



Information Technology (IT) Policy of Somersham Parish Council

Version 1.1 - Adopted on 31st July 2025 at the Personnel and Governance Committee Meeting - ratified by FC at the following meeting.

1. Purpose

This policy defines how Somersham Parish Council manages its use of information technology, in line with the Transparency Code for Smaller Authorities (2015) and the 2025 edition of the Practitioners' Guide. It ensures the council's digital operations are transparent, secure, and compliant with data protection laws.

2. Scope

This policy applies to all **councillors, employees, volunteers, and contractors** who access or manage the council's IT resources, including but not limited to:

- Desktop and laptop computers, tablets, and smartphones
- Email and cloud-based systems
- Council website, social media, and digital publication tools
- Video conferencing and messaging platforms
- Personal devices used under Bring Your Own Device (BYOD) provisions

3. Governance and Oversight

IT Oversight: Somersham Parish Council employ a Data Protection Officer (DPO) through CAPALC, managed through the Executive Officer.

The Executive Officer oversees implementation, security, and compliance.

4. Data Protection s Security

All processing of personal data shall comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Privacy Policy: All data collection, processing, and subject rights are governed by the council's Privacy Policy, available on the council website. All users must familiarise themselves with it.

Access and Storage: Data is stored securely, with access granted only to authorised personnel based on necessity.

Retention: Personal data will be retained in accordance with the council's Data Retention Schedule and securely deleted when no longer needed. [Please refer to Somersham Parish Councils Archive Retention Policy]

Security Controls:

- Password protection and multi-factor authentication where applicable
- Regular updates and anti-malware software
- Backups of essential data in secure locations

5. Use of Personal Devices (BYOD)

Authorised Use Only: Councillors and staff may use personal devices for council business only if explicitly authorised and subject to compliance with this policy.

Security Requirements: Devices must be protected by strong passwords, encryption (where possible), and up-to-date antivirus software.

Access to council data on personal devices must be controlled and subject to regular review.

Data Separation: Council data must be kept separate from personal data using dedicated apps or storage areas.

6. Use of Personal Email Addresses

Prohibited Practice: The use of personal email accounts for council business is strictly prohibited. All council correspondence must be conducted through official council-provided email addresses. Emails from council-owned domains must not be forwarded to personal email addresses.

Monitoring and Compliance: Any breaches will be investigated, and appropriate measures taken in line with the council's disciplinary or governance procedures.

Email Retention: All council emails will be stored in compliance with the GDPR and Freedom of Information requirements.

7. IT Infrastructure s Support

Asset Register: Maintained for all council-owned hardware and software.

Maintenance: All devices must be regularly updated and checked for compliance with this policy.

Training: Users will be given training on IT systems, cybersecurity, data handling, and transparency responsibilities.

8. Monitoring and Review

Annual Review: This policy will be reviewed annually, or sooner if legislation or requirement changes.

Audits: Periodic internal audits will check for compliance with security and transparency requirements.

G. Data Breach Process and Protocols

The Parish Council is committed to responding promptly and effectively to any data breaches to minimise risk and comply with UK GDPR requirements.

10. Definition of a Data Breach

A data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include:

- Loss or theft of devices containing personal data
- Unauthorised access to council email accounts or files
- Sending personal data to the wrong recipient
- Malware or ransomware attacks compromising council systems

10.1 Reporting a Breach

Immediate Notification: Any councillor, employee, or contractor who becomes aware of a data breach must report it immediately to the Executive Officer. Somersham Parish Council use CAPALC services to employ a data protection officer (DPO)

Initial Response: The Executive Officer will assess the severity and scope of the breach and determine if mitigation steps are required (e.g., changing passwords, disabling access, enabling 2FA) and will report to the DPO.

10.2 Investigation

A full investigation will be conducted by the Executive Officer or designated officer within 72 hours of the breach being discovered.

The breach will be logged, including:

- Date and time of breach
- Type and volume of data affected
- Cause and extent of the breach
- Actions taken to address the breach

10.3 Notification Requirements

If the breach is likely to result in a risk to the rights and freedoms of individuals, the council must notify the Information Commissioner's Office (ICO) within 72 hours.

* If the breach poses a high risk to the individuals affected, those individuals must also be informed without undue delay, outlining:

- The nature of the breach
- Likely consequences
- Measures taken to mitigate the risk
- Contact information for further support

10.4 Remediation and Review

- The Executive Officer will ensure lessons are learned and policies, procedures, or training are updated as necessary.
- Technical fixes or security upgrades will be prioritised to prevent recurrence.
- Breach logs will be reviewed periodically to identify systemic issues.

11. Approval and Adoption

This policy was adopted by Somersham Parish Council on 31st July 2025 and will be reviewed annually or following a significant incident or legislative change.

Signed: *I Healiss (Executive Officer)*

Date of review: Annually