Data Breach Policy

Yealmpton Parish Council

Adopted:9th February 2026

Review: Annual or upon significant change in systems or processing

1. Purpose of this Policy

This policy sets out how the parish council identifies, manages, and reports personal data breaches. It ensures compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and protects the rights and freedoms of individuals whose data the council processes.

2. Scope

This policy applies to:

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

It covers accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

3. What Constitutes a Data Breach

A data breach may include, but is not limited to:

- Sending personal data to the wrong recipient
- Loss or theft of a device containing council information
- Unauthorised access to email, Dropbox, or WhatsApp groups
- Accidental deletion or alteration of personal data
- Website contact form compromise
- Disclosure of Emergency Plan or volunteer data to unauthorised individuals
- Paper records lost, stolen, or accessed without permission

Breaches may be accidental or deliberate.

4. Responsibilities

4.1 The Clerk

The Clerk is responsible for:

- Receiving breach reports
- Investigating breaches
- Assessing risk to individuals

- Recording breaches in the Breach Log
- Reporting notifiable breaches to the ICO within 72 hours
- Informing affected individuals where required

4.2 Councillors and Volunteers

All councillors and volunteers must:

- Report any suspected or actual breach immediately
- Cooperate with investigations
- Follow this policy and the council's Data Security Policy

5. Reporting a Breach

Any councillor, volunteer, or contractor who becomes aware of a breach must report it immediately to the Clerk.

Reports should include:

- What happened
- When it happened
- What data was involved
- Who may be affected
- Any steps already taken

Delays increase risk and may lead to non-compliance with the 72-hour reporting requirement.

6. Assessing the Breach

The Clerk will assess:

- The type and sensitivity of the data involved
- Whether special category data is affected (e.g., disability, religious belief, vulnerability information)
- The number of individuals affected
- The potential consequences (identity theft, distress, risk to safety, reputational harm)
- Whether the data was encrypted or otherwise protected
- Whether the breach is likely to result in a risk to individuals' rights and freedoms

This assessment determines whether the breach must be reported to the ICO.

7. Notifying the ICO

A breach must be reported to the ICO within 72 hours if it is likely to result in a risk to individuals' rights and freedoms.

The Clerk will submit:

- A description of the breach
- Categories and approximate number of individuals affected
- Categories and approximate number of data records affected
- Likely consequences
- Measures taken or proposed to address the breach

If full details are not yet available, an initial report will be submitted, followed by updates.

8. Notifying Individuals

Individuals must be informed without undue delay if the breach is likely to result in a high risk to their rights and freedoms.

This may include breaches involving:

- Emergency Plan vulnerability information
- Disability or health information
- Religious belief
- Volunteer phone numbers or WhatsApp group exposure
- Loss of unencrypted personal data

Notifications will include:

- A description of the breach
- Likely consequences
- Steps individuals can take to protect themselves
- Measures the council has taken to mitigate harm
- Contact details for further information

9. Containment and Recovery

The Clerk will take immediate steps to limit the impact of the breach, such as:

- Resetting passwords
- Removing unauthorised access
- Recovering lost data where possible
- Securing devices or accounts
- Contacting third-party processors (email provider, Dropbox, website host, WhatsApp support if necessary)

10. Recording Breaches

All breaches, whether notifiable or not, must be recorded in the Data Breach Log, including:

- Date and time of breach

- Description of incident
- Type of data involved
- Number of individuals affected
- Assessment of risk
- Actions taken
- Whether the ICO or individuals were notified

This log is reviewed annually.

11. Learning and Prevention

Following a breach, the council will:

- Review what went wrong
- Update policies or procedures
- Provide additional training if needed
- Improve technical or organisational measures

This ensures continuous improvement in data protection practices.

12. Review of this Policy

This policy is reviewed annually or sooner if:

- New systems are introduced
- New risks are identified
- Legislation changes
- A significant breach occurs