

TWYWELL PARISH COUNCIL

Data Protection Policy

In accordance with UK GDPR and the Data Protection Act 2018

Document Title	Data Protection Policy
Version	1.0
Date Adopted	June 2026
Next Review Date	June 2027
Responsible Officer	Parish Clerk
Data Controller	Twywell Parish Council
Approved By	Full Council
Legislation	UK GDPR Data Protection Act 2018 PECR

1. Introduction

Twywell Parish Council (the Council) is committed to protecting the personal data of residents, councillors, employees, volunteers and all other individuals whose information it holds. This policy sets out how the Council collects, uses, stores, shares and protects personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The Council recognises that the lawful and correct treatment of personal data is essential to maintaining the trust of those it serves and to operating effectively as a local authority.

2. Scope

This policy applies to:

- All personal data held by the Council in any format (electronic, paper, audio or visual)
- All councillors, the Parish Clerk and any other staff or contractors acting on behalf of the Council
- All processing activities carried out by or on behalf of the Council

This policy should be read alongside the Council's Privacy Notice, Data Breach Policy and Retention Schedule.

3. Key Definitions

For the purposes of this policy:

- Personal data — any information relating to an identified or identifiable living individual

- Special category data — sensitive data including health, race, religion, political opinions, biometric data and trade union membership
- Data Controller — the Council, which determines the purposes and means of processing personal data
- Data Processor — any organisation processing personal data on behalf of the Council
- Data Subject — the individual whose personal data is being processed
- Processing — any operation performed on personal data including collection, storage, use, disclosure or deletion
- ICO — the Information Commissioner's Office, the UK's data protection regulator

4. Data Controller Details

Twywell Parish Council is registered as a Data Controller with the Information Commissioner's Office.

Data Controller	Twywell Parish Council
Contact	Parish Clerk, Twywell Parish Council
ICO Registration	To be confirmed on registration
Supervisory Authority	Information Commissioner's Office — ico.org.uk

5. Data Protection Principles

The Council will ensure that all personal data is:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (data minimisation)
4. Accurate and, where necessary, kept up to date
5. Kept in a form which permits identification of data subjects for no longer than is necessary (storage limitation)
6. Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (integrity and confidentiality)

The Council, as Data Controller, is responsible for and must be able to demonstrate compliance with these principles (accountability).

6. Lawful Basis for Processing

The Council will only process personal data where a lawful basis exists. The lawful bases most commonly relied upon by the Council are:

- Legal obligation — processing necessary to comply with a legal requirement (e.g. financial reporting, employment law, Freedom of Information)
- Public task — processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority

- Legitimate interests — where the Council has a legitimate interest that is not overridden by the rights of the individual
- Consent — where the individual has given clear, informed and freely given consent (used sparingly and never as a condition of services)
- Contract — where processing is necessary to fulfil a contract with the individual

Where special category data is processed, the Council will identify an additional condition under Schedule 1 of the DPA 2018 or Article 9 of UK GDPR.

7. Types of Personal Data Held

The Council may hold the following categories of personal data:

- Names, addresses, email addresses and telephone numbers of residents, councillors and employees
- Financial information for payroll and supplier payments
- Minutes and correspondence containing references to identifiable individuals
- Planning application representations and objections
- Employment and HR records
- CCTV footage (where applicable)
- Special category data where relevant to employment or safeguarding purposes

8. Rights of Data Subjects

Individuals whose data the Council holds have the following rights under UK GDPR:

8.1 Right of Access (Subject Access Request)

Individuals may request a copy of the personal data the Council holds about them. The Council will respond within one calendar month of receipt of a valid request. No fee will ordinarily be charged.

8.2 Right to Rectification

Individuals may request that inaccurate or incomplete personal data is corrected. The Council will action valid requests within one calendar month.

8.3 Right to Erasure

Individuals may request deletion of their personal data where there is no compelling reason for its continued processing. This right is not absolute and does not apply where processing is required by law.

8.4 Right to Restrict Processing

Individuals may request that the Council limits how it uses their personal data in certain circumstances.

8.5 Right to Data Portability

Where processing is based on consent or contract and is carried out by automated means, individuals may request their data in a machine-readable format.

8.6 Right to Object

Individuals may object to processing based on legitimate interests or public task, including profiling. The Council will consider all objections and cease processing unless it can demonstrate compelling legitimate grounds.

8.7 Rights Relating to Automated Decision-Making

The Council does not currently use automated decision-making or profiling in ways that have legal or significant effects on individuals.

To exercise any of the above rights, individuals should contact the Parish Clerk in writing. If a request is refused, the individual will be informed of the reason and their right to complain to the ICO.

9. Data Security

The Council will implement appropriate technical and organisational measures to protect personal data against unauthorised access, loss, destruction or disclosure. These measures include:

- Password protection on all electronic devices used to process Council data
- Secure email practices including appropriate use of BCC and encrypted transmission where required
- Physical security of paper records including locked storage
- Access controls limiting data access to those with a legitimate need
- Secure disposal of personal data — shredding paper records and secure deletion of electronic files
- Regular review of access rights, particularly following a change of Clerk or councillor

All councillors and staff will receive appropriate data protection awareness as part of their induction.

10. Data Retention

Personal data will not be retained for longer than is necessary for the purpose for which it was collected. The Council will maintain a Retention Schedule setting out the retention periods for different categories of data.

Key retention periods include:

- Minutes and agenda — permanent retention as public record
- Financial records — 6 years
- Employment records — 6 years after employment ends
- Planning correspondence — 6 years
- Data Breach Register — minimum 3 years
- General correspondence — 3 years unless subject to an ongoing matter

At the end of the retention period, data will be securely destroyed and destruction recorded.

11. Data Sharing and Third Parties

The Council will only share personal data with third parties where:

- There is a lawful basis to do so
- The recipient has a legitimate need for the data
- A Data Processing Agreement is in place where the third party is acting as a Data Processor

The Council will not sell personal data to any third party. Where data is shared with a Data Processor (such as a payroll provider or IT supplier), the Council will ensure that an appropriate contract is in place requiring the Processor to act only on the Council's instructions and to maintain adequate security measures.

Where the Council is required by law to share personal data (e.g. with HMRC, auditors or the police), it will do so in accordance with the legal requirement.

12. Data Breaches

A personal data breach is any incident resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All suspected or confirmed data breaches must be:

7. Reported to the Parish Clerk immediately upon discovery
8. Recorded in the Council's Data Breach Register
9. Assessed for risk to individuals' rights and freedoms
10. Reported to the ICO within 72 hours if the breach is likely to result in a risk to individuals — reportable via ico.org.uk
11. Notified to affected individuals without undue delay if the breach poses a high risk to them

Deliberate or reckless misuse of personal data by a councillor, Clerk or contractor may constitute a criminal offence under Section 170 of the Data Protection Act 2018 and will be treated as a serious disciplinary matter.

13. CCTV and Other Technologies

Where the Council operates CCTV, drones, body-worn cameras or other surveillance technologies, it will maintain a separate CCTV policy compliant with the ICO's CCTV Code of Practice. Appropriate signage will be displayed and data will be retained for no longer than 31 days unless required for an ongoing investigation.

14. Council Website and Cookies

The Council's website will maintain a separate Privacy Notice and Cookie Policy. No personal data submitted via the website will be used for purposes other than those stated. The Council will not use third-party tracking cookies without the explicit consent of visitors.

15. Roles and Responsibilities

Role	Responsibility
Full Council	Adopting and reviewing this policy. Approving significant data processing decisions. Receiving reports on data breaches.
Parish Clerk	Day-to-day management of data protection compliance. Maintaining the Data Breach Register. Handling Subject Access Requests. Liaising with the ICO. Ensuring secure data handling.
All Councillors	Complying with this policy. Reporting suspected breaches to the Clerk immediately. Not sharing personal data outside their council role.

16. Complaints

Any individual who believes the Council has not handled their personal data lawfully may raise a complaint with the Parish Clerk in the first instance. If the matter is not resolved, the individual has the right to lodge a complaint directly with the ICO:

- Website: ico.org.uk
- Telephone: 0303 123 1113
- Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

17. Policy Review

This policy will be reviewed annually by Full Council, or sooner in the event of:

- A significant data breach
- Changes to UK GDPR, the DPA 2018 or ICO guidance
- Changes to the Council's processing activities

The most current version of this policy will be published on the Council's website.

Adopted by Full Council	9 th July 2026_____
Date	13 July 2026_____
Signed (Chairman)	Russell Robertson_____
Signed (Parish Clerk)	James Totten_____