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 via email to WatfordDP@hertfordshire.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.

Project Aims

The Joint Safeguard and Domestic Abuse policies bring together partner organisations and the council to identify and support people experiencing abuse and require safeguarding. This would include but is not limited to physical abuse; mental abuse and financial abuse. This involves storing sensitive data about individuals.

The data stored will assist with the assessment of risk and ensure the safeguarding of adults and children at risk within Hertfordshire and aims to:

a) Prevent death or serious harm
b) Enable early interventions to prevent the escalation of risk
c) Reduce repeat victimisation
d) Enable the review of safeguarding processes in the event of the death or serious injury of adults who are in need of care and support.
e) Enable audit of partner systems and processes to ensure objectives are met and adults are safe-guarded.

Benefits to the Council and Partners

Through the sharing of data the Council and partners will be meeting their statutory to safeguard vulnerable residents and employees.

Data sharing is a key factor identified in many serious case reviews (SCRs), where poor information sharing has resulted in missed opportunities to take action that keeps vulnerable adults and children safe.

The support offered will be provided by the Council for example the housing Service and its partners for example Social Services and Watford Community Housing. This will require keeping 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.

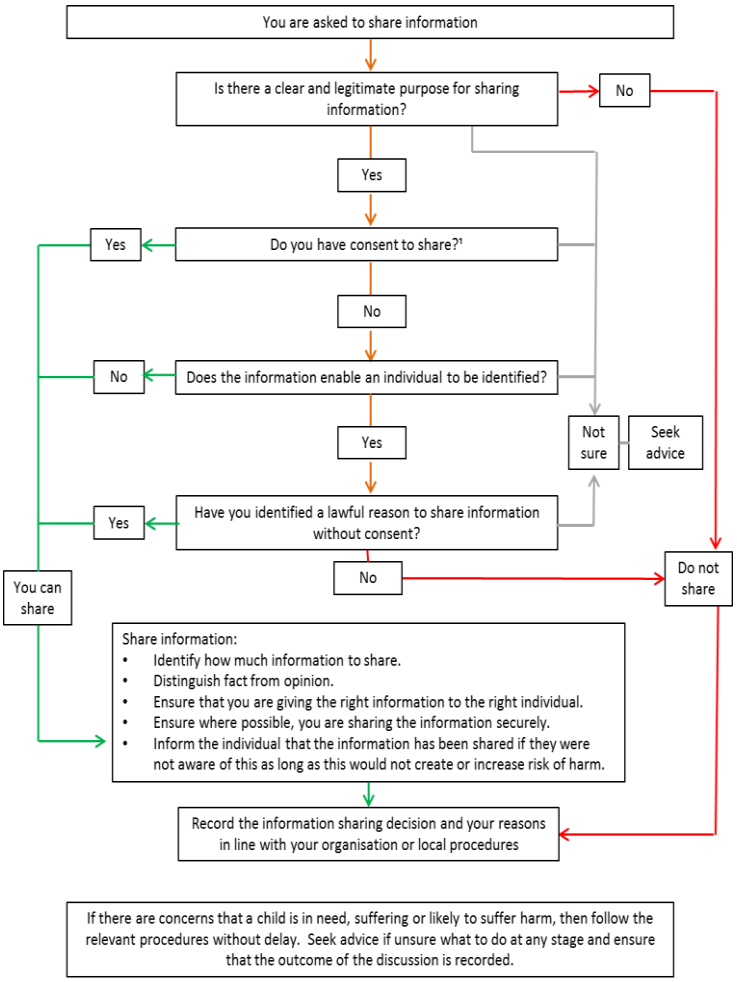
Section 2 - Describe the Processing

1. **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?

Where there are safeguarding concerns a referral will be made to the statutory agencies for example to Social Services. Information is centrally recorded by Adult Social Services and copy of the referral kept by the safeguarding manager

Data related to safeguarding referrals reported to Watford's safeguarding Manager will be stored in a folder in the main drive with restricted access. The Safeguarding and Community Safety manager have access to this data and only the Head of Service can authorise access for officers.

The data held by Watford Council will only be shared with relevant partners in accordance with the data sharing agreement and in most cases only where there are concernss that theprevious referrrals have not been actioned. The data will be updatd as and when new referals are made. All data will be kept for 10 years after the last action is recorded. The decision whether data should be shared is based on the following;



Does it include special category or criminal offence data? Yes.
Information to be shared includes but is not limited to:

- relevant data from social care records
- medical information
- housing status

How much data will you be collecting and using?
Data stored will only relate to cases originating in Watford to assist in identifying trends ensuring that adequate service provisions are available to people in Watford

How often?
As each referral is reported the spreadsheet will be updated

How long will you keep it?
The data obtained will be used to ensure that safeguarding issues are addressed. The data will be stored for 10 years after the last action on the spreadsheet.

How many individuals are affected?
On average 4 referrals are made per month.

What geographical area does it cover?
Only data about Watford individuals will be stored by the Council. The central database may contain significantly more information which could include information about a non-resident of Watford. However only information taken from the referral form will be stored by Watford Council

Describe the context of the processing:

What is the nature of your relationship with the individuals?

The individuals will either reside in the community or work for the Council

How much control will they have?

In the case of an adult unless there is a risk of significant harm the referral will be made with their consent.

If either the victim or perpetrator work for the Council a senior HR advisor will be consulted.

Do they include children or other vulnerable groups?

Yes the data will relate to children and vulnerable adults

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

No

What is the current state of technology in this area?

Referrals are currently kept in an excel spreadsheet. Access is limited to the Safeguarding Manager, the Community Safety Manager and the Head of Service. Further authorisations will be approved by the Head of Service.

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)?
No relevant certification schemes have been approved by the ICO to date.

Describe the purposes of the processing:?

What do you want to achieve?

The reason for storing the data is to identify abuse and safeguarding issues and more effectively align services to their need. Storing 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.

Collecting this data also allows the service to identify any trends in abuse in the borough

What is the intended effect on individuals?

Storing safeguarding data will assist in reducing harm caused to victims of abuse and those in need of safeguarding 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 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. This is a task in public interest, we have a statutory duty to co-operate with others to prevent and reduce abuse.

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 policies 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.

Investigation and detection of criminal offences are exempt from privacy notice requirements, The policy document is published on the Councils website. https://www.watford.gov.uk/downloads/file/3803/special_category_and_criminal_offence_policy

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

The service always tries to achieve consent from the individual unless there is a risk of significant harm

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 including where the subject of the referral is an employee.	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	Reduced	Low	Yes
	Files containing sensitive data will be password protected and access restricted to officers who need it to carry out their safeguarding duties	Reduced	Low	Yes

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:	Elaine Dunnicliffe	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Elaine Dunnicliffe	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Duty on public authorities to co-operate in relation to safeguarding vulnerable adults and children mean this is necessary processing and sharing of information. Guidance in flowchart requires on relevant information to be shared. Officers should ensure they provide material which is required to support safeguarding concerns but be aware this may not require historic elements of a file such as housing which do not impact on safeguarding concerns.		
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