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	**Face to Face Review**	
Project Lead and Information Asset Owner/s	Project Lead	[redacted]
	IAO name and asset	Phil Quickenden – Head of Customer and Registration Services (Camden Customer Relationship Management)
	IAO name and asset	Glendine Shepherd – Director of Housing (Housing Needs group) Steve Harris – Head of Facilities Management (Security Incident Reports)
Summary of the project. *Outline what your project is about. Start with a general headline and then go into more detail. Explain any acronyms on first use.*	**From 2023 – 2024, the council buildings have had a record of 88 security incidents that took place on-site, with some involving suicide attempts. Some of these incidents occur when residents arrive at the building, seeking help with access or use of services from Contact Camden's front desk at 5 Pancras Square (5PS). In 2023, there have been a series of escalated**	

	incidents involving people facing homelessness who were unable to access the help they needed when visiting 5PS. In light of this, we would like to understand the circumstances under which such incidents occur, the experiences of relevant service teams, frontline staff and residents during the visits to 5PS. Subsequently, we would make recommendations to improve the way key services work together to reduce the number of escalated incidents at 5PS, as well as manage the incidents appropriately, safely, and with duty of care to both residents and staff in mind. To do this, we are running a project that will run for 5 weeks. The project involves desk research to review existing incident reports; interviews with council staff (security, customer support officers, and homelessness prevention officers); and a workshop (with the same staff mentioned earlier, as well as - potentially - people with lived experience) to come up with and prioritise ideas for improving the situation. For the desk research, we will review Security Incident Reports and Reports from Homelessness Managers (from the Housing Needs Group (HNG) data platform). We will also review two types of data from Customer Relationship Management (CRM): The first type of CRM data is aggregated and anonymised data showing number of people experiencing homelessness who are in contact with the council and whether it was face to face or via telephony, what the outcomes of the queries were, and CRM notes on motivations for face to face (F2F) interactions. Whilst the project team will be provided with anonymised data, the council as data controller will process this data to locate, extract, collate, and anonymise it.

	The second type of data would be CRM notes of people that are referred to in Security Incidents Reports. This is to make sure that we see a different perspective of the incidents that happened and to get a better understanding of the situation of the person. To get access to this CRM data, we would have to pass on the following data from the Security Incident Reports to the CRM team: the names of the person visiting and the CSO involved in the incident, the data and time of the visit. Similarly to the second type of CRM data noted above, we will review data from the HNG database that the Homelessness Prevention team use to record notes of their engagements with people who are homeless. We will review a sample of records on 5 people, so that we also add the perspectives of the Homelessness Prevention team to our understanding. The selection criteria for sampling these records will be that the person is either currently experiencing or are at risk of experiencing homelessness, and to have visited 5PS to seek support. For the interviews and workshop, we will not be recording audio or video. We will be noting down the conversations through typing it up into a secured folder or writing on paper before being typed up into the same secured folder. We will be contacting people with lived experience of homelessness through the Co-production Team within Camden's Homelessness Transformation programme. This programme already works with 'co-producers' (people who have previous or current experience of homelessness who have consented to take part in creating material designed to support other people experiencing homelessness). We have emailed a summary of this project to the Co-production Lead, who has shared it with the current co-producers. This email has been screenshot and

	saved as appendix 2. The selection criteria for this cohort is the people will have had experience in homelessness and have visited 5PS. We have asked the Co-production Lead to advise us on location of research activities (they have suggested to hold research activities at 5PS as the co-producers are familiar with the building and the Co-production Lead will make sure they are also in the building for any support if needed) and appropriate incentives (Tesco voucher of £15 per hour of participation). We will also share discussion guides with the Co-Production Lead and get their expert advice in sensitivity of the questions and making sure we are limiting the possibility of trauma that may be triggered through participating in the research activity.
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	March 2024

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?	Yes
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?	No
1.7	Does the project involve new processing or significantly change the way in which personal data/special categories of personal data is handled?	Yes
1.8	Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	Yes
1.9	Will data be combined, compared or matched from multiple sources?	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

<table>
<tr><th colspan="11">Step 2: What personal data is being used?</th></tr>
<tr><td>2.1</td><td colspan="8">Is this use of personal data/special categories of personal data a new use? Or is it already happening and this is a change?</td><td colspan="2">New/Changed</td></tr>
<tr><td></td><td colspan="8"></td><td colspan="2">New</td></tr>
<tr><td>2.2</td><td colspan="10">What data will be processed/shared/viewed?</td></tr>
<tr><td></td><td colspan="10"><u>Personal Data</u></td></tr>
<tr><td></td><td>Name</td><td><u>Y</u></td><td>Date of Birth</td><td><u>Y</u></td><td>Gender</td><td><u>Y</u></td><td>National Insurance Number</td><td><u>Y</u></td><td>Financial Information about the person</td><td><u>Y</u></td></tr>
<tr><td></td><td>Address</td><td>Y</td><td>Email address</td><td>N</td><td>Telephone number</td><td>N</td><td>NHS No</td><td>N</td><td>Other eg a reference number such as Mosaic ref</td><td>N</td></tr>
<tr><td></td><td colspan="3">Other data (Please state):</td><td colspan="7">- Security Incident Reports

- Records from the Housing Needs Group (HNG) database of 4-5 people who have come into 5PS

- Two types of data from CRM: a) aggregated and anonymised data, and b) CRM notes of individuals who were involved in the incidents noted in Security Incident Reports.</td></tr>
</table>

<table>
<tr><td></td><td colspan="8">In all the above, there is likely going to be other miscellaneous personal data that the project team will access</td></tr>
<tr><td></td><td colspan="8"><u>Special Categories of Personal Data</u></td></tr>
<tr><td></td><td>Racial or ethnic origin</td><td>Y</td><td>Fingerprints/ Biometrics</td><td>N</td><td colspan="3">Religious or philosophical beliefs Political opinion</td><td>May be</td></tr>
<tr><td></td><td>Trade Union membership</td><td>Maybe</td><td colspan="6">Physical or mental health or condition</td><td>Y</td></tr>
<tr><td></td><td>Sexual life or sexual orientation</td><td>Myb</td><td>Housing records Social services records</td><td>Y</td><td>Tax, benefit or pension records</td><td>Y</td><td colspan="2">Employee/HR records</td><td>N</td></tr>
<tr><td></td><td>Other data (Please state):</td><td colspan="7">- Security Incident Reports

- Reports from Homelessness Managers about the incidents

- Anonymised data from CRM</td></tr>
<tr><td>2.3</td><td>Will it include data about any criminal offence committed or alleged, or criminal offence record?</td><td colspan="7">Possibly
Given the nature of the project, the project team may find records of criminal offence when reviewing the security incident reports, CRM data and reports from the homelessness managers, especially if staff or other members of the public were threatened during the recorded incidents. Examples include physical or verbal abuse recorded in the reports.</td></tr>
</table>

Step 3: Describe the data processing		
3.1	Describe in as much detail what is being done with the data	1. Desk research to identify the types of situations that people facing homelessness experience, why they come into 5PS, and the gaps in support that could have benefited them. 2. Semi-structured interviews with staff present at the incidents to map out the experiences of people involved. 3. An observation study at 5PS reception area, noting and sketching flows of movement of people within the space to capture what it's like on a normal day. No conversations will be recorded. 4. Workshops with service teams and (potentially) people experiencing homelessness. This is to review the findings from the last activities, as well as generate and prioritise ideas for how relevant teams could better work together to reduce and manage the number of escalated incidents at 5PS involving people experiencing homelessness. We will be working with the Co-Production Team within Homelessness Transformation service to potentially engage with people with lived experience. We would only invite people facing homelessness who are already part of the Co-production activities, if they would like to be and agree to being involved with our project.

			We will be recording the interview conversations through typing notes saved in a secured folder only for the project team, we will also be recording the interview conversations through worksheets that the participants will interact with. During the workshops we will be recording conversations through notes on paper and interactive worksheets. All names of participants will be converted into pseudonyms, and when referring to participants a code system will be used. For example 'Participant 1'.
3.2	Explain in as much detail as possible why this is being done		We are collecting this data to as part of a Face to Face Review. The Review will form a series of recommendations around how service teams can be better aligned to reduce the number and manage the escalation of incidents at 5ps.
3.3	Are you sharing the data with an external organisation or partner or are they involved in processing the data?		If people experiencing homelessness will be involved in our workshops, then we may share insights (anonymised, processed and synthesised data) with them
	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 mapping exercise been undertaken? If yes, please provide a copy, if no, please undertake	Enlarged image in Appendix 
3.5	How will the information be processed/shared. Details eg secure file transfer	The data will only be accessible by the Strategy and Design Team working on the project only. The data collected will be held on a secure Teams folder which only the design and research team have access to. The data will not be shared more widely. The project outputs will be shared with relevant Camden Council staff. The outputs will not contain any personal or special category data collected throughout the research, but only synthesised insights discovered by the research team around The Face to Face Review. Any quotes/feedback will be pseudonymised. We will be synthesising the data on Miro (a digital platform used to collaborate). Each Miro board that we use to synthesise the data will only be accessible to the project team and will be encrypted with a password that is complex and is a passphrase.

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 Article 6(1)(c) legal duty and 6 (1)(e) public task.	Special Category data UK GDPR Art 9 condition and DPA18 schedule condition Art 9(2) (b) Employment, social security and social protection with the Data Protection Act 2018 Schedule 1 Part 1 condition being Para 1 Employment, social security and social protection Art 9(2) (g) Reasons of substantial public interest with the Data Protection Act 2018 Schedule 1 Part 2 condition being Para 6 Statutory and government purposes and para 18 Safeguarding of children and individuals at risk The underpinning laws for all are the Health and Safety at Work etc Act 1974, the Care Act 2014 and the Children Acts	Criminal data UK GDPR Art 10 condition and corresponding art 6 condition Article 6 (1)(c) legal duty and 6 (1)(e) public task. with the Data Protection Act 2018 Schedule 1 condition being Para 6 Statutory and government purposes and para 18 Safeguarding of children and individuals at risk and the underpinning law the same as for special category data

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 Whilst people will agree to take part in interviews, this is not the same as data protection consent for data processing, and consent is not the legal basis.	
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	
	We will only be asking staff about the interactions that happened if they were present. We will be engaging with people with lived experience to get their views on how we shape our recommendations to the organisation. This will ensure that we are only processing the data which is necessary and proportionate to the project and focus on face to face experience at 5ps. We will be cross referencing the incident reports that have been written by security in 5ps with a) staff interviews and b) conversations during workshops with staff and people with lived experiences and c) CRM data.	
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 all policies will be followed . No contracts required as no processors.	
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?**
	We will keep the information that participants have provided on the agreement to take part form as well as the information participants have told us in interviews for up to 2 years. Notes will be typed into a secured folder or noted on paper before being typed up into the same secured folder. These notes 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 folder on SharePoint **A password encrypted project space on Miro**
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: Senior Service Designer, Service Designer and Design and Research Associate
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.
5.7	**Has the Information Security Manager advised on the security measures? What were his/her comments?**
	Not necessary for this processing, but they have approved the use of Miro with some conditions around role-based access control.

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.	**Likelihood of harm- see table 1**	**Severity of harm- see table 2**	**Overall risk – see table 3**
Unauthorised access to data stored by other council staff.	Possible	Moderate	Medium/high
People facing homelessness could be identified through sharing of outputs and this would lead to privacy intrusion	Rare	Moderate	Low
Retaining data after the retention period which would be breaching art 5 UK GDPR requirements	Possible	Moderate	Medium/high
Privacy intrusion from the processing itself, as people may not expect this to be undertaken, and noting interactions in the reception may be considered intrusive by those being watched	Likely	Moderate	Medium/high

Step 7: Identify Measures to reduce risk				
Identify measures to reduce or eliminate risks identified in step 6. *Remember that risks need to be reduced to an acceptable level, and not all risks can be eliminated.* Then calculate the risk that remains after the mitigations/controls are in place: the residual risk. Tables 1, 2 and 3 will help with this. *Note that risks and scores are subject to review and change by IRT/DPO* The Information Asset Owner/s need to decide if the mitigations are achievable and if the residual risk is accepted in the 'measure approved?' column by inserting a Yes or No. Table 4 provides guidance on what level of residual risk could be acceptable.				
Risk identified in step 6	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved?**
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	
People facing homelessness could be identified through sharing of outputs	In synthesising the data and producing a summary of findings, the research team will pseudonymise quotes and stories heard and not include any details included in participant's stories that could	The risk will be considerably lowered leading to rare likelihood	Low risk	

	lead to the participant being identified.			
Retention after period	Controls are in place along with organizational measures	Reduced	Low risk	
Privacy intrusion	The council's privacy notices cover general processing and research. Records being accessed will be undertaken in a controlled way for specific purposes by council staff and pseudonymisations will be in place. Those being interviewed will agree to take part and there will be no element of compulsion. In terms of those in 5PS being observed this is a tolerated risk, and it is noted that observations are already undertaken by CCTV (which is monitored) and the presence of security guards who observe people. The additional intrusion is the more targeted nature of the observations but the intrusion is	Parts reduced, part tolerated, overall reduced	Medium risk	

	considered not high or excessive, and proportionate to the outcomes			

Residual (remaining) risk level when all mitigations have been applied: *Note IRT/DPO may change this*
Medium

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? If not, name of IRO	No, Sarah Laws, Data Protection Manager
DPO advice	I agree and I am happy with this. The underlying driver for this is really needed.Andrew Maughan, DPO and Borough Solicitor.
Information Asset Owner acceptance of residual risks	Phil Quickenden, Head of Customer and Registration
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

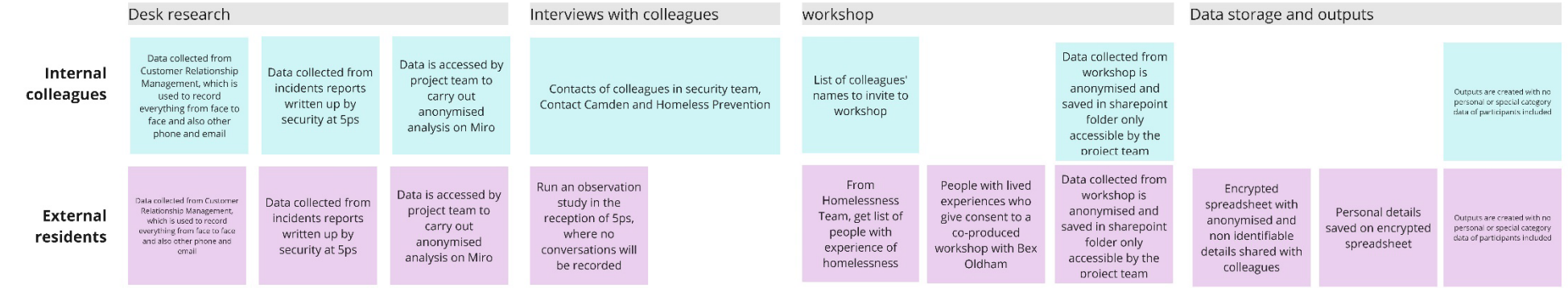
IMPACT	Score:	PROBABILITY				
		Rare	Unlikely	Possible	Likely	Almost Certain
	Catastrophic	5	10	15	20	25
	Major	4	8	12	16	20
	Moderate	3	6	9	12	15
	Minor	2	4	6	8	10
	Negligible	1	2	3	4	5

Table 4: is the risk level acceptable?

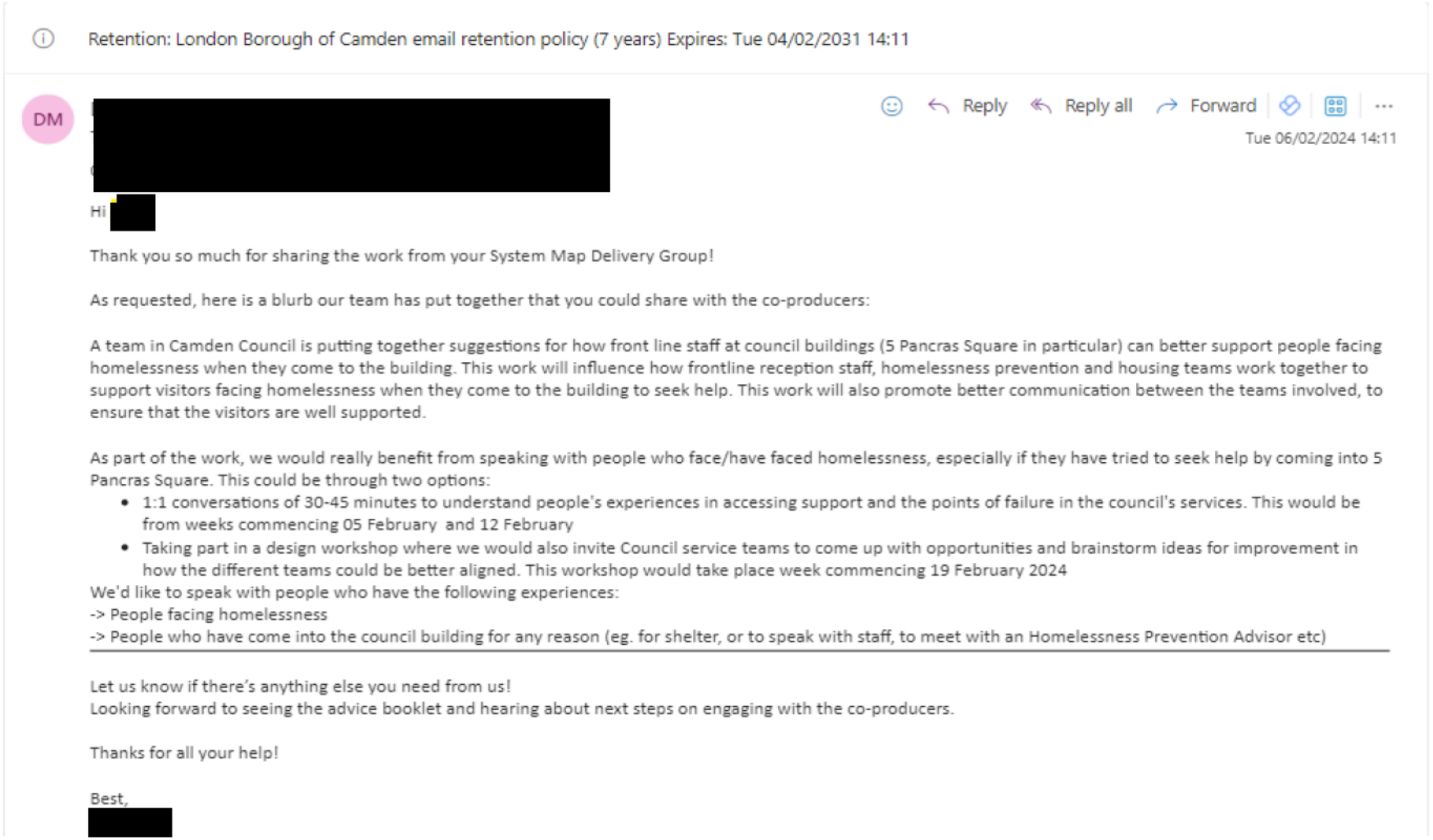
Level of risk	
1-3 Low Risk	Acceptable risk No further action or additional controls required Risk at this level should be monitored and reassessed at appropriate intervals
4-6 Moderate Risk	A risk at this level may be acceptable, if so no further action or additional controls required If not acceptable, 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: 1: Data flow mapping

Face to Face Review: Data Flow Mapping



Appendix 2: Email sent to Co-production Lead for inviting people with lived experience to participate in this project.



Retention: London Borough of Camden email retention policy (7 years) Expires: Tue 04/02/2031 14:11

DM [redacted]

Reply Reply all Forward

Tue 06/02/2024 14:11

Hi [redacted]

Thank you so much for sharing the work from your System Map Delivery Group!

As requested, here is a blurb our team has put together that you could share with the co-producers:

A team in Camden Council is putting together suggestions for how front line staff at council buildings (5 Pancras Square in particular) can better support people facing homelessness when they come to the building. This work will influence how frontline reception staff, homelessness prevention and housing teams work together to support visitors facing homelessness when they come to the building to seek help. This work will also promote better communication between the teams involved, to ensure that the visitors are well supported.

As part of the work, we would really benefit from speaking with people who face/have faced homelessness, especially if they have tried to seek help by coming into 5 Pancras Square. This could be through two options:

- 1:1 conversations of 30-45 minutes to understand people's experiences in accessing support and the points of failure in the council's services. This would be from weeks commencing 05 February and 12 February
- Taking part in a design workshop where we would also invite Council service teams to come up with opportunities and brainstorm ideas for improvement in how the different teams could be better aligned. This workshop would take place week commencing 19 February 2024

We'd like to speak with people who have the following experiences:
-> People facing homelessness
-> People who have come into the council building for any reason (eg. for shelter, or to speak with staff, to meet with an Homelessness Prevention Advisor etc)

Let us know if there's anything else you need from us!
Looking forward to seeing the advice booklet and hearing about next steps on engaging with the co-producers.

Thanks for all your help!

Best,
[redacted]