



Twyning Parish Council

DATA PROTECTION POLICY

Purpose

The council is committed to being transparent about how it collects and uses the personal data of staff, and to meeting our data protection obligations. This policy sets out the council's commitment to data protection, and your rights and obligations in relation to personal data in line with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

The council has appointed the clerk as the person with responsibility for data protection compliance within the council. Questions about this policy, or requests for further information, should be directed to them.

Definitions

"Personal data" is any information that relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information. It includes both automated personal data and manual filing systems where personal data are accessible according to specific criteria. It does not include anonymised data.

"Processing" is any use that is made of data, including collecting, recording, organising, consulting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data as well as criminal convictions and offences.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Legal Duties

The Parish Council is registered with the Information Commissioner's Office and recognises its responsibility to comply with the Data Protection Act 1998 and the UK General Data Protection Regulation (UK GDPR).

The UK General Data Protection Regulation sits alongside the Data Protection Act 1998. The Act applies to 'personal data' which is data relating to a living person who can be identified from that data. 'Processing data' means any operation performed on that personal data such as collection, recording or use. The Parish Council does have data that relates to living individuals and does process data in order to perform its role.

This page explains to Councillors, staff and members of the public about the General Data Protection Regulation.

When dealing with personal data, The Parish Council staff and Councillors must ensure that:

- **Data is processed fairly and lawfully** - Staff, Councillors and Volunteers will be open and honest about why information is required.
- **Data is processed for specific purposes only**
- **Data is relevant to what it is needed for** – Data will be monitored so that too much or too little is not kept; only data that is needed will be held.
- **Data is accurate and kept up to date** – Only accurate personal data will be kept. Inaccurate data will be corrected.
- **Data is not kept longer than it is needed**
- **It is processed in accordance with the rights of individuals** – Individuals will be informed, upon request, of all the information held about them.
- **It is kept securely** – Data will be stored securely so it cannot be accessed by members of the public.

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply to process personal data:

- **(a) Consent:** the individual has given clear consent to process their personal data for a specific purpose.
- **(b) Contract:** the processing is necessary for a contract with the individual, or because they have asked you to take specific steps before entering into a contract.
- **(c) Legal obligation:** the processing is necessary to comply with the law (not including contractual obligations).
- **(d) Vital interests:** the processing is necessary to protect someone's life.
- **(e) Public task:** the processing is necessary to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (Public

authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.)

Information Audit

The Parish Council may need to retain certain information to carry out its day-to-day operations, to meet its objectives and to comply with legal obligations. The type of information the Council holds tends to be limited to name, address, telephone number and email address. More detailed information is held for employees. In the normal course of business, the Parish Council will receive personal data in connection with the following council activities:

- Administration of Parish Council Meetings
- Administration of facilities for hire
- Administration of employment matters
- Managing Councillor membership
- Receiving and dealing with correspondence
- Contractual matters
- Receiving and processing grant applications
- Creating Volunteer lists for specific activities
- Responding to contact made via the Parish Council social media or Parish Council website.
- Processing PAYE reporting to HMRC

The Clerk may also be provided with a copy of the electoral roll with updates throughout the year. Data Protection associated with the electoral roll is predominately the responsibility of Tewkesbury Borough Council and the policies of Tewkesbury Borough Council regarding use of the electoral roll must be observed. The Clerk or members of the council may independently request access, but they are not permitted to view or share the document with other council members or a third party. The Clerk may share certain details from the electoral roll where permitted by Tewkesbury Borough Council policies for the purpose of electoral activities such as verifying residents' status to vote at the parish meeting or providing election candidates with details required for election forms.

Sensitive data

The Act requires 'sensitive data' to be treated differently. Categories of sensitive data includes racial or ethnic origins, political opinions, religious beliefs, health issues. The Parish Council does not collect such data.

Where the Council carries out future village-wide surveys, the responses should be anonymous and questions are not generally asked on a topic that is classified as sensitive.

Storage of data

All Council paper documents are stored in a secure location.

All digital records are stored securely in line with the IT policy and only accessed on devices compliant with the IT policy.

Once data is not needed anymore, if it is out of date or has served its purpose and falls outside the minimum retention time of the council's retention policy, it will be destroyed or deleted from the computer.

How the data is used

Data will be used only for the purpose for which it has been supplied. Data will not be passed to a third party without the express consent of the data subject or where the Council is required to do so by law. The Council will not share or sell data.

If a Councillor needs to access information to help carry out their duties, they may only access as much information as is necessary for the particular task and it will be used only for that specific purpose. Information will not be released without the prior knowledge or consent of the Clerk. Data will never be used for political reasons unless the data subjects have consented.

Individual rights

As a data subject, you have a number of rights in relation to your personal data.

Subject access requests

You have the right to make a subject access request. If you make a subject access request, the council will tell you:

- whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from yourself;
- to whom your data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long your personal data is stored (or how that period is decided);
- your rights to rectification or erasure of data, or to restrict or object to processing;

- your right to complain to the Information Commissioner if you think the council has failed to comply with your data protection rights; and
- whether or not the council carries out automated decision-making and the logic involved in any such decision-making.

The council will also provide you with a copy of your personal data undergoing processing. This will normally be in electronic form if you have made a request electronically, unless you agree otherwise.

If you want additional copies, the council may charge a fee, which will be based on the administrative cost to the council of providing the additional copies.

To make a subject access request, you should send the request to the Clerk of the Council. In some cases, the council may need to ask for proof of identification before the request can be processed. The council will inform you if we need to verify your identity and the documents we require.

The council will normally respond to a request within a period of one month from the date it is received. Where the council processes large amounts of your data, this may not be possible within one month. The council will write to you within one month of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, the council is not obliged to comply with it. Alternatively, the council can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the council has already responded. If you submit a request that is unfounded or excessive, the council will notify you that this is the case and whether or not we will respond to it.

Other rights

You have a number of other rights in relation to your personal data. You can require the council to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if your interests override the council's legitimate grounds for processing data (where the council relies on our legitimate interests as a reason for processing data);

- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override the council's legitimate grounds for processing data.
- complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk).

To ask the council to take any of these steps, you should send the request to the Clerk of the Council.

A link for contact details for the Clerk are published in the footer of this page.

Data Protection Officer

The Clerk will perform the tasks required of a Data Protection Office. The GDPR does not define a parish council as a public authority therefore does not require it to appoint a Data Protection Officer.

Data breaches

The council have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur the council must take notes and keep evidence of that breach.

If you are aware of a data breach you must contact the Clerk of the Council immediately and keep any evidence, you have in relation to the breach.

If the council discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of yourself, we will report it to the Information Commissioner within 72 hours of discovery. The council will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell you that there has been a breach and provide you with information about its likely consequences and the mitigation measures we have taken.

International data transfers

The council will not transfer personal data to countries outside the EEA.

Confidentiality

When complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential.

Policy adoption and Review

Policies will be reviewed annually or when further advice is issued or a need arises.

All Councillors, employees and volunteers are expected to comply with the policies set by the Parish Council to protect privacy, confidentiality and the interests of the Council.

Contact Details

A link to the contact details for the Clerk are published in the footer of this website page.

Training

The council provides training to all individuals about their data protection responsibilities.

Date of policy: February 2026

Approving committee:

Date of committee meeting:

Policy version reference: V1

Policy effective from:

Date for next review: