

Laverstoke & Freefolk Parish Council

DATA BREACH POLICY

1. Introduction

Laverstoke & Freefolk Parish Council is committed to protecting the personal data it holds and processes in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy outlines the Council's procedure for identifying, managing, recording, and reporting personal data breaches.

2. Purpose of the Policy

The purpose of this policy is to:

- Ensure that personal data breaches are handled promptly and effectively.
- Minimise the risk and impact of any breach.
- Ensure compliance with statutory reporting requirements.
- Provide a clear process for councillors, staff, and volunteers.

3. Definition of a Personal Data Breach

A personal data breach is any incident that results in:

- Unauthorised access to personal data
- Unauthorised disclosure or sharing
- Loss or theft of personal data
- Destruction or alteration of personal data
- Loss of availability (data cannot be accessed when needed)

Examples include:

- Sending emails to the wrong recipient
- Loss of an unencrypted laptop
- Unauthorised access to records
- Accidental deletion of important files
- Cyberattacks or system failures

4. Responsibilities

Clerk/RFO (Data Protection Lead): Manages breach investigations, maintains records, and liaises with the Information Commissioner's Office (ICO).

All councillors, staff, and volunteers: Must immediately report any suspected data breach.

Council: Ensures appropriate safeguards and resources are in place.

5. Identifying a Data Breach

Any person working on behalf of the Council must consider whether an incident involves:

- Personal data
- A breach of confidentiality, integrity, or availability
- Potential risk or harm to individuals

If the answer is yes, the incident must be treated as a potential breach.

6. Reporting a Breach

All suspected breaches must be reported immediately to the Clerk/RFO, providing:

- Date and time of the incident
- Description of what happened
- Type of personal data affected
- Number and category of individuals involved
- Any actions already taken

If the Clerk/RFO is unavailable, the Chair or Vice-Chair must be informed.

7. Assessment of the Breach

The Clerk/RFO will:

- Conduct an initial assessment
- Determine whether personal data is involved
- Assess the scale and severity of the breach
- Identify who is affected and potential consequences
- Recommend actions to contain and resolve the breach

Risk factors include: identity theft, financial loss, distress, reputational harm, safeguarding concerns.

8. Reporting to the ICO

If the breach is likely to result in a risk to individuals' rights and freedoms, the Council must notify the ICO within 72 hours of becoming aware of the breach.

The notification will include:

- The nature 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 contain the breach

If reporting is required, the Council will follow ICO guidance.

9. Informing Affected Individuals

Where the breach is likely to result in a high risk to individuals (e.g., identity theft, financial damage, safeguarding issues), the Council will inform individuals as soon as possible, including:

- The nature of the breach
- What data was affected
- Actions individuals should take
- Measures the Council has taken
- Contact details for further information

10. Managing and Containing the Breach

Actions may include:

- Recovering lost data
- Changing passwords or access rights
- Shutting down compromised systems
- Informing the Council's IT provider
- Enhancing physical and digital security
- Reviewing relevant procedures

11. Recording Data Breaches

The Council will maintain a Data Breach Log, recording:

- Nature and date of the breach
- Number of individuals affected
- Actions taken
- ICO reporting decision
- Lessons learned
- Follow-up actions

All breaches, regardless of severity, must be logged.

12. Learning from Data Breaches

- Following any breach, the Council will:
- Review existing policies and procedures
- Identify areas for improvement
- Provide additional staff/councillor training if required
- Update risk assessments and privacy notices as needed

13. Review of This Policy

This Data Breach Policy was approved by Laverstoke & Freefolk Parish Council on:

Date: 9.12.2025

This policy will be reviewed annually in May or sooner if legislation changes or following a significant data breach.