Initial Risk Assessment	Yes/No
1.1	Does the project introduce new or additional information technologies that have privacy implications? (like facial recognition, AI?)	No
1.2	Will there be large scale systematic monitoring in a publicly accessible place – like a new CCTV system	No
1.3	Will you use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?	No
1.4	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Mosaic ref, Northgate ref, and/or will use intrusive identification or identity management processes and/or electronic linkage of personal data?	No
1.5	Might the project cause data that was previously anonymous or pseudonymised (where a code is used instead of eg names) to become identifiable ?	No
1.6	Does the project involve multiple organisations, eg public sector agencies eg joined up government initiatives, or private sector e.g. outsourced service providers/ business partners?	No
1.7	Does the project involve new processing or significantly change the way in which personal data/special categories of personal data is handled?	Yes
1.8	Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	Yes
1.9	Will data be combined, compared or matched from multiple sources?	No
1.10	Will you process biometric (finger print /facial recognition) or genetic data?	No
1.11	Will the personal data be processed out of the U.K? Eg any provers have out of UK servers?	No
1.12	Will children's personal data be processed for profiling or automated decision-making or for marketing purposes, or offering online services directly to them?	No
1.13	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	No
1.14	Will personal data be processed in a way which involves tracking individuals' online or offline location or behaviour?	No
1.15	Will personal data be processed which could result in a risk of if there was a security breach?	Yes
1.16	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	No

Step 2: What personal data is being used?									
2.1	**Is this use of personal data/special categories of personal data a new use? Or is it already happening and this is a change?**					New/Changed			
2.2	**What data will be processed/shared/viewed?**								
	Personal Data								
	Name	**YES**	Date of Birth	**YES**	Gender	**YES**	National Insurance Number	**NO**	Financial Information about the person	**YES**
	Address	YES	Email address	YES	Telephone number	YES	NHS No	NO	Other eg a reference number such as Mosaic ref	YES
	Other data *(Please state):*									
	Special Categories of Personal Data									
	Racial or ethnic origin	Yes	Fingerprints/ Biometrics		Religious or philosophical beliefs Political opinion					
	Trade Union membership		Physical or mental health or condition							Yes
	Sexual life or sexual orientation	x	Housing records Social services records		Tax, benefit or pension records		Employee/HR records			
	Other data *(Please state):*									
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?	Where criminal offence data is processed, we meet the article 10 requirements by the Article 6 legal basis above, and the DPA18 schedule 1 condition is para 18, Safeguarding of children and individuals at risk. Survivors who are in touch with the service might disclose details of offences against them, and perpetrator names.								

Step 3: Describe the data processing			
3.1	**Describe in as much detail what is being done with the data - how is the data being used, how it is being handled, stored and transferred/shared?**		The data is client data, relating to their personal information and case notes to allow domestic abuse navigators to support victims with their case. The data will be stored on Mosaic – it will not be transferred or shared. It will be viewed only by domestic abuse navigators team.
3.2	**Explain in as much detail as possible why this is being done**		We will be providing a domestic abuse navigator service to provide holistic and wrap around support to domestic abuse victims in Camden. This will require us to process personal data about the clients to allow us to deliver this service. The domestic abuse navigators service will provide support to victims of domestic abuse with multiple disadvantages and additional needs. The service will provide holistic support, and workers will be outreach workers based in the community and visiting survivors near their homes and locations that they visit. The workers will have small caseloads, enabling them to support survivors who find it harder to engage with mainstream services and advocate for them.
3.3	**Are you sharing the data with an external organisation or partner or are they involved in processing the data?**		No, only aggregate level data
	External organisation or partner Name	**Controller or Processor?**	**Is there an existing contract or Data Sharing Agreement between the council and the parties which covers information security and data protection ? Yes/No/In progress**
	MOPAC	Data Controller	Yes
3.4.	**Has a data flow mapping exercise been undertaken? If yes, please provide a copy, if no, please undertake**		Yes and attached
3.5	**How will the information be processed/shared. Details eg secure file transfer**		**On Mosaic secure database**

<table>
<tr><th colspan="4">Step 4: Assess lawful basis, necessity, and proportionality</th></tr>
<tr><td>4.1</td><td colspan="3">Identify Lawful Basis for processing personal data/special category /criminal data. Ask IRT for advice if needed (DPA@camden.gov.uk if you have no named Information Rights Officer advising)
If not processing the category say N/A</td></tr>
<tr><td></td><td>Personal data Article 6(1) UK GDPR condition

Art 6(1)(e) public task, and The processing is necessary to perform a task in the public interest around keeping victims of domestic abuse safe. The service will also help to protect the lives of victims of domestic abuse and to reduce the risk that they are experiencing.

.</td><td>Special Category data UK GDPR Art 9 condition and DPA18 schedule condition

Art 9((g) Reasons of substantial public interest (with a basis in law). The Part 2 of Schedule 1 of the DPA 2018 condition is para 18, Safeguarding of children and individuals at risk, with the underpinning law being the Children Acts and the Care Act.</td><td>Criminal data UK GDPR Art 10 condition and corresponding art 6 condition

Where criminal offence data is processed, we meet the article 10 requirements by the Article 6 legal basis in the first column, and the DPA18 schedule 1 condition is para 18, Safeguarding of children and individuals at risk</td></tr>
<tr><td rowspan="2">4.2</td><td colspan="3">If consent is a legal basis how is it obtained? Note that in most cases consent is not the basis relied on by the council. Only use consent when Information Rights Team have advised this is appropriate</td></tr>
<tr><td colspan="3">N/a</td></tr>
<tr><td rowspan="2">4.3</td><td colspan="3">How will you ensure data quality and data minimisation- how will you ensure the data is accurate and you are only using the minimum data to achieve your aims? If this is covered in a pre-screen refer to the pre-screen, otherwise detail below</td></tr>
<tr><td colspan="3">We will ensure data quality and reliability of data by only processing data that we have received from victims and staff. We will not use any existing data sources which may have inaccuracies or historic or out of date information on clients. We will ensure that we only process the data that is necessary and proportionate through a number of ways. The domestic abuse navigators when they start will be required to do GDPR mandatory training, ensuring that they understand the requirement to only process data which is necessary and proportionate. In addition to this, any requests for further data analysis and processing will need to be discussed and approved by the project team [redacted], VAWG Lead, [redacted] Policy Designer, [redacted], Head of Housing Needs, [redacted], Housing Commissioning and Partnerships Manager and [redacted], Strategy and Commissioning Manager).</td></tr>
</table>

4.4	**Have individuals been informed about the proposed use of their data?** For example, do all the organisations/partners who will process the data (inc the council) cover this use in their Processing Notice online	Yes
4.5	**Will you comply with the council's policies on to Subject Access Requests and other data subject rights? Do contracts with any processors for the council contain the council's clauses on data subject rights?**	
	Yes	
4.6	**Will the processing of data include automated individual decision-making, including profiling?** If yes, please outline the profiling processes and the rights of the data subject	
	No	
4.7	**Data Retention Period - how long will the data be kept?**	
	For the duration of the project – currently 2 years, until June 2024.	
	Step 5: Information Security Process	
5.1	**On what systems 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.*	
	The data will be recorded on spreadsheets and word documents that will be stored in a protected folder on Camden's server only accessible by the Navigators team. The data will also be captured on the MOSAIC case management system in a separate environment from other services using MOSAIC. We are awaiting further information about performance monitoring data we need to submit to MOPAC but this will be aggregated data. Aggregated data which is required to be submitted to MOPAC as part of the grant agreement will be stored on share point, securely with limited individuals having access to this.	
5.2	**Where is the data stored geographically?**	
	In the UK	
5.3	**What roles will have access to the information?** (List individuals or staff groups)	
	Caitriona Scanlan Domestic Abuse Navigators Lead	

	Administrative staff member (TBC)
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**
	There is RBAC enforced on Mosaic with audit capabilities
5.5	**Is there an ability to audit access to the information?**
	Yes
5.6	**What security and audit measures have been implemented to secure access to and limit use of personal data/special categories data and/or criminal data?**
	Personal data will be limited and special categories data will be limited. Only set individuals will have access to the data. There is RBAC enforced on Mosaic with established polices and protocols.
5.7	**Has the Information Security Manager advised on the security measures? What were his/her comments?**
	Not necessary as established system being used in line with existing protocols.

Step 6: Identify and Assess Risks			
Describe source of privacy (data protection, privacy and information security) risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. **These are the risk *before* any controls (mitigations are applied).** Assess risk assuming there are no controls in place- controls/mitigations are discussed in the next step. **Use tables 1, 2 and 3 in the appendix to help you.** *Note that risks and scores are subject to review and change by IRT/DPO*	**Likelihood of harm- see table 1**	**Severity of harm- see table 2**	**Overall risk – see table 3**
Misuse of data; Personal data could be used in a manner incompatible with the project aims which would be privacy	Medium	High	Medium/high

intrusive to the data subject and may be processing they would not expect to occur. Compliance risk: could be a breach of purpose limitation and transparency Corporate risk: Reputational risk. Loss of trust from data subjects and the partners providing the data. Legal implications.			
Privacy Intrusion – sensitive data being shared internally or externally with people that did not need this information (did not need to know) or unintended third parties (should not know). Compliance risk: unrestricted control of the data to parties beyond the scope of this assessment and understanding of what is/is not legally processable. Corporate risk: breach of GDPR legal processing, legal risk and loss of trust of data subjects. Increased risk to data subject if information shared with third party	Medium	High	Medium/High
Misuse of data – data is shared with other teams or third parties for reasons other than it is being legally processed. Compliance risk: services/teams having access to information on data subject and using this for reasons other than protecting them from domestic abuse. Corporate risk: breach of GDPR legal processing, risk from any appeals or legal challenges e.g. ombudsman. Services using information and taking steps using information that should not have been shared for that reason. There also is a risk with data on survivors being misused and shared either advertently or inadvertently, verbally or electronically, with their perpetrators of domestic abuse or other individual which creates safety concerns and risks for victims of domestic abuse.	Medium	High	Medium/High
Data collection – data not collected and processed in line with this risk assessment. Not fully understanding or using the incorrect GDPR basis for the processing of these data. Compliance risk: data subjects are not informed or misinformed about the reasons for collecting this data. Corporate risk: data subjects challenge the council if they do not feel that their data is processes correctly. Scrutiny from ICO.	Unlikely	High	Medium/high
Data Breach – data is lost or sent to unauthorised parties e.g. members of the public or internal officers who do not need to see it. Compliance risk: Officers/data handlers making mistakes or not taking correct steps to minimise this risk. Corporate risk: Data subject challenges the organisation around data breach. Scrutiny/fines from ICO.	Medium	High	Medium/High

Step 7: Identify Measures to reduce risk

Identify measures to reduce or eliminate risks identified in step 6. *Remember that risks need to be reduced to an acceptable level, and not all risks can be eliminated.*

Then calculate the risk that remains after the mitigations/controls are in place: the residual risk. Tables 1, 2 and 3 will help with this. *Note that risks and scores are subject to review and change by IRT/DPO*

The Information Asset Owner/s need to decide if the mitigations are achievable and if the residual risk is accepted in the 'measure approved?' column by inserting a Yes or No. Table 4 provides guidance on what level of residual risk could be acceptable.

Risk identified in step 6	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved?**
Privacy Intrusion	Only named staff members including the Navigators, service managers, and analysts will have access to individual level data held on Mosaic and in protected folders. Given the sensitive nature of domestic abuse ,the Team Leader will emphasise to staff the importance of not sharing this data. The service will be advocating for victims, and therefore will keep up a level of independence. This will mean that data will not be shared with other services as a matter of practice to ensure the safety of survivors.	Reduced	Medium	Yes
Data Misuse	Only named staff members will have access to the Mosaic data system. Staff members who have access to the Mosaic data on clients supported by DA Navigators will be reviewed by the core project team [redacted] to ensure that only staff who require it have access to reduce data misuse. The job profile for these new roles will also highlight the importance of GDPR and following data protection laws to ensure that postholders have demonstrated a commitment to data privacy prior to being successful.	Reduced	Low	Yes
Data collection and usage	As part of their initial engagement with the service, clients will be informed by the domestic abuse navigators team of the Privacy Notice and data sharing agreement. This will ensure that clients are aware of the reasons for processing the data, and that domestic abuse navigators staff are regularly reminded of the importance of this.	Reduced	Low	Yes

Data Breach	All staff members will be required to do mandatory GDPR and security training, which highlights what counts as a data breach. In addition to this, as part of the induction process and within team meetings, examples of data breaches will be discussed. The council has existing policies and procedures around data protection and information security and appropriate handling. Compliance with these is a condition of employment and they are well embedded into the organisational culture.	Reduced	Low	Yes
Residual (remaining) risk level when all mitigations have been applied: ***Note IRT/DPO may change this***				
Medium				

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? **If not, name of IRO**	Sarah Laws, Data Protection Manager
DPO advice	Cleared April 2022
Information Asset Owner acceptance of residual risks	Names of IAOs
This DPIA will kept under review by: *(usually the author or the IAO)*	[redacted], Policy Designer [redacted], VAWG Lead

Version Control

Version	Reason	Date	Author(s)
1.0	**New draft**	**April 2022**	[redacted]
1.1	**DPAT comments**	**April 2022**	**Sarah Laws**
1.2	**Updated with minor changes not affecting risk rating**	**May 2023**	[redacted]

Appendix 1

Risk Assessment Tables

Table 1 Likelihood of Risk Occurring

Rare	One-off failure
Unlikely	Possible that it may reoccur but not likely
Possible	Might happen or reoccur on a semi-regular basis (no more than once a quarter)
Likely	Will reoccur on a regular basis, pointing to some failure in controls
Almost Certain	Willful act, systemic failure in controls

Table 2 Impact of Risk if it occurs

Negligible	No personal data involved, or risk won't have any impact.
Minor	• Short-term, minimal embarrassment to an individual • Would involve small amounts of sensitive personal data about an individual • Minimal disruption or inconvenience in service delivery to an individual (e.g. an individual has to re-submit an address or re-register for a service)
Moderate	*More than a minimal amount of sensitive personal data is involved at this level* • Short-term distress or significant embarrassment to an individual or group of individuals (e.g. a family) • The potential of a financial loss for individuals concerned • Minimal disruption to a group of individuals or significant disruption in service delivery or distress to an individual (e.g. availability to a set of personal information is lost, requiring resubmission of identity evidence before services
Major	Significant amount of HR, or resident personal, and / or sensitive data released outside the organisation leading to significant actual or potential detriment (including emotional distress as well as both physical and financial damage) and / or safeguarding concerns
Catastrophic	Catastrophic amount of HR or service user personal and or sensitive data released outside the organisation leading to proven detriment and / or high-risk safeguarding concerns. Data subjects encounter significant or irreversible consequences which they may not overcome (e.g. an illegitimate

	access to data leading to a threat on the life of the data subjects, layoff, a financial jeopardy)

Risk Assessment: Table 3 - risk level

IMPACT	Score:	PROBABILITY				
		Rare	Unlikely	Possible	Likely	Almost Certain
	Catastrophic	5	10	15	20	25
	Major	4	8	12	16	20
	Moderate	3	6	9	12	15
	Minor	2	4	6	8	10
	Negligible	1	2	3	4	5

Table 4: is the risk level acceptable?

Level of risk	
1-3 Low Risk	Acceptable risk No further action or additional controls required Risk at this level should be monitored and reassessed at appropriate intervals
4-6 Moderate Risk	A risk at this level may be acceptable, if so no further action or additional controls required If not acceptable, existing controls should be monitored or adjusted
8-12 Medium / High Risk	Not normally acceptable Efforts should be made to reduce the risk, provided this is not disproportionate Determine the need for improved control measures
15-25 High Risk	Unacceptable Immediate action must be taken to manage the risk A number of control measures may be required

Appendix 2: Ethics screen.

Only complete this if you have skipped the DPIA pre-screen and proceeded straight to a full DPIA. If you did the ethics screen as part of the DPIA pre-screen ignore this section.

Ethical Assessment. In assessing ethics you need to take into account the benefits, proportionate use, possible biases and transparency of the impact of the proposed processing and analysis of personal data on individuals and groups. It is the responsibility of the Project Manager and Sponsor to assess the potential ethical impacts that the intended processing may pose. (These answers can be reused for questions dealing with the same issues in the Full DPIA if the outcome of this pre-screen requires you to do one) This will be a link to Camden's Data Charter but this does not exist yet

1. *Effects on Residents* a) *How does use of this data benefit our residents? (Is there evidence of this approach being likely to meet a public need?)* • b) *What would be the harm in not processing this data?* •
2. *Data Bias* a) *How do you plan to identify errors and biases in data collection, analysis and algorithms?* • b) *Once errors and biases have been identified in data collections, how will they be taken into account for any future policy or service which uses this work as an evidence base?* • c) *Who could be negatively affected by processing this data?* (How can you show there is a **fair balance** between the **rights of individuals** and the **interests of the community**? •
3. *Limitations of Data* a) *How will you make sure that you only process the data that is necessary and proportionate for the purpose of the project, and no more than is necessary?* • b) *How are you ensuring the data used is reliable? (**Data quality**)* i) *What processes do you have in place to ensure maintenance of data accuracy? (**Data integrity**)*

-

ii) *How have you clearly marked origins and destinations of data used to trace source of errors? (**Data lineage**) (Are all metadata and field names clearly understood)*

-

d) *How could the objectives of this project be completed without processing the data?*

-