Data Protection Impact Assessment (DPIA) - Full Assessment

Guidance for the Project Manager and Sponsor

Use the pre-screening template first. If that shows a high risk in processing the data then you must carry out this full DPIA. **Do not complete this form unless you have already completed the pre-screening and it shows high risk and the DPO as advised you to do a full DPIA.**

The Data Privacy Impact Assessment (DPIA) will enable you to systematically and thoroughly analyse how your project or system will affect the privacy of the people whose data you are dealing with and show how you will minimise the privacy risks. This template has been designed to incorporate the legal requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Conducting a DPIA is a legal requirement under the GDPR particularly if the proposed processing is using new technologies and poses a high-risk to people's data. Further information and guidance on the DPIA is also available on the ICO website here: ICO's PIA code of practice and the Article 29 Working Party here.

GOVERNANCE ARRANGEMENTS

This DPIA will be submitted to the Corporate Information Governance Group (CIGG) and the advice of the Data Protection Officer (DPO) will be sought as part of that process. You must keep the signed DPIA and all supporting documents with your project file for audit purposes.

1. **PROJECT SUMMARY**

Project Name	Covid vaccinations for health and social care staff	**Directorate and Service**	Supporting People and Supporting Communities
Project Sponsor and Position	Jo Brown, Director of People & Inclusion	**Project Manager and Position**	Head of Social Work in Mental Health Head of Transformation & Performance
Project Start Date **Project End Date**	ASAP 01/01/2023	**Project Go Live Date (anticipated/planned)**	Immediate

Third parties involved/associated with the Project:	North Central London CCG (NCL) and the NHS	**Does this DPIA cover multiple projects?**	No
High Level description of the Project: • Facilitating Covid-19 Vaccination of front facing staff including in adult social care, children's and homelessness staff. • Sharing of necessary data with NHS to enable eligible staff to be vaccinated against Covid-19			

2. DESCRIPTION OF THE PROJECT

Include here a plain English description of:

- *the Project (set the context so that it is clear what you want to do)*

  We want to record details in the Oracle HR System of frontline staff that are eligible for priority vaccination (JCVI) due to their role, and of those whether they have received or declined the vaccination.

- *what will be done with the data (the processing activities)*

  Data will be recorded on the employee's existing staff record on the Oracle HR system to confirm date of receiving first and second vaccine or whether they have declined the vaccine.

  Reporting will be done on number/percentage of staff in the eligible group that have been vaccinated. This may include diversity breakdowns, by ethnicity, age, gender, disability to inform the organisations approach to addressing vaccine hesitancy, which may include targeted communications to key groups. This may include personal communications to and discussions with individuals.

  Aggregated (non-individual) data will also be reported onwards to NCL to confirm whether all JCVI staff have received staff to

inform national strategy on offering vaccine.

The reason we are collecting this data is to enable us to confirm to NCL that all eligible staff have had the vaccination or do not wat to have the vaccination - so NCL can then move priority vaccinations on to the next eligible group as part of the government strategy for vaccine roll out.

- *the reasons why you need to process the data (the purpose)*
    - To facilitate the offering of priority vaccination of 'eligible staff' in frontline services, to ensure those that want to be/can be vaccinated receive vaccination ahead of these being offered more widely in the population.
    - Knowing who has been vaccinated and who had declined the vaccination will enable Camden to report accurately to NCL/NHS on coverage of vaccination across the JCVI group. It is important for us to know which staff do not wish to receive the vaccine in order for us to report to NCL/NHS when all eligible staff that want the vaccine have received it and the priority vaccination slots can then be opened up to the wider population.
    - To enable the council to effectively monitor vaccine take up in front line staff and vulnerable staff, as part of its duties as a responsible employer for health safety and welfare of staff and others.
    - Should vaccination be proved effective in limiting individuals passing on C-19 infection to others and/or be effective longer term in eliminating/reducing risk of C-19 illness to the individual. The data will be used to inform risk assessments with the aim of ensuring the Council do their utmost to protect vulnerable residents/other colleagues from C-19 infection.
- *the benefits that this project will provide*
    - This will reduce potential C-19 infections in the following ways. This is beneficial to the health and wellbeing of individuals, ensuring resources are available to deliver frontline services, and more globally supports strategy of reducing infections generally and to limit opportunity for more C-19 variants to develop as well as the easing of pandemic restrictions.
    - Enabling vaccination to be rolled out effectively to priority groups and the general populations as part of the government's strategy. The NHS is at risk of collapse due to Covid pressures and the more health and social care staff who are vaccinated quickly, the better.
    - Enabling managers to make informed decisions on risk assessments for work - that balance the risk to both staff and residents with the aim of ensuring the Council do their utmost to protect vulnerable residents/other colleagues from C-19

infection

- Vaccinated staff will mean that far fewer staff will have to take sick leave, self- isolate or be at risk of serious ill-health or even death. This means that front line services will be able to be maintained and increase over time. Currently there is a risk to residents of mental ill-health due to lack of face to face service provision and this will be significantly reduced as more staff are able to carry out face to face work. There is evidence of this being an approach to meet a public need- there is a widespread vaccination programme throughout the country which is a massive national priority.

- *how the data will be processed (for example, who will carry out the processing and will they use software or other devices to do it)*
  - Data will be entered on to the Oracle HR system by HR staff. Managers have a valid requirement to in having access to this information for the purposes of risk assessments and discussions with individuals to facilitate priority access to vaccination, should they decide to have it after the initial vaccinations of JCVI staff is 'complete'.
- *how will the data be stored?*
  - In the existing Oracle HR Payroll system. Oracle servers are held in the Netherlands and discussions are ongoing with Oracle to regularise the position prior to the end of the UK withdrawal agreement grace period.
- *where have you obtained the data from?*
  - Staff
- *How long will you be processing the data for and how often? For example, once a week for six months.*
  - Ongoing in line with the COPI notice processing conditions (currently 30 September 2021 - though it may be extended)
- *What is the volume of the data? For example, 150 records of service users.*
  - c700 members of staff - current number eligible as per JCVI Priority (workforce) Group 2 definition.

Types of personal data to be processed and data flow map(s):

Personal data:

List the types of data that you intend to process and the types of data subject (for example, names, addresses of residents, service users etc):

- *Refer to this guidance to assess what is personal data:* https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/
    - Data will be entered against the individual's employee record in oracle to confirm
    - Person's Name
    - Job Title (linked with vaccination eligibility)
    - first vaccination - Date - Received/declined at this time
    - second vaccination - Date - Received/declined at this time

Special category data:

List the types of special category data and the types of data subject:

- health information
    - first vaccination - Date - Received/declined at this time
    - second vaccination - Date - Received/declined at this time

- *Refer to this guidance to assess what is special category data:* **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/**
- *Any criminal convictions data?*

None

Data Flows:

- *You may find it useful to use a flowchart, which you can attach at Annex A.*
- *The flowchart should show, for example: Data entry and exit points, location, user categories, data subject categories*

3. DATA PROTECTION PRINCIPLES

This section demonstrates how the project meets the data protection principles.

- 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?
- If the data was originally collected for one purpose and you intend to use it for another purpose, explain how you will inform the data subjects.
- How will you make sure that the data is kept accurate and up to date?
- How long will you keep the data for and how will you destroy it at the end of the retention period?

To avoid accidental recording of vaccine data on non-eligible employees (as per JCVI) the data can only be entered by HR staff. Data will be entered onto the secure Oracle system and retained in line with the COPI notice provisions. The minimum amount of data is being recorded which is a discrete and defined set of data. The oracle system does not allow for free text input which avoids unnecessary data being collected. The data has not been previously collected so there is no repurposing issue arising. The data will be kept up to date by the employee updating the council, but this is considered acceptable in the circumstances. The data will be kept for as long as is required by the COPI notice currently end sept 2021 but this is subject to change. At the end of the COPI notice the council will consider whether there is a requirement to delete the data or not and if not whether there is a legal basis to keep it longer term is this is considered necessary

- Have you cleared the information security arrangements with the Information Security Manager? YES/ NO

- **Record the Information Security manager's comments here:**

n/a - covered by existing arrangements for Oracle HR system. The current issue with Oracle data store in the Netherlands is noted. Negotiations are underway to regularise this position post Brexit

4. BASIS OF PROCESSING

- Which legal basis in Article 6 are you relying on? See this guide to help you identify the legal basis https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/
- If you think you need to rely on legitimate interests then ask the Information and Records Management Team for advice.
- If you are processing special category data, you will also need a legal basis under Article 9 to process this. See this guide to help you identify the legal basis **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/**

If you are processing criminal convictions data or data for law enforcement reasons then you should speak to the Legal team as you need an additional legal basis to do this.

Basis for processing under Art 6 (and Art 9 if special category data): Legal basis is art 6(1)(e) public task, art 9(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, 9 (g) public task and with the Part 2 of Schedule 1 of the DPA 2018 condition being para 6(1) - the exercise of a function conferred on a person by an enactment or rule of law, being the council's duties under the COPI notice and various public health requirements; 9(i) public health with the Part 1 of Schedule 1 of the DPA 2018 condition being para 3 public health. If retention post COPI notice is legally permitted and deemed necessary this DPIA will be updated with an updated legal basis.

5. DISCLOSURES OF DATA

- Will you be transferring/ sharing/giving this data to a data processor or a sub-processor? **YES**
- Tick here to agree that you will be entering into a data processing agreement with them **[Y] We have a contract in place with Oracle and sharing with NCL/NHS is done under existing data sharing agreements**
- Will you be sharing data with any other third party? **YES - sharing with NCL/NHS is done under existing data sharing agreements**
- List the third parties that you propose to share with: North Central London CCG (NCL) and the NHS - inputting numbers of staff into their online vaccination capacity trackers
- Tick here to agree that you will be entering into a data sharing agreement with the third parties **[Y]**

6. TRANSFERS OF DATA OUTSIDE OF THE UK

Will any personal data be processed outside of the UK? YES - Oracle servers are held in the Netherlands and discussions are ongoing with Oracle to regularise the position prior to the end of the UK withdrawal agreement grace period. This is considered an acceptable risk as mitigation efforts are actively underway
See a list of countries here: https://www.gov.uk/eu-eea

If your answer is yes, you must consult the DPO straight away, and see the guidance here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

If there WILL be a transfer out of UK enter comments of the data protection advisor:

Oracle servers are held in the Netherlands and discussions are ongoing with Oracle to regularise the position prior to the end of the UK withdrawal agreement grace period. This is considered an acceptable risk as mitigation efforts are actively underway

7. DATA SUBJECT RIGHTS AND COMPLIANCE WITH CORPORATE POLICIES

Information in Camden contains the Council's policies and procedures on data protection compliance, including how to respond to requests from people to enforce their rights under data protection law.

- You must comply with the requirements in Information in Camden. Tick here to agree that you will be complying with IIC on Data Subject Rights **[Y]** If there is a reason why you cannot do this, please explain why here:

8. CONSULTATION WITH INTERESTED PARTIES

Is one of the outcomes of your project going to make a change which will have a direct effect on data subjects?, For example: introducing CCTV into a library? If so, contact the Information and Records Management Team for advice at dpa@camden.gov.uk about whether you need to consult with stakeholders.

Record the comments of the data protection adviser here:

Advice is to consult with the recognised Trade Unions and relevant staff representation groups - particularly those affecting higher risk groups. • The DPIA was shared with recognised Trade Union representatives and discussed in a meeting on 11/02/2021

9. RISK ASSESSMENT AND MITIGATION

Risk is a combination of **impact**- how bad the effect of the risk would be- and **probability** – the likelihood of the risk happening. Risk is assessed from the perspective of the data subject (as opposed to risk to the Council) and what the impact could be on them as a result of the proposed data processing. For each of the risks you identify:

1. think about how likely they are to occur and categorise them according to **Table 1 in the appendix (e.g., rare, unlikely etc)**.

2. Then consider the impact each risk will have and categorise them according to **Table 2 in the appendix (e.g., minor, moderate etc)**.

3. Then look at **Table 3** and see the risk level. Where the level says mitigations are needed, think about what these will be and how they will reduce the risk level down.

4. Enter the details in the grid below

There is more information on the council's approach to risk here
https://lbcamden.sharepoint.com/sites/intranet/finance/Pages/Risk_Management.aspx

Risk 1	**Risk Level Before any Mitigations**	**Risk Level After Mitigations**
Source of risk: Data is stored on Oracle servers in the Netherlands. **Potential impact on individuals:** Transferring data from the EU server to the UK post the Brexit grace period ending in June 2021 will be difficult, and the current contract with Oracle does not adequately cover this position. The impact may be difficulties in retrieving and processing our data with effects on the data subjects of that. **Threats that could lead to illegitimate access, undesired modification and disappearance of data:** Whilst there is no issue with us sending data to the EU there may be challenges to us obtaining access and sending information back to the UK **Any compliance or corporate risks?** (refer to the council's approach to risk here https://lbcamden.sharepoint.com/sites/intranet/finance/Pages/Risk_Management.aspx if you need to) Risk of breach or GDPR and corporate procedures on information security. **Where mitigations are required what are these?**	12 Likely and Moderate	6 Unlikely and Moderate

The Netherlands is subject to EU data protection regulations and these offer a high standard of protection, equal to (and in some cases better than) under UK_GDPR. During the process of writing this DPIA Oracle have agreed to incorporate standard contractual clauses into the contract which will address the problem; additionally the draft adequacy decision by the European Data Protection Board suggests that adequacy may be obtained by the UK which would also resolve the problem.		
Risk 2	**Details and Risk Level Before any Mitigations**	**Risk Level After Mitigations**
Source of risk: Privacy intrusion -the data being stored relates to individual's medical record and therefore considered very personal and sensitive data. **Potential impact on individuals:** Individuals may consider requests to share this data intrusive and be reluctant to share. They may also have concerns about potential for differential treatment/suffering detriment as a result of them sharing or refusing to share this data. **Threats that could lead to illegitimate access, undesired modification and disappearance of data:** Data held within Oracle/TRIM is secure however there is risk that information is not managed securely outside of the system e.g. storage of individual risk assessments outside of TRIM. **Any compliance or corporate risks?** Risk of breach or GDPR and corporate procedures on information security. **Where mitigations are required what are these?** Data will be stored securely in the oracle system and not made widely available. Data will be used for the defined purposes only and any use of individual data to facilitate activities outside the system e.g. individual risk assessments will be done in accordance with usual process for ensuring this information is managed securely e.g. with completed risk assessments being securely stored on individual's HR TRIM	8 Likely and Minor	6 Possible and Minor

file. Clear communications to staff on what data will be used for and why will be undertaken, acknowledging that they may find the request intrusive. Managers and HR staff that have access to information will be reminded of the importance of ensuring the data is managed securely at all times in line with corporate standards and never stored on an unsecure shared drive/area.		
Risk 3	**Risk Level Before any Mitigations**	**Risk Level After Mitigations**
Source of risk: Data is recorded for staff outside the eligible staff group. Privacy intrusion -the data being stored relates to individual's medical record and therefore considered very personal and sensitive data. They may also have concerns about potential for differential treatment/suffering detriment as a result of them sharing or refusing to share this data. **Potential impact on individuals:** Data is stored for individuals where there is no legitimate interest in breach of their data protection rights. Privacy intrusion -the data being stored relates to individual's medical record and therefore considered very personal and sensitive data. They may also have concerns about potential for differential treatment/suffering detriment as a result of them sharing or refusing to share this data. **Threats that could lead to illegitimate access, undesired modification and disappearance of data:** **Any compliance or corporate risks?** Risk of breach or GDPR and corporate procedures on information security. **Where mitigations are required what are these?** To avoid any accidental recording of data for individuals outside the eligible staff group data will be input to Oracle by HR staff only.	12 Likely and Moderate	4 Unlikely and Minor

10.
OVERALL RISK RATING FOR THE PROJECT AS A WHOLE ONCE THE MITIGATING MEASURES HAVE BEEN PUT IN PLACE:

LOW	**MODERATE**	**MEDIUM/ HIGH**	**HIGH**

ANNEX A: DATA FLOW MAPS

ANNEX B 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	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

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

Annex C:
Any DPO Advice or comments not included above

I am happy with this. Given all the circumstances which are explained in the document this processing is justified.

Andrew Maughan
Borough Solicitor and Data Protection Officer
25th February 2021