

Digital and Data Policy



Adopted: 16th October 2025

Review Date: September 2027

1. Purpose

This policy outlines how Sopley Parish Council manages its digital systems, data protection responsibilities, and online presence to ensure transparency, security, and legal compliance.

2. IT and Digital Governance

- All council business must be conducted using official council email addresses (e.g. *clerk@sopleyparishcouncil.gov.uk*).
- Personal devices used for council work must be secured with passwords and antivirus protection.
- Cloud storage and backups must be encrypted and accessible only to authorized personnel.
- The council website must meet **WCAG 2.2 AA** accessibility standards and comply with the **Public Sector Bodies Accessibility Regulations 2018**.

3. Data Protection and GDPR Compliance

Sopley Parish Council is both a **Data Controller** and **Data Processor** under the **Data Protection Act 2018** and **UK GDPR**. Key

Principles:

- **Lawfulness, fairness, and transparency** in data handling
- **Data minimisation:** Only collect what is necessary
- **Accuracy:** Keep data up to date
- **Storage limitation:** Retain data only as long as needed
- **Integrity and confidentiality:** Protect data from unauthorized access

Responsibilities:

- The Clerk oversees data compliance and coordinates responses to Subject Access Requests (SARs) and Freedom of Information (FOI) requests.
- All councillors and staff must complete annual data protection awareness training.

4. Email and Communications

- All correspondence must be retained in council-managed systems to ensure auditability.
- Councillors must avoid using personal email accounts for council business.
- Email signatures should clearly identify the sender's role and contact details.

5. Website and Transparency

- The website must publish required documents under the **Transparency Code for Smaller Authorities**, including:
 - Meeting agendas and minutes
 - Financial reports and budgets
 - Councillors contact details and declarations of interest
- Accessibility checks must be conducted annually, with remedial actions documented.

6. Cybersecurity

- Strong passwords and two-factor authentication (2FA) must be used where available.
- Suspicious emails or breaches must be reported immediately to the Clerk.
- Regular software updates and security patches must be applied to all council devices.

7. Data Sharing and Retention

- Data sharing must be limited to what is necessary for council operations.
- Personal data must not be disclosed without lawful basis.
- A **Data Retention Schedule** will guide how long different types of data are kept.

8. • Policy Review and Adoption

- This policy will be reviewed annually or upon significant changes in legislation.
- Any amendments must be approved by Full Council and minuted accordingly.