Data Breach Notification Policy

1. Purpose

This Data Breach Notification Policy sets out how the Parish Council will respond to a personal data breach and meet its legal obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The purpose of this policy is to:

- Ensure personal data breaches are identified, contained, investigated, and reported appropriately.
- Protect the rights and freedoms of individuals whose personal data may be affected.
- Ensure compliance with statutory reporting requirements.

2. Scope

This policy applies to:

- All Parish Councillors.
- The Clerk/RFO and any other employees.
- Contractors, volunteers, and third parties who process personal data on behalf of the Parish Council.

It applies to all personal data processed by the Parish Council, whether held electronically or in paper form.

3. Legal Framework

This policy is based on the following legislation and guidance:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Guidance issued by the Information Commissioner's Office (ICO).

4. Definition of a Personal Data Breach

A personal data breach is a security incident that leads to the accidental or unlawful:

- Destruction of personal data.
- Loss of personal data.
- Alteration of personal data.
- Unauthorised disclosure of personal data.
- Unauthorised access to personal data.

Examples include (but are not limited to):

- Loss or theft of paper files or electronic devices containing personal data.
- Sending personal data to the wrong recipient.
- Accidental publication of personal data on a website.
- Unauthorised access to systems or email accounts.

5. Roles and Responsibilities

5.1 Parish Council

The Parish Council is the Data Controller and is responsible for ensuring appropriate policies, procedures, and training are in place.

5.2 Clerk to the Council

The Clerk is the nominated Data Protection Lead and is responsible for:

- Coordinating the response to a data breach.
- Assessing the risk to individuals.
- Deciding whether the breach must be reported to the ICO.
- Ensuring affected individuals are notified where required.
- Maintaining the data breach register.

5.3 Councillors, Employees, and Others

All individuals covered by this policy must:

- Act in accordance with data protection principles.
- Report any actual or suspected data breach immediately to the Clerk.
- Cooperate fully with any investigation.

6. Reporting a Data Breach

Any actual or suspected data breach must be reported to the Clerk as soon as possible and no later than 24 hours after discovery.

The report should include, where known:

- The date and time the breach occurred and was discovered.
- A description of the breach.
- The type of personal data involved.
- The number of individuals affected (if known).
- Any immediate action taken.

7. Containment and Initial Response

Upon becoming aware of a breach, the Clerk will:

- Take immediate steps to contain the breach and prevent further unauthorised access or loss.
- Secure any relevant systems, documents, or equipment.
- Recover personal data where possible.
- Preserve evidence for investigation.

8. Risk Assessment

The Clerk will assess the breach to determine the likelihood and severity of risk to the rights and freedoms of individuals. This assessment will consider:

- The nature and sensitivity of the personal data.
- Whether special category data is involved.
- The number of individuals affected.
- The ease of identifying individuals.
- The potential consequences for individuals (e.g. distress, financial loss, identity theft).

9. Notification to the ICO

The Clerk will notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of a breach if it is likely to result in a risk to the rights and freedoms of individuals.

Where notification is made after 72 hours, the reasons for the delay will be documented.

If the breach is not reported to the ICO, the reasons for this decision will be recorded.

10. Notification to Affected Individuals

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Parish Council will inform affected individuals without undue delay.

The notification will:

- Be clear and in plain language.
- Describe the nature of the breach.
- Provide the name and contact details of the Clerk.
- Explain the likely consequences of the breach.
- Describe measures taken or proposed to address the breach.
- Provide advice on steps individuals can take to protect themselves.

Notification may be delayed or avoided where permitted by law, for example where it would prejudice an ongoing investigation or appropriate security measures have rendered the data unintelligible.

11. Record Keeping

All personal data breaches, regardless of whether they are reported to the ICO, will be recorded in a Data Breach Register. The record will include:

- The facts relating to the breach.
- Its effects.
- The remedial action taken.

12. Review and Remedial Action

Following a breach, the Parish Council will:

- Review the causes of the breach.
- Identify and implement any necessary improvements to policies, procedures, or security measures.
- Consider whether additional training is required.

13. Training and Awareness

The Parish Council will ensure that Councillors, employees, and relevant third parties receive appropriate data protection training and are aware of this policy.

14. Review of Policy

This policy will be reviewed at least every two years or sooner if required by changes in legislation, guidance, or working practices.

Adopted by the Parish Council: 12/02/2026
Minute Ref: 26.011

Reviewed 14/05/2026

Minute Ref: 26.059.3