Data Protection Impact Assessment

A Data Protection Impact Assessment ("DPIA") is a process that assists organizations in identifying and minimizing the privacy risks of new projects or policies.

The DPIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

Working through each section of this form will guide you through the DPIA process.

The requirement for a DPIA will be identified by answering the questions below If a requirement has been identified, you should complete all the remaining sections in order.

Conducting a DPIA should benefit the Council by producing better policies and systems, and improving the relationship with individuals.

The Data Protection Impact Assessment Statement in **Section 7** should be completed in all cases, and a copy of this document should be sent to the Data Protection Officer to record and review.

The Data Protection Officer will review the DPIA and will provide feedback. The feedback will confirm whether the proposed measures to address the privacy risks identified are adequate, and make recommendations for additional measures needed.

These measures will be reviewed once in place to ensure that they are effective.

Advice can be found at the beginning of each section, but if further information or assistance is required, please contact the Data Protection Officer on 01923 278362 or via email to bahzad.brifkani@watford.gov.uk.

More information on DPIA can be found on ICO website

This checklist helps you make that assessment and provides a springboard for some of the issues you will need to consider in more detail if you do need to carry out a DPIA.

1. Are you collecting more than an individuals' name and contact details.

   Yes ☒ No☐

2. Are you going to use the data you collect to do any evaluation or scoring relating to that individual

   Yes ☐ No☒

3. Is the system you are going to use able to make automated decisions relating to the individual

Yes ☐ No☒

4. Is the system capable of undertaking systematic monitoring of the individual

   Yes ☐ No☒

5. Is the system going to process sensitive or highly personal data

   Yes ☒ No☐

6. Is the system going to process large volumes of personal data

   Yes ☒ No☐

7. Is the system going to be used to record the personal data of vulnerable individuals

   Yes ☒ No☐

8. Is the system using untried or cutting edge technology

   Yes ☐ No☒

If you have answered Yes to any of these statements a DPIA may be required

Section 1 - Identifying the Need for a DPIA

Briefly explain what the project aims to achieve, what the benefits will be to the Council, to individuals, and to other parties.

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

The Joint Safeguard and Domestic Abuse policies bring together partner organisations and the council to identify and support people experiencing abuse. This involves collected storing and sharing sensitive data about individuals. The support offered will be provided by the Council and its partners. This will require keeping and sharing sensitive personal data about vulnerable individuals to ensure victims and those at risk of abuse are properly supported and that any suspicions of abuse can be investigated by the appropriate organisation.

Section 2 - Describe the Processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

All allegations of abuse will be centrally recorded and the Designated Safeguarding officers and their Managers will be responsible for collating and monitoring referrals and reporting these to the Council's Safeguarding Group.

Effective information sharing underpins integrated working and is a vital element of both early intervention and safeguarding. Information sharing agreements are in place with the partners the service works with to safeguard vulnerable adults and children

Describe the scope of the processing:

Does it include special category or criminal offence data?

Yes. Special category data will be processed as well as criminal offence data.

How much data will you be collecting and using?

The data collected could potentially be from several different agencies and could be substantial.

How often?

This is included in the Information Sharing agreement already in place.

How long will you keep it?

The data will be securely retained indefinitely. This allows the Council to respond to any future serious incidences which may be subject to a serious case review and may involve cases that do not have a statute of limitations. The data obtained will be used to ensure that safeguarding issues are addressed. Once the information is no longer needed it will be deleted.

How many individuals are affected?

There will be few individual cases referred annually where we will need to store their data

What geographical area does it cover?

Only data about Watford individuals will be stored by the Council

Describe the context of the processing:

What is the nature of your relationship with the individuals?

The individuals could be suspected perpetrators of abuse or potential victims

How much control will they have?

The individual will have little control over the data we hold due the potential criminal offences involved

Do they include children or other vulnerable groups?

Yes the data will relate to children and vulnerable groups

Are there prior concerns over this type of processing or security flaws?

No

What is the current state of technology in this area?

Cases that are referred are currently kept in an excel spreadsheet. Access is limited to the Safeguarding Manager, the Community Safety Manager and the Environmental Health Manager (Communities).

Are there any current issues of public concern that you should factor in?

No

Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The service has information sharing agreements with all partners the Council shares data with.

Describe the purposes of the processing:?

What do you want to achieve?

The data relates to sharing information related to potential safeguarding concerns. Sharing data has been shown to be critical to safeguarding residents from abuse and to ensure that the appropriate agencies are able to support the individual.

What is the intended effect on individuals?

Sharing safeguarding data will reduce the harm caused to victims of abuse and prevent perpetrators from continuing their abusive behaviour.

What are the benefits of the processing – for you, and more broadly?

Sharing data helps the Council meet its statutory safeguarding responsibilities and to protect vulnerable residents

Section 3 – Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

No

Section 4 Necessity and Proportionality

Describe compliance and proportionality measures, in particular:

What is your lawful basis for processing?
The following substantial public interest conditions set out in Schedule 1 of the DPA 2018 apply to the both the Safeguarding and Domestic Abuse policies:

- Statutory and government purposes
- Preventing or detecting unlawful acts
- Protecting the public
- Regulatory requirements
- Suspicion of terrorist financing or money laundering
- Support for individuals with a particular disability or medical condition
- Safeguarding of children and individuals at risk

Does the processing actually achieve your purpose?
Yes: Sharing information about vulnerable people at risk will meet the conditions set out above and will meet our legal obligations to safeguard vulnerable adults and children

Is there another way to achieve the same outcome?
No: Agencies need to process data so that victims of abuse are supported by all partner agencies and patterns of abuse can be identified

How will you prevent function creep?
The DPIA will be reviewed annually to ensure the aims of the data sharing remains in line with the current policies

How will you ensure data quality and data minimization?
These polices fall under data sharing agreements and the quality and quantity of data is set out in that agreement.

What information will you give individuals?

Information will only be withheld from the individual if it is in the interest of the vulnerable adult or child.

How will you help to support their rights?
We will support the individual's rights by being rigorous when assessing whether to inform the individual about the information held and to ensure that there is limited access to their data.

What measures do you take to ensure processors comply? How do you safeguard any international transfers?

There will be no international transfers of data

Section 5- Identifying the Privacy Risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Hackers get access to the data through breaches in WBCs or partners databases.	Remote	Severe	Medium
People obtaining access to the data without a legal reason	Possible	Minimal,	Medium
Perpetrators of abuse might get information about the victim if there is unauthorized access to the data	Unlikely	Severe	Medium

Section 6- Identifying measures to reduce the Risks

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
	Corporate information security in place Files containing sensitive data will be password protected and access restricted to officers who need it to carry out their safeguarding duties and to provide resilience	Reduced	Low	Yes/no

Section 7 – Sign Off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA