



TATWORTH AND FORTON PARISH COUNCIL

DATA PROTECTION ACT (2026 Edition)

Reviewed and approved

1st October 2026

Minute

189/26

1. Purpose of this Policy

Tatworth & Forton Parish Council (“the Council”) collects, stores and processes personal data to carry out its statutory functions, deliver services, employ staff, and manage its operations. This policy sets out how the Council complies with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018 (DPA 2018)**.

The Council is committed to ensuring personal data is handled lawfully, fairly, securely and transparently.

2. Scope

This policy applies to:

- Councillors
- The Clerk and any employees
- Volunteers acting on behalf of the Council
- Contractors and third-party processors

It covers all personal data processed by the Council, whether held electronically, on paper, or in other formats.

3. Definitions

- **Personal Data:** Information relating to an identifiable living person.
- **Special Category Data:** Sensitive data requiring additional protection (e.g., health, political opinions, religious beliefs).
- **Processing:** Any operation performed on personal data.
- **Data Subject:** The individual whose data is processed.
- **Data Controller:** The organisation determining how and why data is processed (the Council).
- **Data Processor:** A third party processing data on behalf of the Council.

4. Lawful Bases for Processing

The Council processes personal data under one or more of the following lawful bases:

1. **Public Task** – performing a task in the public interest or exercising official authority.
2. **Legal Obligation** – compliance with UK law (e.g., financial reporting, employment law).

3. **Contract** – where processing is necessary for an employment or service contract.
4. **Consent** – freely given, specific, informed and revocable.
5. **Vital Interests** – to protect life.
6. **Legitimate Interests** – only for non-statutory activities where appropriate.

Special category data is processed only under Article 9 conditions, typically:

- Employment obligations
- Substantial public interest
- Explicit consent

5. Data Protection Principles

The Council adheres to the seven UK GDPR principles:

1. **Lawfulness, fairness and transparency**
2. **Purpose limitation**
3. **Data minimisation**
4. **Accuracy**
5. **Storage limitation**
6. **Integrity and confidentiality (security)**
7. **Accountability**

6. Accountability Measures

The Council maintains:

- **A Record of Processing Activities (ROPA)**
- **A Data Audit Register**
- **Privacy Notices** for staff, councillors, residents and service users
- **Contracts with all data processors**
- **Regular training** for councillors and staff
- **Annual review** of data protection compliance (AGAR Assertion 10)

7. Data Subject Rights

Individuals have the right to:

- Be informed
- Access their data (Subject Access Request)
- Rectification
- Erasure (“right to be forgotten”)
- Restriction of processing
- Data portability (where applicable)
- Object
- Rights related to automated decision-making

Subject Access Requests must be submitted in writing and will be responded to within **one month**. All SARs must be referred to the **Parish Clerk**.

8. Data Retention & Disposal

The Council retains personal data only as long as necessary for statutory or operational purposes.

Retention periods follow:

- **NALC / SLCC retention guidance**
- **ICO recommendations**
- **Statutory requirements** (e.g., financial records: 6 years; HR records: up to 7 years)

Data is disposed of securely:

- Paper documents are **shredded**
- Electronic data is securely deleted
- Backups are managed and purged appropriately

9. Data Security

The Council implements appropriate technical and organisational measures including:

- Password protection and access controls
- Secure email using the council’s official domain
- Encrypted storage where appropriate

- Locked filing cabinets for paper records
- Regular software updates
- Website compliance with **WCAG 2.2 AA** accessibility standards

Personal data is not disclosed to unauthorised parties.

10. Data Sharing

Data may be shared with:

- Government bodies (e.g., HMRC, auditors)
- Law enforcement
- Contractors providing council services
- Other authorities where legally required

Data will **not** be transferred outside the UK unless adequate safeguards exist.

11. Data Breach Procedure

A personal data breach includes loss, unauthorised access, destruction or alteration.

The Council will:

1. **Report breaches immediately** to the Clerk.
2. Assess risk to individuals.
3. Notify the **ICO within 72 hours** if the breach is likely to result in risk.
4. Inform affected individuals where necessary.
5. Record all breaches in the **Breach Log**.

12. Training & Awareness

All councillors, staff and volunteers must:

- Complete periodic data protection training
- Follow this policy
- Report concerns promptly

Training is reviewed annually.

13. Use of Council Email & Devices

Councillors and staff must:

- Use the **official council email domain** for council business

- Avoid using personal devices without appropriate security
- Not store council data on personal cloud services
- Follow the Council's IT & Communications Policy

14. Privacy Notices

The Council publishes clear privacy notices explaining:

- What data is collected
- Why it is collected
- Lawful bases
- Retention periods
- Rights of individuals

These are available on the Council website and on request.

15. Roles & Responsibilities

- **Parish Clerk** – Data Protection Lead, responsible for compliance, SARs, breach reporting, ROPA maintenance.
- **Councillors & Staff** – must follow this policy and complete training.
- **Processors** – must comply with UK GDPR and contractual obligations.

16. Policy Review

This policy is reviewed annually or sooner if legislation changes.