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.

Project Name	**Digital Inclusion Challenge – Discovery research**	
Project Lead and Information Asset Owner/s	Project Lead	[redacted]
	Information Asset Owner name and asset	Tariq Khan, Chief Data and Information Officer
Summary of the project	The discovery project focuses on building understanding of the residents' experiences of digital exclusion and inclusion in Camden. The research team will conduct qualitative interviews with residents. We will be making notes during the interviews and, where consent will be given, we will be recording the conversations with a dictaphone (when happening face to face) or via Microsoft Teams (when conversations would be held on Microsoft Teams). Written notes will be kept for up to 5 years; recordings will be kept for up to 1 year. The outputs from this project should allow the council to make evidence-informed decisions and will inform the next steps towards addressing the challenge of the digital divide. This should include contributing to the next iteration of the Digital Strategy and providing recommendations for addressing this challenge.	
Implementation Date:	October, November 2022	

Pre-screen: If you have not already done a pre-screen please do the questions below. If you have a pre-screen, attach it to the DPIA. 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 and the rest of the DPIA should be completed.

Q 1	Screening question	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, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or 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?	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?	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?	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			
							New			
2.2	**What data will be processed/shared/viewed?**									
	Personal Data									
	Name	y	Date of Birth	y	Gender	y	National Insurance Number	n	Financial Information about the person	n
	Address	n	Email address	y	Telephone number	y	NHS No	n	Other eg a reference number such as Mosaic ref	n
	Other data *(Please state):*									
	Special Categories of Personal Data									
	Racial or ethnic origin	x	Fingerprints/ Biometrics	*n*	Religious or philosophical beliefs Political opinion					*N n*
	Trade Union membership	n	Physical or mental health or condition							n
	Sexual life or sexual orientation	n	Housing records Social services records	n	Tax, benefit or pension records	n				
	Other data *(Please state):*									
2.3	Proceedings for any offence committed or alleged, or criminal offence record?		n							

Step 3: Describe the sharing/processing			
3.1	**Describe in as much detail what is being done with the data**		The qualitative data gathered through conversations with residents will be used for research purposes to gain understanding on participants' experiences of being digitally excluded and/or of accessing digital inclusion support. The qualitative will be analysed and synthesised by the research team and will lead to the formulation of research insights and recommendations. We will collect high level diversity monitoring data to ensure we speak to a representative group of people.
3.2	**Explain in as much detail as possible why this is being done**		We want to speak to Camden's residents to understand their experiences of digital exclusion and inclusion. We need to collect some personal and special category data about the participants to help us in ensuring that we are representing a wide range of views and experiences. Ultimately processing the data will allow the research team to create outputs based upon the insights uncovered from the synthesis which will help the Digital and Data Services teams understand residents' experiences and needs and make decisions about next steps towards addressing the digital exclusion in the borough.
3.3	**Are you sharing the data with an external organisation or partner or are they involved in processing the data?**		No
	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**
	N/A		No
3.4.	**Has a data flow mapping exercise been undertaken?**		Yes **If yes, please provide a copy, if no, please undertake**
3.5	**How will the information be processed/shared**		The data will only be accessible by named individuals working on the project only. The data collected will be held on a secure Teams folder which only the research

		team have access to. The data will not be shared more widely. The project outputs will be shared with the Chief Digital and Data Officer (Sponsor of the project) and relevant senior officers. The outputs will not contain any personal or special category data collected throughout the research, but only synthesised insights uncovered by the research team around residents' experiences. Any quotes/feedback will be anonymised.

Step 4: Assess lawful basis, necessity, and proportionality			
4.1			
	Personal data Article 6(1) UK GDPR condition Article 6(1)(a) Consent, Article 6(1)(e) Public task	**Special Category data UK GDPR Art 9 condition and DPA18 schedule condition** Article 9(2)(g) Substantial public interest and 9(2)(a) explicit consent	**Criminal data UK GDPR Art 10 condition and corresponding art 6 condition** N
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		
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 h***ow long will the data be kept?*
	We will keep the information that participants have provided on the screener and consent form as well as the information participants have told us in interviews for up to 5 years. Recordings will be held for 1 year and then deleted.

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.*	
	an encrypted spreadsheet saved on Microsoft Teams	
5.2	**Where is the data stored geographically?**	
	UK	
5.3	**What roles will have access to the information?** (list individuals or staff groups)	
	The research team: Weronika Sarnowska, Policy Designer; Afreen Saulat, Design Researcher	
5.4	Is there role based access control on all applicable systems? **How will access to information be controlled?**	
	Access to information is controlled by only granting members of the research team access to the data who will not grant access more widely.	
5.5	**Is there an ability to audit access to the information?**	
	Only members of the research team have access to the data and they will not share or grant access to anyone outside of the team.	
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?**	

	We will ensure secure access to and limit use of personal data/special categories data in a number of ways. All members of the project team have been informed about the requirement to only process data which is necessary and proportionate – a list of personal data that needs to be collected has been agreed upon (above) and no additional data will be stored. No criminal data will be collected.
5.57	**Has the Information Security Manager advised on the security measures? What were his/her comments?**

Step 6: Identify and Assess Risks			
Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. **These are the risk *before* any controls (mitigations are applied)** Add in additional rows as necessary. The completed row is an examples	**Likelihood of harm- see table 1**	**Severity of harm- see table 2**	**Overall risk – see table 3**
Unauthorised access to data stored	Possible	Moderate	Low/Medium
Residents could be identified through the stories they share with the research team relating to their individual circumstances	Possible	Moderate	Low/Medium

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, not all risk can be eliminated. Then calculate the risk that remains after the mitigations/controls are in place- the residual risk. Decide if this is accepted in the measure approved? column				
Risk identified in step 6	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved?**
Unauthorised access to data stored.	The research team will use a single encrypted file for personal data storage which will be securely stored and only a.	The risk will be considerably lowered leading to rare likelihood	Low risk	yes
Residents could be identified through the stories they share with the research team relating to their individual circumstances	In synthesising the data and producing a summary of findings, the research team will anonymise quotes and stories heard and not include any details included in participant's stories that could lead to the participant being identified.	The risk will be considerably lowered leading to rare likelihood	Low risk	yes
Residual (remaining) risk level when all mitigations have been applied:				
Low				

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? If not, name of IRO	Veron Reece-Jones
DPO advice	Approved Andrew Maughan DPO and Borough Solicitor 19/10/2022
Information Asset Owner acceptance of residual risks accepted by	Tariq Khan, Chief Data and Information Officer
This DPIA will kept under review by:	Tariq Khan, Chief Data and Information Officer

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	Wilful 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

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