BARLASTON PARISH COUNCIL

DATA RISK REGISTER

GDPR7

DATA RISK REGISTER

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	GDPR7	New Document	-

Barlaston Parish Council: Data Risk Register

Linked to: Data Map / Article 30 Record of Processing Activities

Introduction – Risk Assessment

This Risk Assessment has been prepared by Barlaston Parish Council to support its data protection compliance framework. It reviews all personal data processing activities recorded in the Council's Data Map and considers the potential risks to the rights and freedoms of individuals. For each activity, the Council has identified possible threats, who may be affected, the severity of any potential impact, and the measures in place to reduce risk. This assessment is proportionate to the scale and nature of the Council's activities, ensuring that personal data is processed securely, only as necessary, and in line with statutory requirements. It is reviewed annually, or sooner if processing activities change.

Key:

- **Likelihood:** Low / Medium / High – probability of incident
- **Impact:** Low / Medium / High – effect if incident occurs
- **Residual Risk:** Level after applying mitigation controls
- **DPIA Needed:** Only for high-risk or new processing (e.g., CCTV, cloud with special category data)

Business Function	Data/Activity	Potential Risk	Who Affected	Likelihood	Impact	Controls/Mitigation	Residual Risk	Notes / DPIA Needed
Elected Members	Name, role, contact details, register of interests	Accidental disclosure, unauthorised access	Councillors, public	Low	Medium	Password-protected devices, original scanned then shredded	Low	No DPIA
Elected Members	Contact info for website (email, phone, address if consent given)	Posting personal info without consent	Councillors, public	Low	Medium	Consent checked, 2FA website access	Low	No DPIA
Finance / Banking	Bank mandates, ID verification	Fraud, data theft	Councillors, council finances	Low	High	Shred physical copies, secure electronic data, restricted access	Low	No DPIA
Staff – Clerk/RFO	Payroll, pension, sickness/leave, NI	Data breach, misuse	Staff	Medium	High	Password-protected files, restricted access, deletion after 6 years	Medium	No DPIA
Finance & Suppliers	Invoices, bank details, grant info	Financial fraud, leak of supplier info	Suppliers, council	Low	Medium	Secure banking, restricted access, only publish required info	Low	No DPIA

Business Function	Data/Activity	Potential Risk	Who Affected	Likelihood	Impact	Controls/Mitigation	Residual Risk	Notes / DPIA Needed
Residents Correspondence	Enquiries, complaints	Accidental disclosure of sensitive info	Residents	Medium	Medium	Secure email, shred notes, delete emails after case closed	Low	No DPIA
Residents / Social Media	FB / WhatsApp messages	Data left on personal devices, accidental disclosure	Residents, staff	Medium	Low	Messages auto-delete, not stored on device, secure accounts	Low	No DPIA
Website	Publishing council info	Out-of-date info, unauthorised edit	Public	Low	Low	Password + 2FA, only authorised staff can edit	Low	No DPIA
Social Media	Promotion of council activity	Accidental disclosure of personal info	Public	Low	Medium	Only public info shared, limited admin access	Low	No DPIA
CCTV / Security	Footage	Unauthorised access, data breach	Residents, visitors	Medium	High	Locked server, restricted access, signage, 30-day retention	Medium	Mini DPIA recommended (*see below)

Business Function	Data/Activity	Potential Risk	Who Affected	Likelihood	Impact	Controls/Mitigation	Residual Risk	Notes / DPIA Needed
Cloud / IT Storage (Dropbox)	Council documents, minutes, correspondence	Data breach, loss, international transfer risk	Staff, councillors, residents	Medium	Medium	Passwords, 2FA, restricted folders, SCCs in place for US servers	Medium	No DPIA
Register of Electors (Paper)	Name, address, electoral roll	Loss / unauthorised access	Residents	Low	High	Locked filing cabinet, authorised access only	Low	No DPIA
Council Admin – Historic / Legacy	Staff, councillors, residents, suppliers	Loss, accidental disclosure	Multiple	Low	Medium	Locked cabinet, restricted access, phased secure destruction	Low	No DPIA

CCTV is covered by the Barlaston Parish Council CCTV DPIA (March 2026). Footage is stored securely, access is restricted, signage is displayed, and retention is 31 days. Residual risk is medium. Full DPIA reviewed regularly; no new DPIA required unless system changes.

_____ _____

Chairman Date: 10 March 2026