

Sampford Brett Parish Council

Adopted May 2026, Appendices Adopted June 2026
Review date May 2028



DATA MANAGEMENT POLICY

Appendix A Retention Schedule

Sampford Brett Parish Council

DATA MANAGEMENT POLICY

Adopted June 2026



1. Purpose

The purpose of this policy is to ensure that Sampford Brett Parish Council manages all data—paper and electronic—in a lawful, secure, and efficient manner. This policy supports compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Council's statutory responsibilities.

2. Scope

- 2.1 This policy applies to all data held by the Parish Council, including:
- Personal data relating to residents, staff, councillors, and contractors
 - Council records, correspondence, and documents
 - Electronic files, emails, and digital storage
 - Paper records, minutes, agendas, and archives
- 2.2 It applies to all councillors, the Clerk, and any third parties acting on behalf of the Council.

3. Roles and Responsibilities

- 3.1 The **Clerk** is responsible for:
- Managing Council data in accordance with this policy
 - Ensuring secure storage and appropriate retention
 - Responding to data access requests
 - Maintaining the Council's Information Asset Register
 - Reporting data breaches to the Council and ICO where required
- 3.2 **Councillors** must:
- Handle Council information securely
 - Use Council-provided information only for Council purposes
 - Not store personal data on private devices unless authorised and protected

3.3 The **Council** is the Data Controller and is responsible for ensuring compliance with UK GDPR.

4. Data Collection and Use

- 4.1 The Council will only collect data that is:
- Necessary for lawful Council functions
 - Relevant and proportionate
 - Provided voluntarily or under a statutory requirement
- 4.2 The Council will comply with the seven data protection principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.
- 4.3 Personal data will only be used for the purpose for which it was collected.

4.4 Data will not be shared with third parties unless:

- Required by law
- Necessary for a statutory function
- Explicit consent has been obtained

5. Data Storage and Security

5.1 Electronic data must be stored on secure, password-protected devices or approved cloud storage.

5.2 Paper records must be stored securely and protected from unauthorised access.

5.3 Backup copies of essential Council records will be maintained by the Clerk.

5.4 Councillors must not store Council data on personal devices unless:

- It is necessary for Council duties
- The device is password-protected
- The data is deleted once no longer required

6. Email and Electronic Communication

6.1 Council business must be conducted using official Council email accounts wherever possible.

6.2 Personal email accounts must not be used to store or forward personal data relating to Council business.

6.3 Sensitive information must not be shared via social media or messaging apps.

7. Data Retention and Disposal

7.1 The Council will follow its **Retention Schedule** to determine how long data is kept.

7.2 Data will be securely destroyed when no longer required, including: • Shredding paper documents • Permanently deleting electronic files • Removing data from backup systems where possible

7.3 Minutes, agendas, and statutory records will be retained permanently as required by law.

8. Access to Information

8.1 Individuals have the right to request access to their personal data (Subject Access Request).

8.2 Requests must be submitted to the Clerk and will be responded to within one month.

8.3 The Council may request proof of identity before releasing information.

9. Data Breaches

9.1 A data breach includes loss, unauthorised access, or accidental disclosure of personal data.

9.2 All breaches must be reported immediately to the Clerk.

9.3 The Clerk will assess the breach and, where required, report it to the Information Commissioner's Office (ICO) within 72 hours.

10. Use of Personal Devices

10.1 Councillors using personal devices for Council business must ensure:

- Devices are password-protected
- Data is stored securely
- Council information is deleted when no longer needed

10.2 Lost or stolen devices containing Council data must be reported immediately.

11. Training and Awareness

11.1 Councillors and the Clerk will receive periodic guidance on data protection responsibilities.

11.2 New councillors will be provided with this policy as part of their induction.

12. Review

This policy will be reviewed annually or sooner if required to reflect changes in legislation or Council procedures.

Sampford Brett Parish Council

APPENDIX A

RETENTION SCHEDULE



This Retention Schedule forms part of the Council's Data Management Policy and sets out how long different categories of information are kept before secure disposal. Retention periods reflect statutory requirements, ICO guidance, and operational need.

1. Governance and Administration

Record Type	Retention Period	Notes
Minutes (signed)	Permanent	Legal record
Agendas	5 years	
Meeting papers / reports	5 years	Unless required longer for audit
Council policies & procedures	Current version + 6 years	Keep superseded versions
Declarations of Acceptance of Office	Term of office + 1 year	
Register of Members' Interests	As long as current + 1 year	

2. Finance and Audit

Record Type	Retention Period	Notes
Annual Accounts (final)	Permanent	Statutory
Audit reports	6 years	
Receipts & payments records	6 years	HMRC requirement
Bank statements / reconciliations	6 years	
Invoices / purchase orders	6 years	
VAT records	6 years	
Insurance policies	6 years after expiry	
Insurance claims	6 years after settlement	

3. Personnel and Staffing

Record Type	Retention Period	Notes
Employee records	6 years after employment ends	
Payroll information	6 years	HMRC requirement
Pension records	12 years	
Recruitment records (unsuccessful applicants)	6 months	Equality Act compliance
Training records	6 years	

4. Contracts and Asset Management

Record Type	Retention Period	Notes
Contracts (suppliers/contractors)	Duration of contract + 6 years	Limitation Act
Tenders / quotations	6 years	
Asset register	Permanent	
Maintenance records	6 years	

5. Planning

Record Type	Retention Period	Notes
Planning applications (Council copies)	3 years	Originals held by planning authority
Planning responses submitted by Council	3 years	

6. Correspondence and Communications

Record Type	Retention Period	Notes
Routine correspondence (email or paper)	2 years	Unless needed longer
Complaints (resolved)	3 years	
Complaints (serious or ongoing)	6 years	
Press releases / public notices	3 years	

7. Data Protection Records

Record Type	Retention Period	Notes
Subject Access Requests	2 years	ICO guidance
Data breach records	6 years	Limitation Act
Consent forms	Until withdrawn or no longer needed	

8. Website and Social Media

Record Type	Retention Period	Notes
Website content	Current + 1 year	
Social media posts (official Council account)	2 years	Unless part of a complaint

9. Disposal of Records

All records must be disposed of securely:

- Paper documents must be **shredded or cross-shredded**.
- Electronic files must be **permanently deleted** from devices and backups where possible.
- Confidential waste must be handled securely.

A brief log of destroyed records should be maintained by the Clerk.

10. Review

This Retention Schedule will be reviewed annually or sooner if required.