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	**Debt and Financial Stability**	
Project Lead and Information Asset Owner/s	Project Lead	[redacted], Senior Service Designer [redacted], User Researcher
	IAO name and asset	Kate Robertson (Director of Customer Services)
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.*	Millions in individual debt (e.g. rent arrears, council tax, parking, etc.) is owed to Camden Council; the levels of debt have risen significantly over the past few years, exacerbated by COVID. These levels are expected to continue to rise with the cost-of-living crisis. Our task is to understand whether individual debtors can be categorized based on certain key characteristics such as motivations, experiences, and/or pain points in engaging with Camden Council, to understand how we may best support them out of debt and towards financial security. Phase 1 of this project will aim to understand whether we have a shared perspective of these profiles within our organisation, among our subject matter experts (SMEs) across all services which hold debt. The key objectives from this stage are (a) to create a shared understanding within SMEs of the types of debtors we have at Camden; (b) to prioritise together the specific profiles we want to better understand; and (c) to create hypotheses of these profiles of debtors in terms of their identifiable characteristics, motivations, and experiences. The hypotheses of these prioritized profiles will be tested in Phase 2. A DPIA Pre-Screen has been submitted for this phase, and approved on November 14th, 2022 by Veron Reece-Jones. This Full DPIA is submitted for Phase 2 of this project, which aims to understand whether the hypotheses created by staff can be validated by interviewing individual debtors who fall within each of the prioritized profiles. 1-hour interviews will be conducted with personal debtors for this	

	phase, either virtually via MS Teams or phone, or in person, depending on the participant's preference. This project is sponsored by Kate Robertson (Director of Customer Services).
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	Monday, December 5th, 2022 – Start of Recruitment

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?	Yes – Please see section 3.1, part B for details
1.7	Does the project involve new processing or significantly change the way in which personal data/special categories of personal data is handled?	No
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?	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?	No
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			
							New			
2.2	**What data will be processed/shared/viewed?** Put a YES in the box as appropriate									
	Personal Data									
	Name	**Yes**	Date of Birth		Gender	**Yes**	National Insurance Number		Financial Information about the person	**Yes** ****
	Address		Email address	**Yes**	Telephone number	**Yes**	NHS No		Other eg a reference number such as Mosaic ref	
	Other data *(Please state):*	• Age • Camden residency status **Financial information: We would be interested in learning about the debtor's level of debt (to Camden), sources of debt, and level of financial resilience (e.g. not at risk of bankruptcy, at risk, or bankrupt); other information such as the debtor's other sources of debt (e.g. credit card debt) will not be asked directly, but may be disclosed voluntarily by the debtor in the course of the interview								
	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		Housing records Social services records		Tax, benefit or pension records		Employee/HR records			
	Other data *(Please state):*	We will not be collecting housing or social services records; however, we will be asking questions related to the participant's housing situation, benefits situation, and employment status, as these factors will paint a								

		more holistic picture of each person's situation, allowing us to better understand their unique life circumstances. We will not directly ask for any other special category data; however, we recognize that some participants may supply special category data by their own volition, if deemed relevant to their context. In these cases, we will record these pieces of information to ensure the participant's original meaning and contributions are preserved.
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?	As above, we do not intend to ask or to collect data on criminal offence; however, these may come up in conversation if supplied by the participant and deemed relevant to their context.

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? Please use plain English!**	We have created a diagram which outlines the entire participant experience, from recruitment to follow-up, to answer questions 3.1, 3.4, and 3.5. Please access the flow chart here: DPIA - Data Flow Mapping.pdf The top level of the diagram shows the phases of work, such as participant recruitment, research, and analyses and sharing – these phases show what data is collected in that phase. Briefly, the principle of data minimization underpins each phase—we have designed our process such that only enough personal and special category data is collected at each stage to enable us to conduct our research. Further, access is controlled: only people with a need-to-know basis will have access to the data in each stage. As an overview, we will be recruiting participants through three channels: incoming calls to our debt teams, outbound calls from our credit control team (as part of their Monday call campaigns to debtors), and voluntary and community sector organizations (VCSs). Below, we first briefly discuss the process for incoming and outbound calls, then discuss the process for VCSs. **(A) For both incoming and outbound calls**: Officers will ask customers if they are interested in participating in our research. If they are interested, officers will ask for their name, email, and phone number to pass onto the research team to get in touch. The officers will store these contact details in an internal, encrypted MS Excel spreadsheet, which will be saved in an access-controlled OneDrive folder. Each debt team (e.g. Housing, Council Tax, Credit Control, Parking) will have their own spreadsheet to populate; thus they would not be able to view the contact details which have been populated by officers in other teams. If the customer does not wish to participate, no personal information will be shared with the project team.

		The project team will then reach out to interested customers using their contact information, and call or email them to determine their eligibility to participate. To determine their eligibility, the research team will ask the customer questions listed on the Screening form, which is stored securely on the team's OneDrive. This form includes personal and special category data such as financial information in terms of debt to Camden, Camden residency status, and other factors which determine their eligibility to participate. **If the participant passes screening, they may chosen for research**. At this phase, their availability, their preferred mode of interview, ability to complete the consent form on MS Forms, and desire to receive a calendar invitation to block off the time will be confirmed. Chosen participants will be provided a consent form with the privacy notice on a Microsoft Office Forms, which is stored securely in our private, access-controlled OneDrive folder. If they would like, a calendar block will be sent out to their email address. **If the interview is conducted remotely**, we will use either phone or Microsoft Teams video or audio call, depending on the participant's preference. With their consent, we will record the interviews on audio or video, according to their preference. These recordings will be stored securely on our access-controlled OneDrive folder. Taking these recordings will allow the research team to play back interviews to ensure their written notes accurately reflect the participants' sentiments, and that direct quotes are transcribed verbatim. The video and audio recordings will not be used for any other purpose than transcription. Notes will also be taken, with the participant's consent, and will be stored in the OneDrive folder.

		If the interview is conducted in-person, with the participant's consent, the interview will be recorded on Microsoft Teams as an audio file. As above, these recordings will not be used for any other purpose than transcription. As above, notes will also be taken, with the participant's consent, and will be stored in the OneDrive folder. **(B) For participants sourced through VCSs:** The officer will first explain the research project and ask customers if they are interested in participating. If they are interested in participating, they will be directed to a link to complete the MS Forms screening form. If they are unable to complete the form due to digital exclusion or other factors, the VCS officer will receive their verbal consent to participate, then record their name and contact information (phone and/or email) in the unique, access-controlled MS Excel spreadsheet, which is stored securely in our access-controlled OneDrive folder. Each VCS organization will only have access to their own spreadsheet; thus, no customer details will be shared across other VCS organizations involved in this project. The research team will then reach out to these participants and conduct the phone screen using the MS Form. Once selected for interview, the process for participants sourced through VCSs is identical to the process for participants sourced through Camden's inbound or outbound calls.
3.2	**Explain in as much detail as possible why this is being done**	We require personal contact information to contact the participants. We collect special category data to screen participants for their eligibility to participate in our research: if they for example, do not owe debt to Camden, they must be excluded from our research sample as they are irrelevant to our line of inquiry.

<table>
<tr><td></td><td colspan="2"></td><td>We then record the interviews and take notes (given consent) to allow us to review the participants' contributions, to ensure the original sentiment is maintained in our key findings and synthesis.

We have chosen to store our documents securely in our OneDrive folders. We use individual sub-folders and Excel sheets with custom permission settings to ensure that only those who are required to access the spreadsheets or folders to fulfil their duties are granted permission. No additional access is granted.

Raw transcripts and recordings will be deleted after 1 year, in line with suggested best practices.</td></tr>
<tr><td rowspan="4">3.3</td><td colspan="2">Are you sharing the data with an external organisation or partner or are they involved in processing the data?</td><td>No</td></tr>
<tr><td>External organisation or partner
Name</td><td>Controller or Processor?</td><td>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</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>3.4.</td><td colspan="2">Please explain your process from start to finish. you can do this is a diagram if you wish, or a flow chart, or describe it. You can attach a document if that's easier.</td><td>We designed a flow chart to answer all questions in section 3 – please see here: DPIA - Data Flow Mapping.pdf</td></tr>
<tr><td>3.5</td><td colspan="2">How will you handle data in your project, how will use store and share it. Please explain</td><td>Please see above in section 3.1 for an overview, and this data flow map for details: DPIA - Data Flow Mapping.pdf</td></tr>
</table>

<table>
<tr><th colspan="4">Step 4: Assess lawful basis, necessity, and proportionality</th></tr>
<tr><td>4.1</td><td colspan="3">Identify the Lawful Basis for processing personal data/special category /criminal data.

Article 9(2)(a) Explicit consent; and, Article 9(2)(g) Substantial public interest</td></tr>
<tr><td></td><td>Personal data Article 6(1) UK GDPR condition

For recordings art 6(1)(a) consent, for other processing art 6(1)(e) public task. Where safeguarding information is disclosed such that the council is required to act then art 6(1)(c) legal duty</td><td>Special Category data UK GDPR Art 9 condition and DPA18 schedule condition

For recordings art 9(2)(a) explicit consent.

For other processing art 9(2)(g) public task, with the Data Protection Act 2018 schedule 1 part 2 condition being para 6 Statutory and government purposes, and the underlying law being the Localism Act 2011.

Where safeguarding information is disclosed such that the council is required to act then art 9(2)(b) (b) Employment, social security and social protection (if authorised by law) with the Data Protection 2018 schedule 1 part 1 condition being para 1 Employment, social security and social protection and (g) Reasons of substantial public interest (with a basis in law) with the Data Protection Act 2018 schedule 1 part 2 condition being para 6 Statutory and government purposes and para 18 18. Safeguarding of children and individuals at risk with the underlying laws being the Care Acts and Children Acts</td><td>Criminal data UK GDPR Art 10 condition and corresponding art 6 condition

Criminal offence data is not being directly collected, but if provided by a participant the article 6 legal basis is that as for personal data and the DPA18 schedule conditions will be the same as for special category data</td></tr>
<tr><td>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 Data Protection Advice Team have advised this is appropriate</td></tr>
</table>

	Consent form – see supplementary materials for reference
4.3	**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
	Data Quality Participants can review and update their contributions at any time by emailing or phoning the members of the research team. **Data Minimisation: (1) Personal Data; and (2) Special Category Data** It is key to first note that data minimization is jointly determined between us, the researchers who are designing the research experience, and the participants, who can determine if the data we ask for is deemed unnecessary for their personal context. While we only ask for data which is required for contact and screening purposes, some participants may find that they do not wish to supply certain pieces of information due to personal preferences or concerns. To address this, we uphold the principle that data supplied is completely voluntary. Participants can choose the number of queries they respond to, and these disclosures may be revoked at any time before, during, or after the research interviews, simply by contacting a member of the research team via their preferred method of phone or email. Secondly, in terms of the deliberate design of our research process, data minimization is a key value which underpins our approach for collecting both personal and special category data. Below, we have explained our approach for each category. **(1) Personal Data** Personal data is collected on three basis only: (a) to contact participants; (b) to control for correlates of financial debt and insecurity; and, (c) to ensure our sample is representative. **To contact participants:** We are only collecting an individual's name, email address, and/or phone number (depending on the participant's contact preferences) to contact the participants to conduct the research. **To control for correlates of financial debt and insecurity:** Extant research has shown that gender and age may be correlated to financial debt and insecurity. Collecting these pieces of information will allow us to not only follow the guidance of existing research. **To ensure our sample is representative:** In addition to allowing us to follow existing research in financial debt and insecurity, collecting a participant's gender and age will allow us to achieve a more holistic picture of each person's unique circumstance. It will also allow us to ensure that the percentage of participants we interview is representative of the demographic statistics we hold on the profiles of debtors. An example of how we are limiting the amount of personal data we collect is in how we decided not to collect participants' addresses. A key demographic feature of people who hold parking debt is that most

	debtors are not Camden residents. Thus, we would aim to interview mostly non-resident debtors to ensure our sample is representative. Instead of unnecessarily collecting a participant's address to deem them as a resident or non-resident, we are simply asking if they are (a) a current London Borough of Camden (LBC) resident, (b) a former LBC resident; or (c) someone who has never lived in LBC. This ensures that we can achieve our research aims of being representative, while holding the principle of data minimization. **(2) Special Category Data** We are only collecting enough special category data to ensure key factors related to individual debt levels and financial outlook are factored into our analysis and synthesis of findings. An example of this is collecting data on one's physical or mental health condition. In speaking with our frontline debt collection officers, we have found that a physical or mental health condition may not only impact an individual's ability to manage their debt, but may also – depending on the degree of severity – result in a different process officers must undertake in order to recover debt. Thus collecting information on one's mental and physical health would allow us to understand which set of communications, policies, and laws govern the experience an individual has with our debt teams. This necessary distinction would allow us to devise more nuanced findings and suggestions on the tangible changes we can make to improve the experiences of our debtors.	
4.4	**Have/ will 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 Privacy Notice? Remember telling people is not the same as asking for consent	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? What will happen to the data at the end of the project – deleted or kept? If you're using a processor what are the arrangements with them for data at the end of the project?**	
	1 year, to be deleted at the end of the retention period	

Step 5: Information Security Process	
5.1	**On what systems will the data will be stored** *Examples include Mosaic, OneDrive, shared drives,*
	A private, access-controlled OneDrive folder. Only members of the core research and design team (listed in 5.3) will have access.
5.2	**In what country is the data stored?**
	United Kingdom
5.3	**What roles will have access to the information?** (List individuals or staff groups)
	Only the core research and design team members (listed below) will have access: • Senior Service Designer • Senior Service Designer / Researcher • User Researcher • Events Assistant • Design Lead
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**
	Yes – we will be storing information on the private, access-controlled OneDrive folder for this project. Specific collaborators will have limited access –- they will only be permitted to access documents and/or sub-folders which are necessary for them to complete their contribution to this project. Only members of the research team will have access to all data. Access to information is controlled by only granting members of the research team access to the data who do not grant access more widely.
5.5	**Is there an ability to audit access to the information?**
	Yes – only members of the research team will access the data, and they will not share or grant access to anyone outside of this group.
5.6	**What security and audit measures will there be to make sure that data is kept safe?**
	All team members have completed the mandatory GDPR learning offering as part of their onboarding process. Team members will only access this data for the purposes of this project and will not share or grant access to anyone outside of this group.
5.7	**Has the Information Security Team advised on the security measures? What were their comments?**

	No

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.**	**Likelihood of harm- see table 1**	**Severity of harm- see table 2**	**Overall risk – see table 3**
Participants could be identified through their opinions and quotes by debt collection officers, who may have supported or who may currently be supporting the participants	Unlikely	Moderate	Moderate
Recordings going astray or retained beyond retention period	Likely	Moderate	Medium/high
Participants' contact information may be revealed to other Camden employees via the calendars of researchers	Likely	Minor	Moderate
Unnecessary personal data is collected	Unlikely	Moderate	Moderate
Researcher contact information such as personal email may be revealed to participants	Rare	Moderate	Moderate
The emotional wellbeing of participants may be compromised as they may disclose distressing information during the interview. This is likely as the topic of personal debt can be a highly emotional and private experience.	Likely	Negligible from a data privacy perspective but noted due to its importance	Moderate

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 /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?**
Participants could be identified through their opinions and quotes by debt collection officers, who may have supported or who may currently be supporting the participants	Firstly, while we are relying on debt collection officers as one source of recruitment, we do not expect a high subscription of participants from this source, due to the nature of the topic (debt owed to Camden Council). We anticipate participants' attitudes and potential fears towards owing debt towards Camden to moderate their interest in participating in this research, as it is more difficult to frame this piece of research as independent and neutral when it is pitched by Camden officers. In terms of potential controls: While debt collection officers may be aware of who is interested in participating, they will not be privy to the final list of participants. Thus, any suspicion they have about a participant's identity will remain a hypothesis. However, debt officers – if working closely with the customer over time, may be able to identify them still if our excerpts entail details such as a debtor's specific amount of debt…in these cases, we may combine several debtors to create one 'profile'; or we may paraphrase a quote and replace an identifiable number with a broader, descriptive term. Further, all quotes will be anonymized.	Reduced	Low	

Participants contact information may be revealed to other Camden employees via the calendars of researchers	The default settings in our calendars shows all appointments as visible to our team. If a calendar invitation is sent to participants, their contact information and participation would be visible to Camden employees. To eliminate this risk, all calendar invitations sent will be marked 'Private', which ensures no details will be visible to anyone except the diary holder and meeting invitees.	Eliminated	Low	
Unnecessary personal data is collected	The risk of this is considerably lowered as we have designed a research process based on the principle of data minimisation. For example, to understand whether a participant lives in Camden, instead of asking for their address or postal code, we simply ask for their resident status.	Reduced	Low	
Researcher contact information such as personal email may be revealed to participants	Researchers will only contact participants through their Camden email addresses and Camden-issued phone numbers (which operate via MS Teams). In the event MS Teams is unable to support the interview call, researchers will not use their personal email addresses or phone numbers to attempt to contact the participant. The interview will be rescheduled so that contact remains secure and the researchers' contact information remains private.	Eliminated	Low	
Recordings going astray or retained after retention period	All recordings are stored in a secure folder on SharePoint. At the expiry of the 1-year retention period, the Project Lead (Elsa Bardout) will delete all recordings from our SharePoint. The Project Lead will set an appointment in her calendar 1 year from the date of the last interview, to ensure all records are deleted in the future. Within the Strategy and Design team, there are plans to integrate a file-cleaning procedure every 6 months. While there is not yet a date for implementation, this will likely occur before the 1-year anniversary of this	Reduced	Low	

	project, and would therefore help reduce the risk of recordings going astray or retained after the 1-year period.			
The emotional wellbeing of participants may be compromised as they may disclose distressing information during the interview. This is likely as the topic of personal debt can be a highly emotional and private experience	If the participant is covering a sensitive topic, even if they are not visibly demonstrating signs of distress, the researcher will ask if they feel they are able to continue speaking about the topic. If the participant would like to take a break at any time, the researchers will encourage it. If the participant would like to withdraw from participating, the researchers will encourage it, and stay on the line with the participant to ensure there is no immediate risk of harm. For all participants, researchers will share a list of vetted resources at the end of the interview. This list will signpost participants to services which can help them with their debt. These services range from organisations which are dedicated to supporting individuals during the cost-of-living crisis, to longer-term aid relating to debt advice. Prior to distribution, the researchers will contact these services to understand their capacity to support referrals, to ensure that participants are not directed to oversubscribed services which are unable to provide aid.	Reduced	Low	
Residual (remaining) risk level when all mitigations have been applied: ***Note IRT/DPO may change this***				
Low				

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? If not, name of IRO	No, Sarah Laws, Data Protection Manager
DPO advice	Approved, Andrew Maughan DPO, December 2022
Information Asset Owner acceptance of residual risks	Kate Robertson
This DPIA will kept under review by: (*usually the author or the IAO)*	[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) The Data Charter is here: Camden's Data Charter - Camden Council

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?)*

- Collecting personal contact information enables us to reach out to debtors to gain their insight on their motivations, experiences, pain points with holding debt to the Council. This piece of research would enable us to bring these perspectives to the sponsor of this project, and to internal debt teams, allowing us to develop a shared understanding across the organization of the types of debtors we have, and how we may best support them towards financial security.

- Collecting special category data would allow us to ensure that we are researching participants who represent the profiles of debtors staff have deemed as key priorities for us to understand and support.

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

- Personal Data: We would not be able to contact individuals to gain their insight on their lived experiences of holding debt towards Camden. Our research findings would then only include staff perspectives, which are only one piece of the overall picture of the customer experience.
- Special Category Data: We would not be able to assess whether our sample is relevant and representative, skewing the insights from the research.

2. *Data Bias*

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

- Data Collection: Collecting special category data would allow us to actually control for potential bias. By ensuring we have key voices which represent the prioritized profiles staff have deemed relevant for this project, we can ensure their experiences and needs are considered moving forward.
- Data Analysis: Feedback will be aggregated based on thematic and qualitative analysis; by applying appropriate research methodology, we can minimize the bias which may flow through.

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?*

- Limitations of the research will be clearly stated; including and not limited to: a) small sample size, b) non-response bias, c) limitations of qualitative analysis.

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**?

- Potentially, the participants may experience emotional turmoil from recounting difficult life experiences particularly as they relate to debt; however, participation is entirely voluntary, can be paused, or revoked at any time. We lead with an empathetic approach, where we put our participants, our people, above research results and outcomes. We will also supply a list of support resources after the interview, as part of our compensation package. These support resources will be vetted before being presented to participants, for capacity and ability to provide support, such that we are not directing participants towards outdated or oversubscribed services.

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?*

As noted above in section 4.3, data minimization is a key principle underlying our project. We do not collect any data which is unnecessary to complete our research objectives. Personal and special category data are collected on three basis only: to contact participants; to control for correlates of financial debt and insecurity; and, to ensure our sample is representative.

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**)*

- Participants may revise their comments at any time through contacting us via phone or email, in case they would like to retract or update a previous statement. Any outdated statements will be deleted and will not be used in the final output.

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)*

- Names and contact method (phone or email address) will be attributed with our raw notes

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

- Not possible, as contact information is required to gain insight, and other personal data is required to ensure our sample is representative and eligible.