CHIPPENHAM TOWN COUNCIL
Improving the quality of town life

Data Protection Policy

Policy Statement

Chippenham Town Council issues this policy to meet the requirements incumbent upon them under The Data Protection Act 2018 for the handling of personal data in the role of controller. If appropriate it can also be used for the control and release of data under the Freedom of Information Act 2000.

This policy should be read in conjunction with other Council policies such as the Data Retention Policy, Data Breach Policy, Freedom of Information Policy, Communications Acceptable Use Policy, Disciplinary Policy and Employee Code of Conduct.

Scope of Policy

This policy applies to all employees of Chippenham Town Council including contract, agency and temporary staff, volunteers and employees of partner organisations working for Chippenham Town Council (herein referred to as "the Council").

Review Statement

This policy has been prepared considering prevailing legislation and recognised good practice. New legislation requirements or changes in current legislation may necessitate the review of this policy document. The council will continue to review and amend all or part of this policy on a regular basis. It is the employee's responsibility to ensure that the copy of the policy being referred to is the most up-to-date version.

Equality

In putting the policy into practice, no aspect will discriminate on the grounds of race, sex, sexual orientation, gender reassignment, age, religion, politics, marital status, disability, union membership or any other grounds likely to place any employee at a disadvantage.

Legal Principles

In execution of this policy Chippenham Town Council will comply with the data protection principles of the GDPR specified in Article 5. These are that personal data be:

a) processed **lawfully, fairly and in a transparent manner** in relation to individuals

b) collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

c) **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed

d) **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

e) kept in a form which permits **identification of data subjects for no longer than is necessary** for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the law in order to safeguard the rights and freedoms of individuals

f) processed in a manner that **ensures appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

Chippenham Town Council will adopt the appropriate technological and organisational measures to ensure compliance with the Data Protection Principles by carrying out the necessary procedures. In all aspects of our work we will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of our work. The rights of the data subject as defined in law are:

a) The right to be informed in a clear, concise and transparent manner

b) The right of access

c) The right to rectification

d) The right to erasure

e) The right to restrict processing

f) The right to data portability

g) The right to object

h) Rights related to automated decision making

Sensitive Personal Data

In most cases where we process sensitive personal data, we will require the data subject's explicit consent, unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). In the vast majority of data processing activities, a statutory power will be the reason for data processing. Any such consent will need to clearly identify what the relevant data is, why it is being processed, to whom it will be disclosed and an appropriate method of removing the individual's personal data should consent be revoked.

Accuracy and Relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data

obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this. Individuals may ask that we correct inaccurate personal data relating to them.

Your Personal Data

Individuals must take reasonable steps to ensure that personal data we hold about them is accurate and updated as required. For example, if personal circumstances change, the changes should be reported to your Line Manager, so that they can update their records.

Data Security

Individuals must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing Data Securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded, or sent to our secure disposal company when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly
- Data stored on CDs or memory sticks must be encrypted and locked away securely when they are not being used
- The DPO must approve any cloud used to store data
- Data should never be saved directly to mobile devices such as tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data Retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines. For further information please see the Data Retention Policy.

Data Protection by Design

It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data must be assessed with a Data Protection Impact Assessment. Prior to the assumption of any such activity the DPO must be consulted and an initial screening be conducted to assess the risk.

Any activity involving the processing of personal data must be registered on the Register of Processing Activity and reviewed at the very least annually.

Transferring Data Internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the DPO.

Subject Access Requests

Under the General Data Protection Regulations 2018, individuals are entitled, subject to certain exceptions, to request access to information held about them. This includes confirmation that their data is being processed, access to their personal data and other supplementary information. There are restrictions on the information to which a subject is entitled under applicable law.

In applying these regulations Chippenham Town Council is obliged to adhere to the following schedules relating to subject access:

a) Subject Access Requests (SARs) whereby an individual may request personal information held by Chippenham Town Council about themselves or a nominated individual on their behalf must be responded to within 1 month

b) Where the above is found to be complex or numerous an extension may be granted allowing an additional 2 months, however the subject must be informed within 1 month of their request

c) No fee shall be charged for the above except where it is found to be excessive, repetitive or manifestly unfounded in accordance with the law.

Further information can be found at APPENDIX A.

Freedom of Information Requests

a) Freedom of Information Act Requests (FOIs), whereby an individual may request information held by the Council but not containing information relating to individuals, subject to certain exceptions, must be responded to as soon as possible within 20 working days

b) Environmental Information Regulation requests (EIR) must be responded to as soon as possible but within 20 working days

c) No fee shall normally be charged for the above. However, in exceptional circumstances a fee may be charged.

Subject Access Requests and Freedom of Information Requests will be processed by the Head of Democratic Services, with advice from the DPO. Further information can be found in the Council's Freedom of Information Policy.

Training

All staff will receive training on this policy. New starters will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Conditions for Processing and Justification for Personal Data

We will ensure any use of personal data is justified using at least one of the 'conditions for processing/ six data protection principles' and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. We will document the additional justification for the processing of sensitive

data.

If consent is the condition, the data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal Record Checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data Portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right To Be Forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Data Audit and Register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting Breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority of any compliance failures.

All actual or potential breaches must be reported to the DPO at the soonest opportunity. In their absence, the breach must be reported to the Chief Executive.

Monitoring

Everyone must observe this policy. We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to the Corporate Management Team.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation, in consultation with senior management, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

Complaints

Where an individual makes a complaint relating to the processing of their personal data or is unhappy with any response to an SAR, FOI or EIR (if appropriate) request they may request an internal review (IR) be conducted. Requests for an IR should be within 40 days of the original response. The responsibility for the conduct of an IR is with the Town Council who will discuss with the appointed DPO. The Town Council contact is:

Chief Executive,
Chippenham Town Council,
Town Hall,
High Street,
Chippenham,
SN15 3ER

If an individual is unhappy with the outcome of the IR they have the right to appeal to the Information Commissioner's Office (ICO) for assessment, the ICO is contactable at:

Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF.

Security Incidents

Wherever it is believed that a security incident or a 'near miss' has occurred, the Data Protection Officer must be informed immediately, and the Security Incident Management (SIM) process must be carried out. The SIM is designed to manage, investigate, report and provide 'Learning From Experience' (LFE) to avoid future incidents occurring.

In any case an incident must be reported no later than 24 hours from identification, except where a malicious incident has occurred. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

Further details on security incidents and data breaches can be found in the Data Breach Policy.

Further Information

For further information or clarification on any part of this policy, please contact your Line Manager.

Appendix A

Subject Access Request Procedures

The organisation shall complete the following steps when processing a request for personal data (Subject Access Request or SAR) with advice from its Data Protection Officer.

1. Ascertain whether the requester has a right to access the information and in what capacity

2. Obtain proof of identity (once this step has been completed the clock can start)

3. Engage with the requester if the request is too broad or needs clarifying

4. Make a judgement on whether the request is complex and therefore can be extended to a 2 month response time

5. Acknowledge the requester providing them with:

   a. The response time – 1 month (as standard), an additional 2 months if complex

   b. Details of any costs – free for standard requests, or you can charge if the request is manifestly unfounded or excessive, or further copies of the same information is required. The fee must be in line with the administrative cost.

6. Use its Record of Processing Activities and/or data map to identify data sources and where they are held

7. Collect the data (the organisation may use its IT support to pull together data sources – for access to emails the organisation can do so as long as it has told staff it will do so in its policies)

8. If (6) identifies third parties who process any data, engage with them to release the data to Chippenham Town Council

9. Review the identified data for exemptions and redactions in line with the ICO's Code of Practice on Subject Access and in consultation with the organisation's Data Protection Officer

10. Create the final bundle and check to ensure all redactions have been applied

11. Submit the final bundle to the requester in a secure manner and in the format they have requested.