

Breage Parish Council



Data Protection Policy

Adopted: 04 November 2025

Review Due: November 2026

Signed: Chair Cllr A.E. Woodhams

1. Introduction

Breage Parish Council is committed to protecting your personal data and respecting your privacy. This policy outlines how we collect, use, store, and protect personal data in accordance with:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Data (Use and Access) Act 2025
- The Freedom of Information Act 2000
- The Transparency Code for Smaller Authorities
- The 2025 Assertion 10 requirements under the Annual Governance and Accountability Return (AGAR)

Breage Parish Council is the Data Controller and is registered with the Information Commission.

2. What is Personal Data?

Personal data refers to any information relating to an identifiable living individual. This includes names, addresses, email addresses, photographs, financial details, and other identifiers.

3. Lawful Basis for Processing

We process personal data under the following lawful bases:

- Consent (e.g. for newsletters or surveys)

- Legal obligation (e.g. financial records, electoral roll)
- Public task (e.g. statutory duties)
- Contract (e.g. employment or service agreements)
- Legitimate interests (e.g. community engagement, fraud prevention)

4. How We Use Your Data

We may use your personal data for:

- Providing services and responding to enquiries
- Managing council operations, meetings, and communications
- Processing financial transactions (grants, payments, invoices)
- Maintaining statutory records (e.g. cemetery, minutes)
- Conducting surveys and consultations
- Ensuring website accessibility and digital compliance
- Protecting individuals from harm or fraud
- Complying with legal and audit requirements

5. Data Sharing

Your data will only be shared:

- With your explicit consent
- Where required by law (e.g. HMRC, auditors)
- With trusted third parties under data sharing agreements

We do not sell or trade personal data.

6. Data Retention

We retain personal data only as long as necessary:

- Electoral roll – while current
- Cemetery & Council minutes – permanently
- Financial & staff records – minimum 6 years
- Other data – reviewed annually and deleted when no longer needed
 - Inspection records: **21 years**
 - Financial records: **6 years**
 - Correspondence: **2 years**, unless required longer

7. Data Security

We store data securely using:

- Password-protected council-owned devices
- Encrypted drives and secure cloud services
- Locked physical storage
- Council-owned email domain (e.g. clerk@breageparishcouncil.gov.uk)

- We do not use personal or free email services (e.g. Gmail, Outlook) for council business.

8. Your Rights

You have the right to:

- Access your personal data
- Request correction or deletion
- Withdraw consent
- Object to processing
- Request data portability
- Lodge a complaint with the Information Commission

9. Data Audits & Risk Management

We conduct regular data audits to map:

- What data we hold
- Why we hold it
- Who has access
- Lawful basis for processing

We also perform risk assessments and maintain an IT Policy covering device use, breach response, and data security.

10. Further Processing

If we intend to use your data for a new purpose, we will issue a new privacy notice and seek your consent where required.

11. Our IT Policy

This policy includes:

- **Device Use:** Only council-owned, encrypted devices permitted.
- **Email Practices:** Mandatory use of council domain; personal email prohibited.
- **Data Security:** Secure storage, restricted access, regular backups.
- **Breach Response:** Immediate reporting, ICO notification within 72 hours, and communication with affected individuals.
- **Training:** Annual data protection and IT security training.

Compliance: Supports AGAR Assertion 10 and UK legislation

12. Draft Website Privacy Notice

We will be introducing the following by April 2026

- **Data Collection:** What data is collected via the website (e.g. contact forms, cookies).
- **Lawful Basis:** Consent, legal obligation, public task.
- **Cookie Usage:** Compliance with DUAA 2025—statistical cookies exempt from consent.
- **User Rights:** Access, correction, objection, portability, and complaints.

Contact Info: Clerk's details and ICO escalation path

13. Contact Details

To exercise your rights or raise concerns, contact:

The Clerk to Breage Parish Council
Parish Rooms, Breage, HELSTON, TR13 9PD
Tel: 01326 574781
Email: Clerk@breagepc.org.uk

The Parish Council would prefer any complaints to initially be made direct so it may have the opportunity to see if matters can be put right.

However, if you are unhappy with the way your information has been processed and how the Parish Council has responded to your request to exercise any of your rights in relation to your data, you can raise your concerns direct with the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF. Telephone: 0303 123 1113 or online: <https://ico.org.uk/concerns>

Appendix 1 - Data Breach Policy

Adopted 04 November 2025 AE Woodhams - Chair

1. Introduction

Breage Parish Council is committed to protecting personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy outlines the Council's approach to identifying, managing, and reporting personal data breaches.

2. Definition of a Data Breach

A personal data breach is defined as: 'A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.'

Examples include:

- Loss or theft of data or equipment
- Unauthorised access to data
- Sending personal data to the wrong recipient
- Loss of availability of personal data
- Alteration of personal data without permission

3. Reporting a Suspected Breach

All councillors, staff, and contractors must report any suspected data breach immediately to the Clerk, who acts as the Data Protection Officer (DPO).

The report should include:

- A description of the breach
- The date and time it occurred
- The type of data involved
- The number of individuals affected
- Any initial containment actions taken

4. Investigation and Risk Assessment

The Clerk/DPO will:

- Investigate the cause and scope of the breach
- Assess the potential impact on individuals
- Determine whether the breach is likely to result in a risk to individuals' rights and freedoms

5. Notification Requirements

If the breach is likely to result in a risk to individuals:

- The ICO must be notified within 72 hours of becoming aware of the breach
- Affected individuals must be informed without undue delay

The notification to the ICO must include:

- The nature of the breach
- Categories and approximate number of individuals and records affected
- Likely consequences of the breach
- Measures taken or proposed to address the breach

6. Communication with Affected Individuals

Affected individuals will be informed of:

- The nature of the breach
- The likely consequences
- Actions taken to mitigate the impact
- Contact details for further information

Communication may be withheld if:

- Data was encrypted or otherwise rendered unintelligible
- Subsequent measures have eliminated the risk
- It would involve disproportionate effort (in which case a public communication may be made)

7. Record Keeping

All data breaches, whether reportable or not, must be logged in the Data Breach Register, including:

- Date and time of breach
- Description and cause
- Actions taken
- Outcome and lessons learned

8. Review and Prevention

Following a breach:

- The Council will review the incident and response
- Update policies and procedures as needed
- Provide additional training if required

9. Policy Review

This policy will be reviewed annually or following a significant breach or change in legislation.

Adopted 02 December 2025 AE Woodhams - Chair