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	Caution Register	**Directorate and Service**	Corporate Services
Project Sponsor and Position	Kate Robertson, Director of Customer Services	**Project Manager and Position**	
Project Start Date **Project End Date**	January 2020	**Project Go Live Date (anticipated/planned)**	April 2021

Third parties involved/associated with the Project:	None	**Does this DPIA cover multiple projects?**	no

High Level description of the Project:
The project seeks to create a single organisational 'caution register' and accompanying policy and procedure to capture and appropriately share information on people who may pose a risk to the health, safety and wellbeing of staff. The aim is not to restrict access to services but to ensure appropriate safeguards are put in place to protect staff under the Council's health and safety duties.

It replaces the Council's current arrangements where flags are placed on individual service systems, not shared appropriately or at all and there is no clear policy to ensure fair and equitable decision making, review and challenge.

2. DESCRIPTION OF THE PROJECT

The project seeks to create a single organisational 'caution register' and accompanying policy and procedure to capture and appropriately share information on people who may pose a risk to the health, safety and wellbeing of staff. The aim is not to restrict access to services but to ensure appropriate safeguards are put in place to protect staff under the Council's health and safety duties.

It replaces the Council's current arrangements where flags are placed on individual service systems, not shared appropriately or at all and there is no clear policy to ensure fair and equitable decision making, review and challenge.

A new system will be created using the Council's new CRM system to enable a single source of person data to enable staff (and designed third party contractors) to view if a person or premises is likely to pose a risk to their health, safety or wellbeing, and what mitigations should be taken. The system will hold details of name, address, the nature of incidents and what mitigating actions should be taken. Where a risk is particularly sensitive, the system will not contain details but will instead refer people to the appropriate service for further information.

The system will have a workflow system whereby managers recommend a caution register entry is made and proposed mitigations (2 person visits, pre-arranged meetings at secure premises etc, personal protective equipment for environmental hazards etc). Heads of Service will make the decision to approve or reject the entry and determine a review period of no longer than 12 months. If a decision is made to reject the recommendation, then no entry is stored. Those subject to a flag will be advised of it and the ability to challenge the

decision or mitigation or ask for an earlier review if circumstances have changed. To avoid duplicated records, further incidences will be attached to an existing record to aid decision at review.

Frontline staff and some nominated contractors/trusted third parties will be allowed read only access to the system and will be advised to check the system in advance of visiting a premises or a close interaction with a service user to get the current risk picture. Data will only be shared with third party contractors/ trusted third parties on a need to know basis and in the expectation that only those about to visit or interact with an individual/premises will access the information.

An audit trail coupled with an annual internal audit review will enable checks to be made of unauthorised access/usage.

If after review, the decision the individual or premises no longer poses a risk, the record will be archived and not visible to those with read only access but retained for a period of 2 years in the event of further incidences. After a period of two years with no further incidences, the entry will be removed.

An entry in the register will be based on evidence of a real risk to staff and therefore it is expected that the number of live entries will be relatively small - at less than 500 based on an initial assessment of existing flags in service systems.

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

Personal data:

Names, addresses and nature of risk, mitigations in place for staff visiting the premises

Special category data:

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

Depending on the nature of risk, some sensitive data may be disclosed, for instance high risk drug paraphernalia, aggressive/violent behaviour or previous hate abuse

Data Flows:

See Policy and Procedure document for flows

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?

As set out above – the criteria for inclusion on the register are clearly set out in the policy, and are designed to ensure the minimum amount of data is captured. if the original decision is to reject an entry, no record will be retained. A case management system will ensure structured information capture and workflow for decision making and review. Mandatory reviews of no more than 12 months will ensure the information remains current and accurate with the citizen having the ability to challenge decisions and ask for earlier reviews if circumstances change. Data subjects will be informed of the entry unless there is clear evidence that doing so will lead to escalated risk. Confirmed entries will be retained until review concludes they no longer pose a risk. At this point, entries will be archived and no visible for read only access for a further period of two years in the event of further high risk incidences. If no further incidences occur, the entry will be deleted from the system.

Have you cleared the information security arrangements with the Information Security Manager? YES

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

To be inserted as the CRM system is developed

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):

Art 6(1)(c)Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations). The health and Safety at Work etc Act 1974 places obligations on the council to ensure the health, safety and welfare of its employees and others such as contractors and partners who may be affected by its actions.

Potentially in some cases where there is a serious threat, art 6(2) (d) and 9(c) **Vital interests:** the processing is necessary to protect someone's life.

Art 6(2)(e) and 9(g) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. The legal basis for art 9 is DPA 18, schedule 1, part 2, para 6 (Health and safety at Work etc Act 1974 the para 2(a) enactment)

5. DISCLOSURES OF DATA

- Will you be transferring/ sharing/giving this data to a data processor or a sub-processor? **Yes, through a log in real time live system, controlled by role base access control with relevant people at trusted partners only, and in some limited cases secure sharing of**

updated records

- Tick here to agree that you will be entering into a data processing agreement with them **[Yes]**
- Will you be sharing data with any other third party? **Third party contractors likely to be exposed to risks by directly interacting with or visiting a high risk person or premises**
- List the third parties that you propose to share with: main housing repairs contractors, local police, enforcement agents working on our behalf
- Tick here to agree that you will be entering into a data sharing agreement with the third parties **[yes]**

6. TRANSFERS OF DATA OUTSIDE OF THE EEA

Will any personal data be processed outside of the UK? NO
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 EEA enter comments of the data protection advisor:

n/a

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 **[x]** If there is a reason why you cannot do this, please explain why here:

n/a

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 Rights 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:

It is advised that you engage with the main unions to gain their views. And if there are representative groups of eg social workers or inspectors these should also be consulted

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

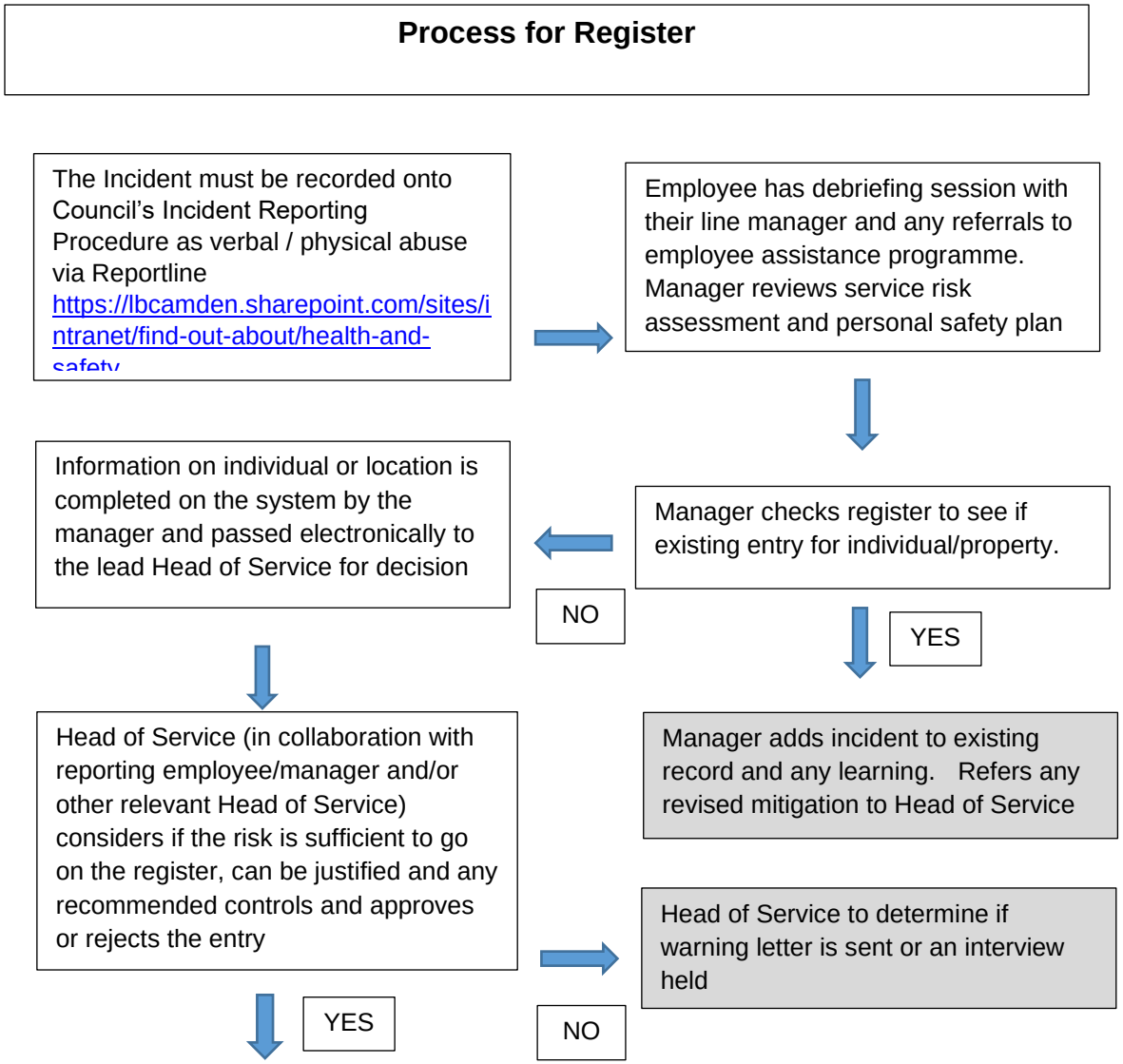
Risks *[include as many rows as necessary to identify each risk individually]*	**Risk Level Before any Mitigations**	**Risk Level After Mitigations**
1. Security breaches leading to large loss of personal data – reputational damage to the council and data subjects and potential risk of harm. Mitigation - the data will be restricted from being downloaded to personal devices and IT system stored within Council's secure network. Council laptops are encrypted and the Council's network up to date with security patches. Role based access control is in place and reviewed. Access is audited. All internal staff subject to code of conduct, externals will sign an AUP.	Impact Major and likelihood possible, overall:12 (medium high)	Impact Major and likelihood rare- 4 (low)
2. Unauthorised or inappropriate access to the data by council employees – sensitive personal data shared in breach of data protection. Mitigation – role based access control, workflow routes for decision making, audit trail of usage and added to internal audit annual programme. Effective training and communication to users. Link to active directory for password protection. All internal staff subject to code of conduct, externals will sign an AUP.	Impact Major and likelihood possible, overall:12 (medium high)	Impact Major and likelihood rare- 4 (low)
3. Inaccurate or out of date data leading to unnecessary restrictions being placed on people's access to services. Mitigation – mandatory reviews at no more than 12 months with escalations if not completed. Users required to check each time they visit or interact to ensure they receive latest information. Data subjects can challenge accuracy of events or decision.	Impact Moderate and Likelihood unlikely : 6 (medium)	Impact moderate and likelihood rare 3 (low)
4. Unauthorised modification or deletion of data leading to risky individuals or premises not being recorded, putting employees at potential risk. Mitigation – data held in secure system with audit trail of actions and rules re: deletion, role based access to approve or amend records	Impact Moderate and Likelihood	Impact moderate and likelihood rare 3 (low)

	unlikely : 6 (medium)	
5. Unauthorized sharing with/use by third parties/contractors. Mitigation – any data sharing covered by data sharing agreements and linked to clear requirement and reasonable expectation of interacting with high risk premise or individual. Externals will sign an AUP	Impact major and likelihood possible : 12 (medium high)	Impact moderate and likelihood rare: 3 (low)
6. Inherent privacy intrusive nature of the register, is an interference with privacy and private life, leading to concerns by data subjects, distress and embarrassment Mitigation- the system only holds information where an assessment has held the data is necessary, and systems in place for review and removal at appropriate intervals. Remaining intrusion is considered acceptable compared to the harms being prevented	Impact moderate and likelihood likely : 12 (medium high risk)	Impact moderate and likelihood possible- medium high

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



Register is updated with decision, relevant codes, review date and any detail (including access restrictions).

A letter is sent to the individual informing them that their name/location is now being held on Caution Register, review date and how to request review.

Head of Service decides if the letter should be sent based on risk assessment*. If no fixed address or unknown, the letter should be held on the system for next interaction

Within 10 working days

Individual requests review to service director with any errors or mitigations. Director decides outcome within 10 working days and writes to confirm

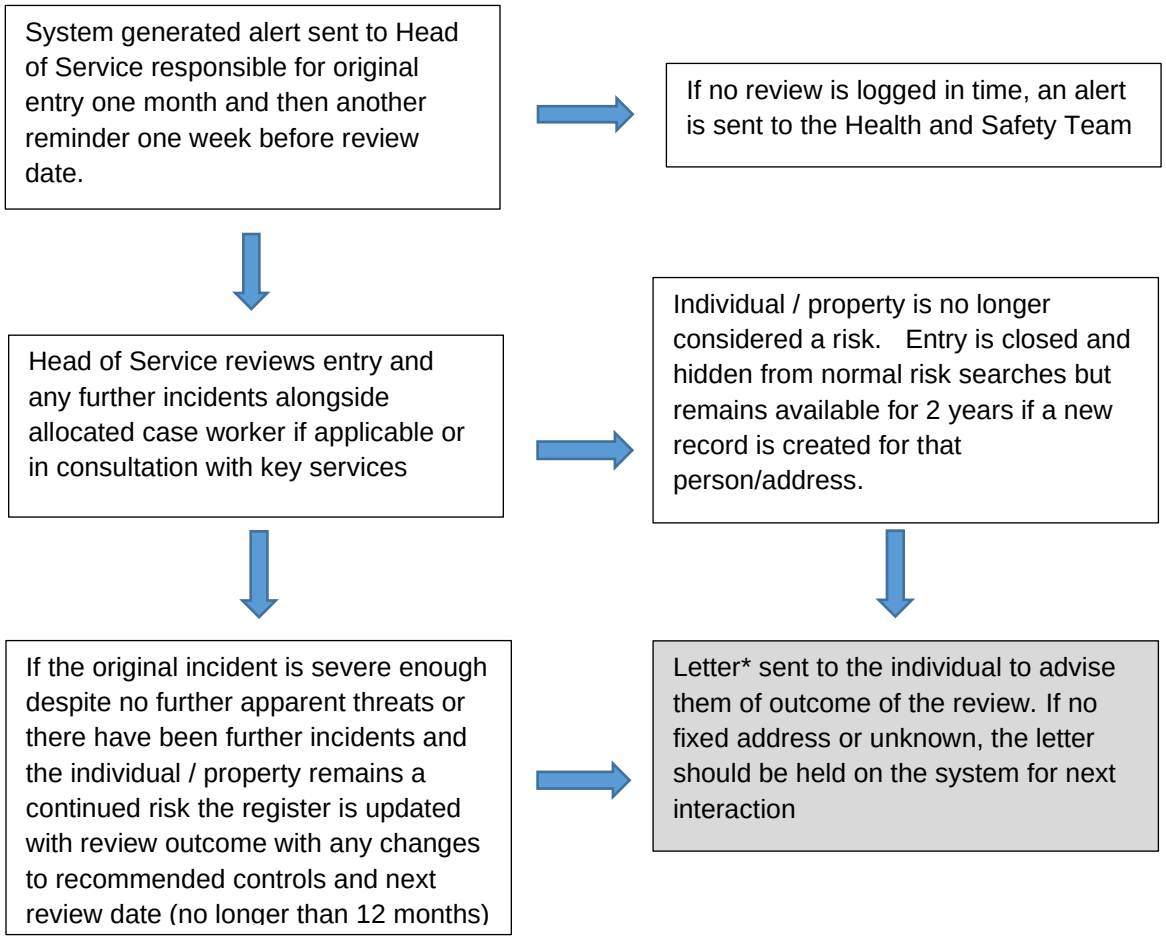
Entry is confirmed, deleted or amended

Process for Officers

All relevant staff dealing with individuals or visiting properties **MUST** check the register before arranging or attending a visit (including visits to Council buildings). The recommended precautionary action should be followed including alerting security and/or booking secure meeting rooms.

Any subsequent incidents should be logged against the original entry on the system as and when they occur by service managers, including any commentary re: escalation of risk

Process for Reviews



***In specific cases where informing the individual might create a substantial risk of a violent reaction from them or cause the individual unwarranted harm or distress, it may not be sensible to inform the individual.*

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

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
	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

Annex C DPO Comments

I think this is justified. While there is clearly an impact on those who appear on the list the reason why we are maintaining this list is fully justified. Also the procedures around this list also seem sound and appropriate and do offer protection to the individuals involved.

Andrew Maughan
Borough Solicitor
4th March 2021