BARLASTON PARISH COUNCIL

DATA HANDLING POLICY

GDPR6

DATA HANDLING 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	GDPR6	New Policy – Assertion 10 2025/26	n/a

Barlaston Parish Council – Data Handling Procedures Policy

Purpose

This policy sets out how Barlaston Parish Council manages and protects personal data in line with the UK GDPR, Data Protection Act 2018, and AGAR Assertion 10 requirements. It complements the Council's IT policy, which covers technical and infrastructure security.

Scope

Applies to all staff, councillors, contractors, and volunteers who process personal data on behalf of Barlaston Parish Council.

Email Handling

- Use official council email accounts for **all** council business.
- Use Bcc when sending emails to multiple recipients to protect privacy.
- Log and respond promptly to any Subject Access Requests (SARs) received by email.
- Emails containing personal data must **not** be forwarded to personal accounts.
- **Current situation:** Some councillors may access council emails on personal devices. All users must ensure passwords are secure, emails are not shared, and council data is not stored on personal apps or devices.

Paper Records

- Store all paper records containing personal data in locked cabinets with restricted access.
- Shred documents when no longer required in accordance with the council's retention schedule.
- Do not leave paper records unattended in public areas.

Cloud / IT Systems

- Use only authorised cloud platforms or software approved by the council.
- Access to cloud-stored personal data is restricted to authorised staff.
- Follow the IT policy for passwords, two-factor authentication, backups, and secure storage.

Council-Issued Devices (Future Update)

- The Council plans to provide iPads to all members for council business. Once issued, council data must only be accessed on these devices.
- The policy will be updated to include device-specific security requirements such as passcodes, encryption, remote wipe, and restricted app use.

Responsibilities

- The Clerk/DPO is responsible for monitoring compliance with this policy.
- All staff and councillors must report any suspected data breaches immediately to the Clerk/DPO.

Review

This policy is reviewed annually or sooner if there are material changes to council data handling practices. It will be updated when council-issued devices are provided.

_____ _____

Chairman Date: 10 March 2026