Warminster Town Council

Delivering a brighter, greener future for all

Data Protection Policy (GDPR) Privacy Policy

May 2024 reviewed
Next review May 2025

1. Introduction

1.1 An essential activity of Warminster Town Council is the requirement to gather, process and store information about its employees, people in the community, suppliers, business contacts and other sources to operate efficiently.

2. General Data Protection Regulation (GDPR) May 2018

2.1 The GDPR 2018 was put into place to help protect people's personal data. It aims to ensure that people know where their data is held, what it is used for and who it is shared with. It also ensures that an organisation treats people's data correctly and has systems and controls in place for effective management of that data. A key principle of the GDPR is that personal data is processed securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.

2.2 A Council acting as an employer is required to comply with the GDPR. In such circumstances, the Council will be deemed to be a 'data controller' for the purposes of the Regulation and in this capacity, it will determine the purposes for which and the way any personal data is, or is to be, processed. 'Processing' includes obtaining, recording, holding, or using information. The 'data processor', in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller – for example Wiltshire Pension Fund.

2.3 The GDPR is underpinned by six important principles which state that personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to the individual.
2. Collected for specified, explicit and legitimate purpose(s).
3. Adequate, relevant, and limited to the purpose(s) for which it was processed.
4. Accurate and kept up to date; inaccurate data shall be erased or rectified without delay.
5. Kept for no longer than is necessary for the purpose(s) for which it was processed.
6. Secure, using appropriate technical or organizational measures.

The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

3. Subject Rights

3.1 The GDPR creates rights for those people who have their data stored and responsibilities for those who store, process, or collect personal data.

3.2 A person who has their data processed by the Council has a number of rights in relation to

the data which is held about them. The person has the following rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object; and
- The right not to be subject to automated decision-making including profiling.

4. Subject Access Requests

4.1 A person who makes a request is entitled to the following information:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

4.2 Once the Council receives such a request, should the data be disclosable, the request must be dealt with within one month of receiving the request.

4.3 The Council can refuse or charge for requests that are manifestly unfounded or excessive.

4.4 If the Council refuses a request, they must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. The Council must do this without delay and at the latest within one month of receipt.

5. A Subject Access Request Which Concerns Other People's Information

5.1 A person may request access to data about them which also carries information regarding a third party. In such circumstances, the Council will assess whether the request can be complied with, without infringing the third party's privacy.

5.2 If the Council receives a request from an employee to access some personal data and complying with the request would mean disclosing information relating to another individual who can be identified from that information, then the request will be legitimately declined unless the third-party consents to the disclosure or it is reasonable for the Council to comply with the request without the third party's consent.

5.3 There is an obligation upon a data controller to comply with as much of a request as possible. If the consent of the third party cannot be obtained and compliance with the request is reasonable, then the Council will consider separating the disclosable information from the non-disclosable information.

6. Personal Data

6.1 The GDPR covers any data which concerns a living and identifiable individual.

6.2 This definition of personal data provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

7. Sensitive Personal Data

The GDPR refers to sensitive personal data as 'special categories of personal data'. These include:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying an individual
- Health and
- Sex life or sexual orientation.

It will be lawful to process sensitive data if:

1. the data subject has given explicit consent to the processing for specified purpose(s);
2. it is necessary for carrying out the controller's or individual's rights and obligations in employment, social security law etc;
3. it relates to personal data manifestly made public by the individual;
4. it is necessary for legal proceedings;
5. it is necessary for assessing the working capacity of an employee (i.e. processing medical or occupational health data).

8. Exceptions

8.1 There are circumstances in which a data controller is not obliged to supply certain information to the requester. Some of the most important exemptions apply to:

- crime prevention and detection;
- confidential references given by you (but not ones given to you);
- information covered by legal professional privilege.

Art. 23 GDPR Restrictions contains the full list.

9. Information Commissioner's Office Data Protection Fee

9.1 As the data controller that determines the purpose for which personal data is processed, the Council must pay the Information Commissioner's Office (ICO) an annual data protection fee. This replaces the annual registration with the ICO that applied under the Data Protection Act.

10. Lawful Basis for Processing Personal Data

10.1 As an employer, the Council has obligations in relation to the data it holds on computer or in structured filing systems about its employees. The main requirements of the GDPR can be complied with in relation to this data if the Council:

- has individuals' consent to holding the information about them;
- uses the information only for the purposes for which they obtained it;
- keeps the information up-to-date, secure and only for so long as it is needed;
- does not disclose the information to others without the individual employee's consent.

11. Consent

11.1 Consent to use personal data will be unambiguous and involve a clear affirmative action (an opt-in). It will be separate from other terms and conditions and will not generally be a precondition of signing up to a service. Consent requests will be concise, easy to

understand and user-friendly.

11.2 Consent will specifically cover the controller's name, the purposes of the processing and the types of processing activity.

11.3 Explicit consent must be expressly confirmed in words, rather than by any other positive action.

11.4 The Council will keep clear records to demonstrate consent.

11.5 Consent must be freely given. The Council will give people genuine ongoing choice and control over how it uses their data.

11.6 There is no set time limit for consent. How long it lasts will depend on the context. The Council will review and refresh consent as appropriate.

11.7 Individuals have the right to withdraw consent. The Council will notify people of this right and offer them easy ways to withdraw consent at any time.

12. Children

12.1 The Council needs to have a lawful basis for processing a child's personal data.

12.2 Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

12.3 Children aged 13 or over can give their own consent. For children under this age the Council will obtain consent from whoever holds parental responsibility for the child.

13. Disclosure Information

13.1 The Council will, as necessary, undertake checks on both staff and members with the Disclosure and Barring Service and will comply with its Code of Conduct relating to the secure storage, handling, use, retention and disposal of disclosures and disclosure information. It will include an appropriate operating procedure.