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	**Individual Risk Assessment Template**	
Project Lead and Information Asset Owner/s	Project Lead	Darren Williams, Health and Safety Manager
	IAO name and asset	Joanna Brown, Director of People and Inclusion
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.*	Individual return to the office Covid 19 risk assessment form to be completed with individual employees should they raise concerns to say that they feel they are at increased risk from Covid due to range of issues – age, health condition, pregnancy or being unvaccinated. As part of the risk assessment, which is done by a manager for their employee we are asking employees to provide information such as their age, health conditions, are pregnant, and Covid vaccination status to allow a personalised return to work risk assessment to be made. There is no requirement for employees to disclose this information to us if they choose not to, but it is accepted that many will feel obliged due to the employee/employer relationship. We will hold a record of this information on Trim, the records management systems used by HR for staff personnel records, but will not report on it in the future. The questions are a prompt that helps us identify whether a person is at more significant risk of contracting covid and therefore enables us to agree with them a set of risk mitigations as part of the assessment process. Completed individual risk assessments are sent by the individual's line manager by email to the secure HR Covid-19 inbox for filing on Trim, the records management system used for staff personnel records.	

	Update October 2022: the vast majority of existing employees when this was introduced, who were happy to complete forms have done so and this is completed. The forms are now only being completed as needed for those who raise concerns that they are at high risk from Covid. The Health and Safety Manager has reviewed the process and concluded that it is still required for those concerned they are at high risk from Covid, and that processing, plus the continued processing by retaining completed forms, given the ongoing covid situation is necessary and proportionate. The situation will be kept under review.
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	Current processing Individual Risk Assessments will remain in place for those staff who are higher risk from getting seriously ill from Covid, such as older people, people with certain health conditions, pregnant women as well as those not vaccinated.

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?	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?	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?	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			
							Change			
2.2	**What data will be processed/shared/viewed?**									
	Personal Data									
	Name	**X**	Date of Birth		Gender		National Insurance Number		Financial Information about the person	
	Address		Email address		Telephone number		NHS No		Other eg a reference number such as Mosaic ref	
	Other data *(Please state):*									
	Special Categories of Personal Data									
	Racial or ethnic origin	x	Fingerprints/ Biometrics		Religious or philosophical beliefs Political opinion					
	Trade Union membership		Physical or mental health or condition							x
	Sexual life or sexual orientation		Housing records Social services records		Tax, benefit or pension records		Employee/HR records			
	Other data *(Please state):*		*Covid vaccination status*							
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?		No							

<table>
<tr><th colspan="4">Step 3: Describe the data processing</th></tr>
<tr><td>3.1</td><td colspan="2">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?</td><td>The data helps us identify whether a person is at more significant risk of contracting covid and therefore enables us to agree with them a set of actions as part of the risk assessment process.</td></tr>
<tr><td>3.2</td><td colspan="2">Explain in as much detail as possible why this is being done</td><td>The Health and Safety at Work etc. 1974 places a legal duty to protect workers from harm, this includes considering the risk to workers who are particularly vulnerable to coronavirus (COVID-19) and put controls in place to reduce that risk.

People at higher risk from COVID-19 include older people, people with certain health conditions and pregnant women as well as those not vaccinated. See Who is at high risk from coronavirus (COVID-19) - NHS (www.nhs.uk) for more information.

To help assess the risk from covid to those who as at increased risk, employers are encouraged to talk to any workers previously defined as clinically extremely vulnerable to explain the measures being taken to ensure they are working safely. There is also a long-standing requirement for employers to put in place measures to ensure workplace safety where a significant health and safety risk is identified for a new or expectant mother.

Understanding the vaccination status of certain individuals who say they are at increased risk will enable us to agree with them proportionate control measures relating to their work.</td></tr>
<tr><td rowspan="3">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>N/A</td><td>N/A</td><td>N/A</td></tr>
</table>

3.4.	**Has a data flow mapping exercise been undertaken?** **If yes, please provide a copy, if no, please undertake**		No
3.5	**How will the information be processed/shared. Details eg secure file transfer**		Completed individual risk assessments are sent by the individual's line manager by email to the secure HR Covid-19 inbox for filing on Trim, the council's records management system used for staff personnel records. With regards to the HR Covid 19 inbox only a small number of nominated staff have access to this while only a limited number of staff have role-based access to the Trim system.

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)(e) "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"	**Special Category data UK GDPR Art 9 condition and DPA18 schedule condition** Article 9 (g) Reasons of substantial public interest (with a basis in law) with the Part 2 of Schedule 1 of the DPA 2018 condition being para 6 statutory and government purposes with the underlying law being the duties under the Health and safety at Work etc Act 1974	**Criminal data UK GDPR Art 10 condition and corresponding art 6 condition** Not applicable
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 Rights Team have advised this is appropriate**		
	Consent is not the legal basis		
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		

	We do not record specific details of why staff are classed as high risk and to ensure accuracy the employee provides the data and we rely on them that the information they are providing is accurate	
4.4	**Have individuals been informed about the proposed use of their data?** For example, do all the organisations/partners who will process the data (inc the council) cover this use in their Processing Notice online	Yes
4.5	**Will you comply with the council's policies on to Subject Access Requests and other data subject rights? Do contracts with any processors for the council contain the council's clauses on data subject rights?**	
	Yes.	
4.6	**Will the processing of data include automated individual decision-making, including profiling?** If yes, please outline the profiling processes and the rights of the data subject	
	No	
4.7	**Data Retention Period - how long will the data be kept?**	
	For a period of 6 years in accordance with our data retention policy (with the exception of those who have worked with children or vulnerable adults, which is 25 years)	
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.*	
	Trim records management system aka Content Manager	
5.2	**Where is the data stored geographically?**	
	Stored on Camden premises – local server at Cressy Road	
5.3	**What roles will have access to the information?** (List individuals or staff groups)	
	Access is role specific to certain HR staff - Business Advisors & Customer Services Advisors	
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**	
	Role based access control is in place	

5.5	**Is there an ability to audit access to the information?**
	Yes - covered by existing arrangements for the Trim (Content Manager) system. Records Management carry out retention audits to identify files that are no longer meant to be kept
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?**
	Covered by existing arrangements for the Trim (Content Manager) system. Different services have different access rights to the system with all data kept separate within the system Council wide retention policy in place which includes HR element and the retention of files and audits carried out to identify those files which are in contravention to this policy
5.7	**Has the Information Security Manager advised on the security measures? What were his/her comments?**
	n/a as existing system used

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**
Privacy intrusion- the privacy implications for staff of being asked intrusive questions about health, vaccination and pregnancy etc by a manager where they may not wish to disclose this information, and may feel that they will be disadvantaged if they do not provide the information. They may feel obliged to provide it due to the employee/employer relationship.	Likely	Minor	Medium/high
Purpose minimisation- risk of managers using data for purposes other than which it was collected for	Possible	Minor	Moderate
Storage- data being held for longer periods than necessary	Possible	Minor	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 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	Employees do not have to disclose this information to us if they don't wish to, it will be made clear to managers their team members have the choice about providing the information and pressure should not be put on staff where they do not want to disclose .	Reduced	Possible, minor - moderate risk	Yes

Purpose minimisation	The date will be held on Trim, a secure system with only small number of role-based employees can access and we will not be reporting on it in the future. Managers will be told that using the information for other purposes is not permitted and will be dealt with as a data breach. This will be clearly communicated to all managers.	Reduced but still moderate	Moderate risk	Yes
Storage	Council wide retention policy in place which includes HR element and the retention of files and audits carried out to identify those files which are in contravention to this policy	Unchanged	Moderate Risk	Yes

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

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? **If not, name of IRO**	No. Sarah Laws
DPO advice	Reapproved 17/11/22 Andrew Maughan, DPO and Borough Solicitor
Information Asset Owner acceptance of residual risks	Jo Brown
This DPIA will kept under review by: (*usually the author or the IAO)*	Darren Williams

Version Control

Version	**Reason**	**Date**	**Author(s)**
1.0	New DPIA	October 2021	Darren Williams and Sarah Laws
1.1	Annual Review	October 2022	Darren Williams 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