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	**Domestic Abuse – multi-disciplinary team approach**	
Project Lead and Information Asset Owner/s	Project Lead	[redacted]
	IAO name and asset	Landlord Services – Angela Spooner (LWP) Housing Needs Group – Shaun Flook (HNG database) Camden Safety Net – Caitriona Scanlan (Mosaic)
Summary of the project. *Outline what your project is about. Start with a general headline and then go into more detail.* E*xplain any acronyms on first use.*	**Taking a multi-disciplinary team (MDT) approach to supporting people experiencing domestic abuse** This piece of work is building on the current practices of the services involved. It's acknowledged that in relation to domestic abuse cases there are typically multiple services involved. No one service has the complete picture or context and best practice is for services to take a multi-disciplinary approach (e.g. MARAC, child protection conferences, Early Help panels). Work has shown that this picture is built up piecemeal over a prolonged period of time, usually by email. This has led to services having an incomplete understanding of how to support survivors of domestic abuse and leads to poorer decision making. It also means that support workers are working in isolation from each other which increases risk to the survivor and can lead to re-victimisation as the survivor has to interact with each service individually. This piece of work seeks to bring together the professional network of support for individual cases (starting with housing tenants experiencing abuse) for a facilitated discussion to understand the survivor and agree supporting strategies. The domestic abuse Multi-Disciplinary Team (MDT) brings together managers and decisions makers in those services to support their front-line workers to provide the best support. The MDT meet once a week for two hours to discuss cases. The meeting is facilitated by an	

	independent Council facilitator. Consideration is given to understanding the person experiencing abuse and any risk factors. Relevant information is shared between the professional support network in the meeting in order to protect people from harm and to help them lead a good life. Notes and actions from the meeting are recorded in writing electronically and stored on a restricted council system. We've trialed 12 weeks of this work and have had very positive results in regard to decision making and providing bespoke support quicker. We'd like to continue with this as we have a backlog of cases awaiting discussion. The survivor of domestic abuse will still get support if we wait to resume this approach but it's likely to be less effective.
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	Currently the professional network carry out this support work on a day to day basis. However, this can be reactive and done over email without the ability to think collaboratively. We have trialled the MDT approach and now want to make it a permanent way of working.

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 have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	No
1.6	Does the project involve multiple organisations, eg public sector agencies like joined up government initiatives, or private sector e.g. outsourced service providers/ business partners?	Yes
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?	No
1.9	Will data be combined, compared or matched from multiple sources?	Yes
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?	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 physical harm in the event of 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			
							Yes, personal data/special category data is already legally processed by the home services providing the support and shared with relevant partner agencies e.g. MARAC, Police etc. The MDT uses this data in a different way by sharing it at an earlier stage and in the context of the person/family situation. This allows all professionals to understand the people they are supporting and mean it is less likely that important facts are missed. This reduces risk.				
2.2	**What data will be processed/shared/viewed?**									
	<u>Personal Data</u>									
	Name	**Yes**	Date of Birth	**Yes**	Gender	**Yes**	National Insurance Number	**No**	Financial Information about the person	**Yes**
	Address	Yes	Email address	No	Telephone number	No	NHS No	No	Other eg a reference number such as Mosaic ref	No
	Other data *(Please state):*			*The persons context is shared and discussed. This includes how details of any abuse they have reported and any allegations they are making in regard to the person using abuse. Other contextual information is shared including the make-up of the family (where applicable), their housing situation, their support networks.*						
	<u>Special Categories of Personal Data</u>									
	Racial or ethnic origin	Yes	Fingerprints/ Biometrics	*No*	Religious or philosophical beliefs Political opinion					*Yes*
	Trade Union membership	No	Physical or mental health or condition							Yes

	Sexual life or sexual orientation	Yes	Housing records Social services records	Yes	Tax, benefit or pension records	Yes	Employee/HR records	No
	Other data *(Please state):*		In order to provide the right support, the professional network will discuss the ethnic and cultural background of the person they are supporting. It may also include reference to their religion or connection with supporting factors like church etc. Where necessary health information (including mental health) will be discussed for example when considering rehousing decisions or suitable temporary accommodation. The person's financial situation will also be considered to ensure that they are claiming the financial support to end the abuse e.g. housing benefit and also that they are not experiencing any financial abuse.					
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?		All records relating to criminal offences are legally processed by the home services involved. The approach allows for professionals to share (where appropriate) any risk assessments which in the case of domestic abuse will likely detail allegations of abuse. The MDT discussion will mark where allegations are being made about abuse by the victim and where factually any alleged perpetrator has been arrested, the police have been called or where the person has been charged or convicted. This data is only recorded and stored as part of the discussion notes.					

Step 3: Describe the data processing		
3.1	**Describe in as much detail what is being done with the data**	All data is legally processed and owned by the respective home services and covered under their processing arrangements. Lead officers in their home services will refer cases to the MDT facilitator by Council email. This referral will typically contain the name and address of the person experiencing abuse. The MDT facilitator will email the other professionals who are supporting that person or family (professional network) to arrange a date for the multi-disciplinary discussion. This email will also contain the name and address of the survivor. A meeting invite is sent to everyone attending that meeting but this contains no details of the case Prior to the agreed meeting the MDT core members and guest professional network will be contacted as a group by Council email to confirm that the meeting is taking place and the time slot for the discussion. This email contains the name and address of the case to be discussed. Any external agencies where there is not an existing data sharing agreement in place will be asked to observe a document detailing the reasonable expectations on which the Council is sharing the data as part of the MDT (as provided by the data management team). The meeting takes place virtually on Microsoft Teams over the Camden network. Each case is discussed for one hour. The professional network is invited to detail their experience of working with the person/family and to share any actions they've taken and what challenges remain in helping them to be safe. This involves detailing any abuse that they have suffered and any impact to the person or children. MDT core members can ask questions to gain further clarity. The group will finish the discussion offering advice and agreeing actions for support. The facilitator will take notes on the discussion contemporaneously. Following the discussion, the facilitator will type up the notes on a MS Word document. These

		notes contain the name and address of the person and a description of the case discussion and any agreed actions. These notes are saved in a secure MS Teams channel and access granted by a link sent to only the professional network and anyone who has an action. It is accompanied by the instruction not to share these notes for any other reason than to support the person to be safe from domestic abuse. Each case discussion does result in notes from the meeting which detail the context of the case, the professional considerations for support and any agreed actions. These notes are a record of what was discussed and agreed and will ensure a continuity of support if personnel leave. They may also be used for other reasons to support the person regarding accessing services. For example, where a direct offer of a council tenancy has been agreed these notes constitute why this has been done and what considerations were taken into account. The original notes are currently stored on the facilitators secure MS one drive. An MS Teams site has been set up for these notes and once transferred, access to this will be shared with two other facilitators ([redacted]).
3.2	**Explain in as much detail as possible why this is being done**	These notes are recorded so that there is clarity about what was discussed and how the support was agreed upon. Without these notes there would be no record of the case discussion. They have also been used to provide the relevant information for accessing certain services e.g. rehousing decisions, housing allocations points.

			These notes can also form part of reviewing and understanding risk over time. Not recording these notes would mean that support would remain fragmented and provided locally without greater understanding of all the citizen's needs. This approach minimises the need for case discussion over email and reduces the amount of information stored on local systems.
3.3	**Are you sharing the data with an external organisation or partner or are they involved in processing the data?**		Yes, mainly with Police and Health providers
	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**
	C&I NHS Trust	Controller	Yes
	Camden Schools	Controller	Yes
	Police	Controller	Yes
	Local Health Partners (including GPs, clinics etc)	Controller	Yes
	London CCGs	Processor	Yes
	National Probation Service	Controller	Yes
	Local Housing Partners e.g. housing associations etc	Controller	Yes (as and when needed)
	Local Voluntary Groups	Controller	Yes (as and when needed)
3.4.	**Has a data flow mapping exercise been undertaken?** **If yes, please provide a copy, if no, please undertake**		Yes (see appendix 1)

3.5	**How will the information be processed/shared. Details eg secure file transfer**	The information is held securely in the home services case management systems under their local arrangements. Notes of the case discussion are only shared to the professional network over internal email (Outlook). Any emails sent to partners without secure emails are sent via Egress.

Step 4: Assess lawful basis, necessity, and proportionality			
4.1	**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**		
	Personal data Article 6(1) UK GDPR condition Art 6(1)(e) Public task: 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. <u>Requirement for data sharing</u> Prevention and detection of crime (s. 115 Crime and Disorder Act 1998). To protect vital interests of the data subject; serious harm or matter of life or death (Schedule 8, DPA 2018) For the administration of justice (Part 3 & Schedule 8 DPA 2018) For the purposes of the prevention, investigation, detection or prosecution of	**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). DPA18 – Schedule 1, Part 2, para 6 (health and social care purposes), para 10 (preventing and detecting unlawful acts) and para 18 (safeguarding of children and of individuals at risk) <u>Requirement for data sharing</u> See previous	**Criminal data UK GDPR Art 10 condition and corresponding art 6 condition** DPA18 – Schedule 1, Part 2, para 6 (health and social care purposes), para 10 (preventing and detecting unlawful acts) and para 18 (safeguarding of children and of individuals at risk) Legal basis for processing: public task <u>Requirement for data sharing</u> See previous

	criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (Part 3 s.31 & 35 DPA 2018) Child protection. Disclosure to Children's Social Care or the Police (Children's Act 1989 & 2004) Overriding public interest (Common law) Right to life Right to be free from torture or inhuman or degrading treatment (Human Rights Act, Articles 2 & 3) Prevention of Abuse and Neglect (The Care Act 2014)		
4.2	**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 Tights Team have advised this is appropriate**		
	N/A		
4.3	**How will you ensure data quality and data minimisation?** If this is covered in a pre-screen refer to the pre-screen, otherwise detail below		
	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 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?**
	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.
	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 discussion notes are held on a secure MS Teams area that. The administrative permission for that team is held by three Camden officers [redacted] Complex Families Manager, [redacted] Independent Domestic and Sexual Violence Advocate and [redacted], Organisational Designer). The information is held in a secure Teams channel and the data is only shared with the professionals for reasons details in this document e.g., keeping someone safe from domestic abuse. Permission to access the document is given to these named individuals and a link to the document will be emailed to them. Permission to download, share or edit the document is not given.
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)

	The facilitators of the MDT ([redacted] - Organisational Designer – HR team & [redacted] Service Manager, Complex Families). The relevant professional network for each case e.g. Neighbourhood Housing Officer, Independent Domestic Abuse Advocate, Social Worker). Any person in the MDT who agrees an action e.g. Housing Service Placements Manager (for housing allocations decisions). Access to this information can be revoked through the permissions e.g., if someone leaves.
5.4	Is there role based access control on all applicable systems? **How will access to information be controlled?**
	The facilitators don't have specific access as part of the project to any additional systems. Information is only shared verbally and recorded as part of the notes. Professional network don't have access to any new systems as part of this work but retain access to their home systems as part of the day to day work. Any information shared with the MDT members is part of their day-to-day job and part of any pre-existing decision-making processes e.g. agreeing direct offers for rehousing. MDT discussion notes are held in a managed MS Teams channel. Permission for these files within this channel is managed by three site owners and will be granted on an individual case basis e.g. professionals support that case will be granted access to the single discussion notes document. Access can be revoked by the administrators at any time.
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?**
	All data is recorded legally for processing as detailed in part 4.1. Data is held securely and not shared beyond the professional network. All data is held on secure Council systems.
5.7	**Has the Information Security Manager advised on the security measures? What were his/her comments?**

	The Information Security Manager has been consulted as part of preparing this DPIA and has contributed to the measures taken and is supportive of the specifics contained in this assessment.

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* Add in additional rows as necessary. *The completed row is an example. Please delete it when you submit the DPIA*	**Likelihood of harm- see table 1**	**Severity of harm- see table 2**	**Overall risk – see table 3**
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.	Possible	Moderate	9 - Major
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.	Possible	Major	12 - Major

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 e.g. dealing with ASB/eviction etc.			
Data sharing with third parties – data shared with third parties which is not controlled in line with this assessment. Third parties not storing or controlling the data in a secure and responsible way. Risks around access to this data. Compliance risk: data is access by unauthorised parties. Data is stored in such a way that it is easily accessible to people not permitted to access it. Corporate risk: As the data controller we have responsibility to ensure that all data is processed correctly by partners. Risk to data subject if information shared inappropriately.	Possible	Major	12 - Major
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	Major	8 - Major
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.	Unlikely	Catastrophic	10 - Major

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	The data from the MDT meeting is held on a secure Microsoft Teams channel. The data is not emailed directly to those that need it, but permission is granted to access the relevant document. This means that copies cannot be sent to third parties without the data controller's permission and knowledge. This document cannot be downloaded, edited, saved or shared without permission.	Reduced	3 - Negligible	Yes
Misuse of data	Data from the MDT is held in a secure Microsoft Teams channel and not saved onto local databases. This means that other teams/officers will not have access to it and therefore unable to use this data for any other reason. Any request for the data for legitimate and legal GDPR compliant reasons can be coordinated through the data handlers and any reason for granting access can be approved in line with this assessment.	Reduced	4 - Moderate	Yes
Data sharing with third parties	As the data is retained in a Microsoft Teams secure channel. Anyone the data is shared with will not be responsible for storing it. This means that it will be almost impossible for third parties to access it without significant effort and almost entirely reduce inadvertent casual access. Any sharing of these data can only be coordinated by the data handler.	Reduced	4 - Moderate	Yes

Data collection	The DPIA is being produced in collaboration with Camden's Information Rights team to ensure that it is GDPR compliant. Data handler has taken training on managing a secure Microsoft Teams channel. Other advice has been sought in regard to information management and retention. Steps, as above, have been taken to ensure data is controller responsibly.	Reduced	3 – Negligible	Yes
Data Breach	Through tighter controls of the data (as above), the chance of information being lost or breached is greatly reduced. The information only exists on a secure Microsoft Teams channel and can only be accessed by named individuals. Permissions can be removed if necessary, e.g someone leaves, or a new case officer is attached. The information cannot be downloaded, edited or shared.	Reduced	5 - Moderate	Yes
Residual (remaining) risk level when all mitigations have been applied: ***Note IRT/DPO may change this***				
Moderate				

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? **If not, name of IRO**	**No** **Sarah Laws, Information Rights Team Leader**
DPO advice	The risks of this processing are acceptable and proportionate compared to the outcomes sought Andrew Maughan DPO March 2022
Information Asset Owner acceptance of residual risks	Landlord Services – Angela Spooner (LWP) Housing Needs Group – Shaun Flook (HNG database)Camden Safety Net – Caitriona Scanlan (Mosaic)
This DPIA will kept under review by:	[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 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?)*

- This approach is there to safeguard vulnerable adults/children at risk of harm.

b) *What would be the harm in not processing this data?*

- The traditional method for case working has put people in high risk situations for longer than necessary.

2. *Data Bias*

a) *How do you plan to identify errors and biases in data collection, analysis and algorithms?*

- Each party 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.

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?*

- Any party learning of the inaccuracy of personal data is responsible for informing the parties with whom that data has been shared.

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**?

- The balance is based on the needs of the individual to be protected from harm. We get consent from survivors to discuss their cases in advance and explain what that means. Not sure that community interests are a consideration here.

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?*

- The case discussion is recorded. Details of the case are only discussed that are relevant with providing tailored support services to help survive and recover from domestic abuse. This document is only shared with the professional network who are supporting the survivor.

*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**)*

- The data is provided by the support worker based on the context of the survivor's situation. It is subjective by nature and we make an effort to record their story in a factual and non-judgemental way.

*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)*

- See above.

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

- No.