

Thwing & Octon Parish Council – Data Protection Policy

Adopted: 13.10.2025

Review: Annually or sooner if required

1. Introduction

Thwing & Octon Parish Council (“the Council”) is committed to protecting the privacy and security of personal data.

This policy sets out how the Council complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The Council is a Data Controller and the Clerk/RFO is the Council’s Data Protection Officer (DPO) (unless otherwise appointed).

2. Principles

The Council will ensure that personal data is:

1. Processed lawfully, fairly and transparently.
2. Collected only for specified, explicit and legitimate purposes.
3. Adequate, relevant and limited to what is necessary.
4. Accurate and, where necessary, kept up to date.
5. Retained only as long as necessary.
6. Processed securely.

3. Data Held

The Council typically holds the following categories of personal data:

- Councillors’ contact details
- Clerk and employee records (employment, payroll, pensions)
- Residents’ correspondence and consultation responses
- Supplier and contractor details (including bank accounts for payment)
- Minutes, agendas and official records (including names of residents where provided in correspondence)
- Financial records and audit information

A full breakdown is maintained in the Information Asset Register (Data Map).

4. Lawful Bases for Processing

The Council relies on the following lawful bases under UK GDPR:

- Public Task – performing its statutory functions as a parish council.
- Legal Obligation – complying with legislation (e.g. financial regulations, employment law).
- Contract – where necessary for entering into or performing contracts (e.g. suppliers).
- Consent – only where none of the above apply (e.g. mailing lists).

5. Data Security

- Electronic files are stored on the Clerk's password-protected laptop.
- Email accounts are protected with strong passwords.
- Paper records are kept securely in a locked cabinet.
- Access to personal data is restricted to the Clerk and, where necessary, councillors.
- Backups are maintained to protect against data loss.

6. Sharing Data

Personal data will only be shared where necessary and lawful, including with:

- East Riding of Yorkshire Council (e.g. planning consultations)
- External and Internal Auditors
- HMRC and pension providers
- Contractors and service providers (where required)
- Members of the public (e.g. names included in minutes)

The Council does not sell or pass data to third parties for marketing purposes.

7. Data Retention

Data is retained in accordance with the Council's Retention and Disposal Schedule, typically:

- Financial records: 7 years
- Employment records: 6 years after employment ends
- Minutes: Permanent
- Correspondence: 1 year (unless part of ongoing matter)

8. Rights of Individuals

Individuals have the right to:

- Be informed about how their data is used
- Access their personal data (Subject Access Request)
- Rectify inaccurate data
- Request erasure (where lawful basis is consent)
- Restrict or object to processing (in certain circumstances)
- Data portability (where applicable)

Requests should be made in writing to the Clerk, who will respond within one month.

9. Breach Procedure

Any suspected data breach must be reported immediately to the Clerk.

The Clerk will assess the breach and, where necessary, report to the ICO within 72 hours and notify affected individuals if there is a high risk to their rights and freedoms.

10. Training & Review

The Clerk and councillors will remain aware of their responsibilities under data protection law.

This policy and the accompanying Data Map will be reviewed annually or sooner if required.