BARLASTON PARISH COUNCIL

DATA SECURITY POLICY

GDPR8

DATA SECURITY 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	GDPR8	New Policy – Assertion 10 2025/26	-

Barlaston Parish Council – Data Security Policy

1. Purpose

This policy sets out how Barlaston Parish Council protects the personal and sensitive data it processes in line with the UK GDPR and Data Protection Act 2018. It ensures that councillors, staff, and third parties handle data securely, minimise risks, and maintain confidentiality.

2. Scope

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

3. Email and Accounts

- All councillors must use their official .gov.uk email addresses for council business only.
- Councillors must enable and maintain two-factor authentication (2FA) on all accounts.
- Sensitive information must not be sent via personal or non-council email accounts.
- Use Bcc when emailing multiple recipients to protect privacy.

4. Devices and Storage

- Council data may only be stored on council-provided devices or authorised cloud platforms.
- Devices must be password-protected, encrypted where possible, and kept secure when not in use.
- Councillors must not store council data on personal devices unless explicitly authorised.

5. Passwords and Access

- Passwords must be strong, unique, and changed regularly.
- Sharing of passwords is strictly prohibited.
- Access to sensitive data is restricted to those who require it for their role.

6. Backups and Cloud Storage

- Critical council data must be backed up regularly.
- Authorised cloud services must meet UK GDPR requirements.

- Access to cloud storage must be restricted to authorised personnel only.

7. Paper Records

- Paper records containing personal or sensitive data must be stored in locked cabinets.
- Access is limited to authorised personnel only.
- Records no longer needed must be disposed of securely (e.g., shredding).

8. Data Breaches and Incidents

- Any suspected data breach must be reported immediately to the Clerk.
- The Clerk will investigate and take appropriate action, including reporting to the ICO within 72 hours if required.

9. Retention and Disposal

- Council data will be retained only as long as necessary for operational, legal, or statutory purposes.
- Disposal of personal data must follow secure methods such as shredding, secure deletion, or approved archival procedures.

10. Responsibilities

- All councillors and staff are responsible for complying with this policy.
- The Clerk and RFO oversee the implementation, monitoring, and review of this policy.

11. Training and Awareness

- New councillors and staff receive induction on this policy.
- Annual refresher training is provided to all staff and councillors.
- Guidance from ICO, NALC, and Staffordshire County Council is shared as appropriate.

12. 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