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	**Reporting Hub**	
Project Lead and Information Asset Owner/s	Project Lead	[redacted]
	IAO name and asset	Jo Brown, HR records
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.*	Reporting Hub – we will be launching a 'hub' for staff to report incidents of discrimination into. This will involve 10 staff volunteers providing a welcoming, supportive spaces for staff members to report that they have experienced discrimination . This reporting will take place over email, over the phone or face to face depending on the individual's preference. The hub member will record the information on a secure sharepoint spreadsheet so that appropriate records are kept for cases and so that HR can analyse the data (in terms of how many incidents are occurring, where they are occurring). Hub members will be able to access the reports they have inputted but not reports that have been inputted by other hub members. The hub members will present options available to the individual (e.g grievance, mediation) and the individual can decide how they want to proceed. HR Business Advisors will be available to offer Hub members support should they need it and to pick up any next steps. Data being collected will include name (optional), the incident, when it occurred, in what area of the organisation it occurred (i.e directorate, service) and what kind of incident it was (i.e homophobia, ableism, racism etc). This is being done so we have a better understanding of what incidents of discrimination look like across the organisation. Currently we are only able to track reports of discrimination when a grievance or dismissal procedure is involved. We want to be able to better understand incidents of discrimination in their entirety, even when the individual who is reporting does not want to go down a formal route. This will enable us to better tailor our work to tackle the issues that exist within the organisation.	

Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	June 2023

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?	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?	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?	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			
							New			
2.2	**What data will be processed/shared/viewed?**									
	Personal Data									
	Name	**Yes**	Date of Birth		Gender	**Yes**	National Insurance Number		Financial Information about the person	
	Address		Email address	yes	Telephone number		NHS No		Other eg a reference number such as Mosaic ref	
	Other data *(Please state):*	It will include information of incidents being reported by the person. We will be capturing name (unless the individual would like to remain anonymous), date of incident, what happened, where in the organisation (i.e team, service, directorate), what course of action the individual would like to take								
	Special Categories of Personal Data									
	Racial or ethnic origin	Yes	Fingerprints/ Biometrics		Religious or philosophical beliefs Political opinion					*Yes*
	Trade Union membership		Physical or mental health or condition							Yes
	Sexual life or sexual orientation	Yes	Housing records Social services records		Tax, benefit or pension records		Employee/HR records			
	Other data *(Please state):*									
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?	Yes it could do – as some incidents of harassment could be a criminal offence.								

Step 3: Describe the data processing		
3.1	**Describe in as much detail what is being done with the data**	The data will be stored on a secure MS Forms system being developed by the Technology Adoption Team. This will then sit in a secure MS Teams folder, only accessible to Reporting Hub members. This will enable Reporting Hub members to input data and view their own reports, but they will not be able to access reports submitted by other hub members to protect confidentiality. The back end of the MS Forms (which transfers onto an excel) doc will be accessible to the HR Management Information team so the data can be analysed. This will enable us to understand the nature of incidents (e.g racist, homophobic, transphobic, ableist), where they are happening within the organisation (e.g are they concentrated in a certain directorate, service or team?) and how frequently.
3.2	**Explain in as much detail as possible why this is being done**	This is being done so we have a better understanding of what incidents of discrimination look like across the organisation. Currently we are only able to track reports of discrimination when a grievance or dismissal procedure is involved. We want to be able to better understand incidents of discrimination in their entirety, even when the individual who is reporting does not want to go down a formal route. This will enable us to better tailor our work to tackle the issues that exist within the organisation.
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	**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	
3.4.	**Has a data flow mapping exercise been undertaken?** **If yes, please provide a copy, if no, please undertake**	Not necessary for this project
3.5	**How will the information be processed/shared. Details eg secure file transfer**	It will be stored in a secure MS Teams file being developed specifically for this purpose by the Technology Adoption team (team led by [redacted])

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	**Special Category data UK GDPR Art 9 condition and DPA18 schedule condition** Article 9(2) (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 6. Statutory and government purposes, with the underlying laws being the Equality Act 2010 and the Health and Safety at Work etc Act 1974.	**Criminal data UK GDPR Art 10 condition and corresponding art 6 condition** The art 6 condition is the same as for personal data and the DPA conditions being the same as for article 9
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**		
	Consent is not the legal basis for processing the personal data		
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		
	The data will be provided by the individual so quality is uncheckable but not a difficulty for this project. The information recorded will be guided by the individual's wish to disclose or not. However they will only be asked to disclose what they feel comfortable with.		
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 LBC's policies will be followed. There are 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?**		

	MS teams do not get deleted as per Camden's data retention policy. Info sec team would have to exclude the site from the policy in order to delete the team and the info it contains. The data will be retained for the current year plus six years, as this is commonly used across all areas of information.
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.*
	MS Forms – an excel spreadsheet that sits behind it.
5.2	**Where is the data stored geographically?**
	In the cloud, as part of our licensing with Microsoft. It is stored within the EU where GDPR laws are binding of that information.
5.3	**What roles will have access to the information?** (list individuals or staff groups)
	HR MI team, Diversity and Inclusion Programme officers. Reporting hub members will have access to their own reports but not those of others
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**
	We would use a Microsoft Form which would sit within an MS team and not an individual's one drive. The Business Solutions team can help check that this is where it is stored. Only members of the MS team would have access to the data within the form. Only members of the team would have access to the data from the form
5.5	**Is there an ability to audit access to the information?**
	There will be limited audit capability, we can only report on who has access to the form and nothing else as is the case currently with all Microsoft products like Excel and Word documents.
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 have a non-disclosure and data protection agreement signed between Microsoft and ourselves. We are also have visibility over our data so that if there is an attempt to extract sensitive data we can see this and therefore prevent it.
5.7	**Has the Information Security Manager advised on the security measures? What were his/her comments?**
	Yes. They are happy with the approach and the data being stored on the sharepoint system. They have emphasised that Reporting hub members should not be able to see what is inputted by other Hub members in order to protect anonymity, which the system will ensure is the case.

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. The data collection and usage is inherently intrusive as it is data processing around highly sensitive and emotive data.	Possible	Minor/Moderate	Medium/High Risk
Further usage. The risk that the Reporting Hub members will use the data disclosed for other, unauthorised, purposes.	Possible	Minor/Moderate	Medium/High Risk
disclosure. The risk that the data may be disclosed to others resulting in harm to the data subjects	Possible	Moderate	Medium/High Risk
Unauthorised access . Ineffective role based access control meaning reporting hub members can access each other's cases, resulting in privacy intrusion and harm.	Possible	Moderate	Medium/High Risk

Retention period failure. Retaining data beyond retention period.	Possible	Minor/Moderate	Medium/High Risk

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	Information is stored on Council kit which has very good information security controls	Lower	Low Risk	yes
Further usage	Reporting Hub members bound by code of conduct committing to using data appropriately and any violation of this could be taken forward as a disciplinary offence	Lower	Moderate Risk	yes
Disclosure	Reporting Hub members bound by code of conduct committing to confidentiality and disclosing any info could be taken forward as a disciplinary offence	Lower	Moderate Risk	yes
Unauthorised access	Tailor built software will ensure that reporting hub members cannot access each other's cases	Lower	Low Risk	yes
Retention period	Policies in place to cover retention.	Lower	Low Risk	yes

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

Medium

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? **If not, name of IRO**	No. Sarah Laws, Data Protection Manager
DPO advice	Approved, Andrew Maughan, DPO, June 2023
Information Asset Owner acceptance of residual risks	Names of IAOs Joanna Brown, Director of People and Inclusion
This DPIA will kept under review by: (*usually the author or the IAO)*	[redacted]

Version Control

Version	Reason	Date	Author(s)
1.0	New document	May 2023	[redacted] and Sarah Laws

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.

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?*

- The data will help us better understand discrimination across the organisation, which will then help us tailor our work to prevent discrimination from happening. While this doesn't affect residents directly, it does mean we will provide a more inclusive workplace for our staff, enabling them to better thrive at work and therefore improving the service they deliver to our residents.

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

- We would remain unable to understand incidents of discrimination across the organisation and therefore would not be able to effectively tackle it.

2. *Data Bias*

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

All information will be collected and it will be based on what has been told to the reporting hub members. The analysis that is undertaken will be based on reports that have been provided to us. We will be mindful that not all of the reports will be viewed the same way from all of those involved in the incident. As we are not collecting personal information per se, I am not sure there are other biases that we need to be aware of.

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?*

We will keep refining the process of the Reporting Hub – it is very much a test and learn approach currently.

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**?

I don't think anyone would be negatively affected by processing this data.

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?*

We will have clear categories for data that is being recorded. We will also provide training for the hub members on recording the data to ensure they do not record anything that is unnecessary.

b) *How are you ensuring the data used is reliable? (**Data quality**)*

Reporting Hub members are recording what they are told. The data recorded is based on that, and they will be trained in using the software.

i) *What processes do you have in place to ensure maintenance of data accuracy? (**Data integrity**)*

Please see above

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

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

Part of the project is collecting data on incidents across the organisation. We couldn't do this another way. What we could do is run the project without collecting the data.