DATA PROTECTION POLICY

Date Ratified: 10 February 2026

Meeting: Finance & General Purpose Committee

Next review date: February 2029 *(3 yearly review)*

Supersedes: Information Data Protection Policy 2023

Contents

PURPOSE

This Data Protection Policy sets out how Thornbury Town Council ("the Council") collects, uses, stores, shares, and protects personal data. The policy ensures compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and related legislation.

SCOPE

This policy applies to:

- All councillors
- All employees, temporary staff, and volunteers
- Contractors, consultants, and third parties processing data on behalf of the Council

It covers all personal data processed by the Council in any format, including paper records, electronic records, emails, photographs, audio/video recordings, and databases.

DEFINITIONS

Personal Data: Any information relating to an identified or identifiable living individual.

Special Category Data: Personal data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, or data concerning a person's sex life or sexual orientation.

Processing: Any operation performed on personal data, including collection, storage, use, disclosure, or deletion.

Data Subject: The individual to whom the personal data relates.

Controller: The organisation that determines the purposes and means of processing personal data. The Council is a Data Controller.

ROLES AND RESPONSIBILITIES

This policy applies to all staff (including volunteers and councillors) who work at the Council, and to external organisations or individuals working on its behalf.

Councillors

The Councillors has overall responsibility for ensuring that the Town Council complies with all relevant data protection obligations.

Chief Executive Officer

Responsibility for data protection compliance is delegated to the Chief Executive Officer, who is designated as the Council's Data Protection Lead. This includes oversight of relevant policies and procedures and acting as the primary point of contact for data protection matters. In the Chief Executive Officer's absence, the Deputy Clerk shall assume these responsibilities.

All staff

All staff are responsible for:

- Familiarising themselves with and complying with this policy and acceptable use policies for staff; 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. However, staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken;
- Taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times. All staff should adopt the approach that they should treat the personal data of others with the same care with which they would treat their own;
- Using personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data;
- Storing, transporting and transferring data using encryption and secure password protected devices;
- Not transferring personal data offsite or to personal devices
- Deleting data in line with this policy and the retention schedule
- Informing the Council of any changes to their personal data, such as a change of address
- Reporting to the Chief Executive Officer, or in their absence the Deputy Clerk following circumstances:
    - Any questions about the operation of this policy, data protection law, retaining or sharing personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - If they are unsure whether they have a lawful basis upon which to use personal data in a particular way;
    - If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
    - The discovery of a data breach or near miss (immediate action is required) – please refer to the Data Breach Procedure.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
    - If they are to share personal data with a data processor, for example a contractor or someone offering a service, in which case a contract is likely to likely to be required please see - Sharing Personal Data (section 10)

DATA PROTECTION OFFICER (DPO)

Having assessed its functions and processing activities in accordance with Article 37 of the UK GDPR, the Council has determined that it is not required to appoint a statutory Data Protection Officer. The Council

does not carry out large-scale systematic monitoring of individuals or large-scale processing of special category personal data.

DATA PROTECTION PRINCIPLES

The Council will process personal data in accordance with the seven UK GDPR principles. Personal data shall be:

1. **Lawfulness, fairness and transparency**
   The Council will process personal data lawfully, fairly and in a transparent manner. This includes identifying and documenting a lawful basis for processing, providing clear privacy notices, and ensuring individuals understand how their personal data is used.

2. **Purpose limitation**
   the Council explains these reasons to the individuals concerned when it first collects their data. If the Council wishes to use personal data for reasons other than those given when the data was first obtained, it will inform the individuals concerned before doing so, and will seek consent where necessary and appropriate unless the new purpose is compatible with that in respect of which consent was given, or there is another lawful basis for sharing the information/ The Council will document the basis for processing. For special categories of personal data, it will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

3. **Data minimisation**
   the Council must only process the minimum amount of personal data that is necessary in order to undertake its work.

4. **Accuracy**
   The Council will take reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date, and will correct or delete inaccurate data without undue delay in accordance with the Data Protection Act 2018.

5. **Storage limitation**
   Personal data will not be kept in a form which permits identification of individuals for longer than is necessary. Personal data is retained in accordance with the Council's Retention Schedule and securely disposed of when no longer required.

6. **Integrity and confidentiality (security)**
   The Council will implement appropriate technical and organisational measures to ensure the security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

7. **Accountability**
   The Council complies with its obligations under data protection laws including the GDPR and can demonstrate this via the measures set out in this policy, including:
   - Completing Data Protection Impact Assessments (DPIAs) where the Council's processing of personal data presents a high risk to rights and freedoms of individuals, and when

introducing new technologies. This largely involves special category personal data and CCTV.
- Integrating data protection into internal documents including this policy, any related policies and Privacy Notices;
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; the Council also maintains a record of attendance;
- Regularly conducting reviews and audits to test its privacy measures and ensure compliance with relevant legislation and Council policies;
- Maintaining records of its processing activities for all personal data that it holds.

LAWFUL BASES FOR PROCESSING

In order to ensure that the Council's processing of personal data is lawful; it will always identify and document one of the following six grounds for processing before starting the processing:

- The data needs to be processed so that the Council can fulfil a contract with the individual, or the individual has asked the Council to take specific steps before entering into a contract;
- The data needs to be processed so that the Council can comply with a legal obligation;
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life;
- The data needs to be processed so that the Council, as a public authority, can perform a task in the public interest, and carry out its official functions;
- The data needs to be processed for the legitimate interests of the Council or a third party where necessary, balancing the rights of freedoms of the individual). 7 However, where the Council can use the public task basis for processing, it will do so rather than rely on legitimate interests as the basis for processing.
- The individual (or their parent/carer when appropriate in the case of a child) has freely given clear consent. In the case of special categories of personal data, this must be explicit consent. The Council will seek consent to process data from the child depending on their age and capacity to understand what is being asked for.

DATA SUBJECT RIGHTS

The Council recognises and upholds the rights of individuals under data protection law, including the right to:

- Be informed about how their data is used
- Access their personal data
- Rectify inaccurate or incomplete data
- Erase personal data (where applicable)
- Restrict processing
- Data portability (where applicable)
- Object to processing

- Not be subject to automated decision-making

Requests to exercise these rights will be handled within accordance to the Subject Access Request Procedure.

DATA SECURITY

The Council will implement appropriate technical and organisational measures to ensure the security of personal data and to protect against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

These measures include physical security, access controls, staff responsibilities, and secure handling of personal data. Detailed requirements relating to IT systems, network security, device use, remote access, and information security controls are set out in the Council's IT and Security Policy, which all councillors, employees, and relevant third parties are required to follow.

Personal data breaches will be reported and managed in accordance with the Data Breach Procedure.

DATA SHARING AND DISCLOSURE

Please refer to the Council's Privacy Notices.

The Council will only share personal data where there is a lawful basis to do so and where such sharing is identified in the relevant Privacy Notice(s). Personal data will be shared only where necessary and proportionate, and in accordance with data protection legislation.

The following principles apply:

- Personal data may be shared where there are safeguarding concerns or where it is necessary to protect the safety of staff, councillors, or others. In such cases, information may be shared with appropriate agencies without consent where permitted by law and in accordance with recognised safeguarding and information-sharing guidance.
- Personal data may be shared with other organisations where it is necessary for the performance of the Council's functions or to meet statutory obligations. Where appropriate, the Council will provide information to individuals about such sharing through its Privacy Notices.
- The Council may share personal data with contractors and service providers who process data on its behalf. In such cases, the Council will:
    - Only use processors that provide sufficient guarantees of compliance with data protection law;
    - Ensure that appropriate written data processing agreements are in place; and
    - Share only the personal data necessary for the delivery of the service.
- Personal data may be shared with law enforcement agencies and other public bodies where there is a lawful requirement or basis to do so, including for the prevention or detection of crime, the apprehension or prosecution of offenders, the administration of taxation, or in connection with legal proceedings.

- Personal data may also be shared with emergency services and local authorities where necessary to respond to an emergency situation affecting staff, councillors, or the wider community.

Where possible, information will be anonymised or aggregated prior to sharing. The Council does not sell personal data.

RETENTION AND DESTRUCTION OF RECORDS

The Council retains personal data only for as long as is necessary for the purposes for which it was collected, in accordance with its Retention Schedule.

When personal data is no longer required, it will be securely destroyed or deleted in a manner appropriate to the format of the data, including both paper and electronic records.

Where third parties are engaged to dispose of records on the Council's behalf, the Council will ensure that appropriate assurances and safeguards are in place to protect personal data.

Secure disposal arrangements are designed to ensure that personal data is no longer used or accessed once it is no longer required.

TRAINING AND AWARENESS

All councillors, employees, and volunteers will receive data protection training appropriate to their role and responsibilities, to ensure they understand how to handle personal data lawfully and securely.

Basic awareness training will be provided as part of induction. Additional or more detailed training will be provided where individuals have responsibilities that involve regular handling of personal data or higher-risk processing activities.

Data protection forms part of continuing professional development. Updates and refresher activity will be provided where changes to legislation, regulatory guidance, or the Council's processes make this necessary.

BREACH MANAGEMENT

The Council takes all personal data breaches seriously. A personal data breach is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Any actual or suspected personal data breach must be reported immediately to the Data Protection Lead. The Council will assess the breach without delay and, where required, notify the Information Commissioner's Office within 72 hours and affected individuals where there is a high risk to their rights and freedoms.

The Council has a separate Data Breach Procedure which sets out the detailed procedures for identifying, reporting, managing, and reviewing personal data breaches. All councillors, employees, and relevant third parties are required to follow that policy.

POLICY REVIEW

This policy will be reviewed at least every two years, or sooner if required by changes in legislation or Council activities.