BARLASTON PARISH COUNCIL



DATA BREACH POLICY

GDPR5

DATA BREACH POLICY

Revision History

This document was originally written by:

Name	**Position**	**Date**
Vivien O'Dunne	Clerk	February 2026

This document was reviewed by:

The Parish Council	10 March 2026

This document version was adopted by:

The Parish Council at their meeting on	10 March 2026

Document Review schedule:

Next Mandatory Review by	March 2027

Version	**Issue Date**	**Document ID**	**Reason for Change**	**Section changed**
1	10 March 2026	GDPR5	New Policy	n/a

Barlaston Parish Council – Data Breach Policy

1. Purpose

This policy sets out how Barlaston Parish Council identifies, reports, manages, and learns from data breaches in line with the UK GDPR and Data Protection Act 2018. It ensures timely action to protect the rights of individuals and maintain the Council's accountability and transparency.

2. Scope

This policy applies to all councillors, staff, contractors, and volunteers who process personal data on behalf of the Council, whether stored on paper, electronic devices, or cloud systems.

3. Definition

A **data breach** is any incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This includes:

- Loss or theft of devices containing personal data.
- Accidental disclosure of personal data via email, post, or other channels.
- Unauthorised access to council systems, cloud storage, or paper records.

4. Responsibilities

- All councillors and staff must report any suspected or actual data breach immediately to the Clerk.
- The Clerk will take lead responsibility for investigating, containing, and reporting breaches.
- The RFO and relevant committee members may be involved as needed.

5. Reporting and Response

1. **Immediate Action:**
    - Contain the breach to prevent further data loss.
    - Preserve evidence (e.g., emails, logs, screenshots).
2. **Investigation:**
    - Identify the nature, cause, and scope of the breach.
    - Determine the categories and approximate number of individuals affected.
    - Assess the potential impact on individuals' rights and freedoms.

3. **Notification:**
    - If the breach poses a risk to individuals' rights and freedoms, the Clerk will notify the Information Commissioner's Office (ICO) within 72 hours.
    - Affected individuals will be informed if the breach is likely to result in a high risk to their rights.
4. **Documentation:**
    - All breaches, regardless of severity, must be recorded including:
        - Date and nature of the breach
        - Individuals affected
        - Action taken to contain and resolve
        - Lessons learned

6. Containment and Mitigation

- Change passwords or access controls if compromised.
- Recover or securely delete lost or exposed data.
- Apply corrective measures to prevent recurrence.

7. Review and Lessons Learned

- The Clerk will review each breach to identify improvements in procedures, training, or systems.
- Recommendations will be reported to the Council to update policies and procedures as necessary.

8. Training and Awareness

- Councillors and staff receive induction training on recognising and reporting data breaches.
- Annual refresher training is provided to ensure awareness and compliance.

9. Review

- This policy will be reviewed at least every three years, or sooner if there is a legislative or operational change.

_____ _____

Chairman Date: 10 March 2026