

Data Protection - Data Privacy Impact Assessments & Privacy Notices Policy

Definitions

Data Protection Act 1998 (“DPA”) - The law on data protection in the UK

General Data Protection Regulation (“GDPR”) - A new law on data protection that came into force on 25 May 2018 throughout Europe

Data Controller - A person or organisation that handles and processes personal data and determines the way such data should be processed

Personal Data - Any information from which a living individual can be identified

Sensitive Personal Data - Any Personal Data which includes further information as defined in the DPA. Further information includes (i) racial or ethnic origin; (ii) political opinions; (iii) religious beliefs; (iv) membership of a trade union; (v) physical or mental health or condition; (vi) sexual life or preferences; (vii) information about any criminal offence or court proceedings related to a criminal offence

Information Commissioner’s Office (“ICO”) - The statutory regulator of the DPA and the GDPR

Privacy Notice - A description of Personal Data held by the Council, along with details of purpose, retention and other information about how the Council will handle the Personal Data

Data Subject - As defined in the DPA and the GDPR. The Data Subject is the person who the Personal Data is about, or who is identified by the Personal Data

Data Privacy Impact Assessments (“DPIAs”) - The requirement under the GDPR to impact assess all Personal Data that is held and record all processing activities

Statement

Chippenham Town Council (“the Council”) represents the local community, delivering services to meet needs and improving the quality of town life for present and future generations.

In order to make this happen, the Council collects and uses Personal Data about residents, staff, volunteers, councillors and other individuals who all play their part in the community. This information is gathered in order to enable the Council to provide its services. In addition, there may be a legal requirement to use information for the purpose of sharing it with other organisations. In some cases,

the Council must collect information to ensure that it complies with statutory obligations.

The Council holds personal and sensitive data. It is responsible for safeguarding the data it holds and is legally bound under the GDPR to ensure the security and confidentiality of personal information processed. These responsibilities extend to other organisations working on behalf of the Council. The Council will only ever hold Personal Data that it is required or permitted to hold in accordance with lawful processing provisions.

Purpose

A Data Protection Impact Assessment (DPIA) allows the Council to evaluate the risk to individuals of the Council processing Personal Data relating to them. If, as a result of a DPIA indicating a high risk to any individual in the processing of that person's Personal Data, the Council will first consider what mitigation can be applied to reduce that risk, or the impact of that risk. If the risk cannot be mitigated, then the Council will consult with affected individuals and seek the approval of the ICO.

Staff and Councillors are expected to adhere to the principles and spirit of this Policy in order to protect Personal Data belonging to our residents, staff and community. Employees found to have breached this Policy may find that the Council will invoke disciplinary procedures.

This Policy has been approved by the elected members of the Council, and is evidence of the commitment the Council makes to safeguarding Personal Data.

Data Protection Impact Assessments

DPIAs are the most effective tool to enable the Council to identify the best way to comply with its data protection obligations and meet individuals' expectations of privacy.

When must a DPIA be carried out?

The Council will carry out a DPIA in the following circumstances:

1. Prior to the introduction of the GDPR in May 2018, to all of the Council's processing activities which involve Personal Data;
2. When new technologies are contemplated;
3. When the processing is likely to result in a high risk to the rights and freedoms of individuals;

4. When the processing is likely to result in a high risk that includes systematic and extensive processing activities such as:
 - a) Profiling
 - b) Decisions that have legal or significant effects on an individual
 - c) Large scale processing of Sensitive Personal Data or Personal Data relating to criminal convictions or offences
 - d) Large scale, systematic monitoring of public areas (e.g. CCTV)

What information should the DPIA contain?

The DPIA must contain the following information:

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the Council
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An assessment of the risks to individuals
- The measures in place to address risk, including security

How should the template be used?

Staff must complete the template contained in this Policy and present it to the Council's Data Protection Officer (DPO) for approval. The DPO will either approve the DPIA and maintain a record of it or reject it and return it to the member of staff explaining why it has been returned. The member of staff must then determine whether they wish to continue the particular processing activity or not. If they do wish to continue, they should engage with the DPO and make any changes identified by the DPO.

How often must a DPIA be reviewed?

DPIAs once approved must be reviewed either

- a) Annually
- b) Whenever the nature or method of the processing activity changes, including where more (or less) Personal Data is to be collected or where the Council wishes to use Personal Data collected for one purpose for a different purpose.

Lawful Basis for Processing

All Personal Data that is handled or collected by the Council will fit into one of the categories below:

Consent

The data subject has consented - specifically, and with affirmative action - to the processing of the Personal Data. Evidence of this consent should be attached to the DPIA.

Necessary for a Legal Obligation

There is a “clear and precise” statutory obligation that makes it necessary for the Council to collect and process the Personal Data. The relevant statutory obligation should be referred to in the DPIA.

Contractual Obligation

There is a contractual obligation for the Council to process the Personal Data. The contract should be attached to the DPIA.

Vital Interests

The processing of the Personal Data is in the vital interests of the individual, such as to protect someone’s life.

Legitimate Interests

The processing is necessary for reasons such as internal administration, network and information technology provision (including being able to prevent unauthorised access to electronic communications), or prevention of crime or fraud.

Public Task

The processing is necessary for the Council to perform a task in the public interest or for the Council’s official functions, and the task or function has a clear basis in law.

Privacy Notices

Each Data Subject is entitled to basic information about the nature of and manner in which the Council holds their Personal Data. This is known as a Privacy Notice. The GDPR states what information must be provided.

Identity of Council

To include contact details of the Data Protection Officer.

Content

To include the purpose and legal basis for the processing.

Recipients

Who the Personal Data will be shared with.

Retention

The period for which the Personal Data will be retained.

Individual Rights

What the process is for Data Subjects to pursue their rights to:

- Access their data
- Object to their data being used
- Require the Council to rectify incorrect data
- Delete their data

Complaint

The right to complain to the ICO.

Source

The source of the data.

The Council will always publish any Privacy Notices in respect of Personal Data that it holds, usually on its website. Anyone who has difficulties accessing the website can request a paper hard copy by contacting the Council's Head of Corporate Support.

Privacy Notices will be reviewed as often as is necessary, and at least annually.

Training & Development

The Council is committed to ensuring the staff and councillors adopt the highest standards in relation to the processing and handling of Personal Data.

All existing staff and councillors will be trained within 6 months of the dissemination of this Policy.

New staff and councillors will be trained as part of their induction within 3 months of their joining the Council and being able to access Personal Data.

Staff and councillors will be re-trained according to their needs against the tide of new guidance and legislation. It is anticipated that this will usually be annually.

No member of staff or councillors will have access to any Personal Data unless they have read this Policy first.

Further Information

Any person reading this Policy requiring further information or assistance is invited to contact the Council's Head of Corporate Support.

Where any person has a complaint about the way the Council has handled their Personal Data or that of their child's, they may address their concern in writing to the Chief Executive.

For further information about the DPA, GDPR and its application, the Information Commissioner's Office has a wealth of information on its website - www.ico.org.uk

APPENDIX A - DPIA Template

Data Privacy Impact Assessment ("DPIA")			
<i>Please leave this blank (to be completed by the DPO)</i>			
DPIA Reference Number:			
Title or brief description of processing activity:			
Name of person completing DPIA:		Department:	
Version:		Date:	
Approvals			
Please ensure that approval is also sought from the Data Protection Officer			
Name	Job Title	Approved (Yes / No)	Date
	Data Protection Officer		
Distribution			
Please ensure that a copy once approved is sent to the Data Protection Officer for record-keeping			
Name	Job Title	Reason for Distribution	Date
	Data Protection Officer		
Version History			
Version	Reason for change	Author	Date

Screening Questions
Description of process or activity Give a detailed explanation, attach relevant reports or papers, explain why the processing is necessary and proportionate

What Personal Data will you be processing? List the type of personal data that you will be collecting					
What is the lawful basis for processing Select (x) only one					
Consent		Contractual obligation		Legitimate interests of the organisation	
Statutory obligation		Vital interest of the data subject		Public Task	
Explain the lawful basis you are relying on Attach any relevant documents (e.g. contracts, evidence of consent)					
Impact on individuals Explain whether there will be any negative impact on or risks to the affected individuals					
Measures Explain what measures will be put in place to mitigate the impact (e.g. security, deletion, redaction, encryption, restricting access, staff training)					
How many individuals' Personal Data will be affected? Enter the number of individuals					

	Yes (x)	No (x)
Will the personal data collected include "Special Categories of Personal Data"? These include medical/health, religious, political, racial/ethnic or trade union data		

Will the personal data collected include “criminal offence data”?		
Will the data be used for profiling purposes? Profiling means making automated decisions (typically involving algorithms or IT systems) that would have an impact on a person’s life		
Will the activity compel individuals to provide their Personal Data?		
Are you using the Personal Data for a purpose it is not currently used for?		
Does the processing activity involve new technology? This might be perceived as being privacy intrusive. For example, the use of biometrics or facial recognition.		
Is the processing activity likely to be intrusive to an individual’s privacy?		
Will the Personal Data be shared with other organisations?		
If so, who and why? Please include a copy of the contract or agreement governing the sharing of information		

APPENDIX B - Legitimate Interest Assessment

This LIA form should be completed in conjunction with a DPIA, where the “Legitimate Interests” box is ticked.

Legitimate Interests Assessment (“LIA”)			
<i>Please leave this blank (to be completed by the DPO)</i>			
DPIA Reference Number:			
Title or brief description of processing activity:			
Name of person completing DPIA:		Department:	
Version:		Date:	
Checklist Please tick all that apply. If any boxes are not ticked, you may not submit the DPIA for approval until or unless you have rectified the processing so that all the boxes can be ticked			

Please check	Description
☐	We have checked that legitimate interest is the most appropriate basis.
☐	We understand our responsibility to protect the individual's interests.
☐	We have conducted a legitimate interest assessment (LIA) and kept a record of it, to ensure that we can justify our decision.
☐	We have identified the relevant legitimate interests.
☐	We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.
☐	We have done a balancing test and are confident that the individual's interests do not override those legitimate interests.
☐	We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.
☐	We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.
☐	If we process children's data, we take extra care to make sure we protect their interests.
☐	We have considered safeguards to reduce the impact where possible.
☐	We have considered whether we can offer an opt out.
☐	We keep our LIA under review and repeat it if circumstances change.
☐	We include information about our legitimate interests in our privacy information.

APPENDIX C - Privacy Notice Template

Privacy Notice
What is our lawful basis for processing this data
What data do we collect [The categories of this information that we collect, process, hold and share include]
Why do we need it and what do we do with it
How long do we keep it
Who we share this information with and why [Other than this, we/We] do not routinely share this information outside of our organisation, but may share this information with our legal or trusted advisers for the purpose of obtaining

advice, with government agencies if required by law, or with law enforcement agencies for the prevention or detection of crime.

What are your rights

You have a number of rights in relation to your personal information under data protection law. In relation to most rights, we will ask you for information to confirm your identity and, where applicable, to help us search for your personal information. We will respond to you within 30 days after we have received any request (including any identification documents requested).

You have the right to:

1. Ask for a copy of the information that we hold about you;
2. Correct and update your information;
3. Withdraw your consent (where we rely on it).
4. Object to our use of your information (where we rely on our legitimate interests to use your personal information) provided we do not have any continuing lawful reason to continue to use and process the information.
5. Erase your information (or restrict the use of it), provided we do not have any continuing lawful reason to continue to use and process that information;
6. Transfer your information in a structured data file (in a commonly used and machine-readable format), where we rely on your consent to use and process your personal information.

Please see our Data Protection Policy for further information and for details of how to make a request.

Contact information

You can exercise the above rights and/or manage your information by contacting us using the details below:

Identity of data controller: Chippenham Town Council

Postal address: The Town Hall, High Street Chippenham, Wiltshire, SN15 3ER

Email: enquiries@chippenham.gov.uk

Phone: +44 (0) 1249 446699

Our Data Protection Officer is One West and you can contact them at

one_west@bathnes.gov.uk

Complaints

If you wish to raise a complaint on how we have handled your personal data, please contact us at enquiries@chippenham.gov.uk

If you are not satisfied with our response you can complain to the Information Commissioner's Office (ICO). The ICO's contact details are below:

Postal address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Email: casework@ico.org.uk

Phone: 0303 123 1113