

Data Protection Policy

Yealmpton Parish Council

Adopted: 9th February 2026

Review: Annual or upon legislative change

1. Purpose of this Policy

This policy sets out how the parish council complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It ensures that personal data is handled lawfully, fairly, securely, and transparently, and that individuals' rights are respected.

2. Scope

This policy applies to:

- All personal data processed by the parish council
- All councillors, the Clerk, volunteers, and contractors who handle personal data
- All systems used for council business, including email, website hosting, cloud storage, WhatsApp volunteer groups, and paper records

It covers personal data relating to residents, volunteers, contractors, councillors, and any other individuals whose data the council processes.

3. Data Protection Principles

The council complies with the six principles of UK GDPR. Personal data must be:

1. Processed lawfully, fairly, and transparently
2. Collected for specified, explicit, and legitimate purposes
3. Adequate, relevant, and limited to what is necessary
4. Accurate and kept up to date
5. Kept no longer than necessary
6. Processed securely

The council is responsible for demonstrating compliance with these principles.

4. Roles and Responsibilities

4.1 The Parish Council (Data Controller)

The council is legally responsible for ensuring compliance with data protection law.

4.2 The Clerk

The Clerk manages day-to-day compliance, including:

- Secure storage and processing of personal data
- Responding to rights requests

- Managing third-party processors
- Maintaining records of processing
- Reporting data breaches

4.3 Councillors and Volunteers

Must:

- Follow this policy
- Use council-approved systems
- Keep devices secure
- Report any data breaches immediately

5. Lawful Bases for Processing

The council processes personal data under the following lawful bases:

- Public Task – most council functions
- Legal Obligation – finance, governance, transparency
- Consent – club/association contacts, optional communications
- Contract – suppliers and service providers
- Legitimate Interests – volunteer coordination via WhatsApp

6. Special Category Data

The council processes limited special category data, including:

- Religious information (e.g., church membership disclosed through Public Task)
- Health and disability information (if disclosed to Council, it is not routinely collected)
- Vulnerability information for the Emergency Plan
- Volunteer health considerations
- Incidental special category data disclosed in correspondence

Processing is carried out under the following Schedule 1 conditions:

- Paragraph 6 – Statutory and Government Purposes
- Paragraph 8 – Equality of Opportunity or Treatment
- Paragraph 18 – Safeguarding of Individuals at Risk
- Part 1, Paragraph 1 – Explicit Consent

7. Categories of Personal Data Processed

The council processes:

- Contact details for residents, volunteers, contractors, and councillors

- Club and association contact lists (consent-based)
- Emergency Plan contact and vulnerability information
- Salt-gritting volunteer details
- Tidy Village volunteer details (including WhatsApp profile names and phone numbers)
- Email correspondence
- Website contact form submissions
- Documents stored in cloud storage

8. Third-Party Processors

The council uses the following third-party services:

- Email server provider
- Website hosting provider
- Dropbox (cloud storage; data may be stored in the USA under SCCs)
- WhatsApp (volunteer coordination; data may be processed outside the UK/EU)

All processors must provide GDPR-compliant terms and appropriate security measures.

9. Data Security

The council maintains appropriate technical and organisational measures, including:

- Strong passwords
- Secure devices with up-to-date software
- Encrypted cloud storage
- Restricted access to personal data
- Secure storage of paper records

Further detail is set out in the council's Data Security Policy.

10. Data Retention and Disposal

Personal data is retained only as long as necessary and in accordance with the council's Retention and Disposal Policy.

Data is securely deleted or destroyed when no longer required.

11. Rights of Individuals

Individuals have the right to:

- Access their data
- Rectify inaccuracies
- Request erasure (where applicable)

- Restrict processing
- Object to processing
- Data portability (limited circumstances)
- Not be subject to automated decision-making

Requests are handled in accordance with the council's Rights Request Policy.

12. Data Breaches

A data breach includes loss, unauthorised access, accidental disclosure, or destruction of personal data.

All breaches must be reported immediately to the Clerk.

The Clerk will assess, record, and report breaches in line with the council's Data Breach Policy.

13. Privacy Notices

The council maintains clear privacy notices explaining:

- What data is collected
- Why it is collected
- How it is used
- Who it is shared with
- How long it is kept
- Individuals' rights

Privacy notices are published on the council website and updated as required.

14. Training and Awareness

Councillors, the Clerk, and volunteers handling personal data receive guidance on:

- Secure handling of information
- Recognising data breaches
- Responding to rights requests
- Using approved systems

15. Monitoring and Review

This policy is reviewed annually or sooner if:

- Legislation changes
- New systems are introduced
- A breach or rights request highlights a need for improvement