Halling Parish Council - IT Policy Document 10th March 2026

1. Purpose and Scope

This policy sets out how Halling Parish Council manages and uses its information technology systems to ensure security, continuity, and compliance with UK law. It applies to:

- The Clerk/Responsible Finance Officer
- Assistant Clerk
- All councillors
- Contractors or volunteers who access council systems
- All devices used for council business, whether council-owned or personal

The policy covers email, document storage, hardware, software, cloud services, and all digital information created or received by the Council.

2. Governance and Legal Framework

Halling Parish Council operates under:

- UK GDPR and Data Protection Act 2018
- Freedom of Information Act 2000
- Local Government Act 1972 (records and access)
- Local Government Transparency Code
- NCSC Cyber Essentials principles
- Public Records Act 1958
- NALC/SLCC retention guidance

The Clerk is the Data Controller for all council information.

3. Roles and Responsibilities

Clerk / Responsible Finance Officer

- Manages access to all systems and accounts
- Maintains the council's digital records and backups
- Ensures compliance with data protection and FOI requirements
- Oversees IT procurement and asset management
- Coordinates incident reporting and breach management

Councillors

- Use council systems responsibly and securely

- Protect confidential information
- Use council email accounts for all council business
- Follow password and device security requirements

IT Support Provider (not currently engaged)

- Maintains devices, updates, and security controls
- Supports backup and recovery processes
- Advises on cybersecurity risks

All Users

- Safeguard devices, passwords, and information
- Report incidents promptly

4. Acceptable Use

Users must:

- Use council IT systems only for council business, except where minimal personal use is explicitly permitted
- Keep information accurate, secure, and accessible for audit and FOI
- Store all council documents in the official Microsoft 365 environment (SharePoint/OneDrive)
- Avoid installing unapproved software or browser extensions
- Use only council-approved communication channels

Users must not:

- Use personal email or messaging apps (WhatsApp, Facebook Messenger, SMS) for confidential council business
- Store council data on personal cloud services (Dropbox, iCloud, Google Drive)
- Access inappropriate or illegal content
- Disable security settings or bypass controls

5. Devices and Equipment

Council-Owned Devices

Halling Parish Council currently maintains a small number of devices (e.g., Clerk's Assistant Clerk laptop). These must:

- Be encrypted and password-protected
- Have antivirus, firewall, and automatic updates enabled
- Be backed up via Microsoft 365
- Be recorded on the Council's asset register

Personal Devices (BYOD)

Councillors may use personal devices for council work only if:

Approved by the Clerk

- Protected with strong passwords and screen locks
- Kept updated with current operating systems and security patches
- Used only to access council data through Microsoft 365/OneDrive (no local storage)

If a councillor leaves office, any access must be removed immediately if applicable.

6. Email, Communication, and Collaboration

- All official communication must use the @halling-pc.gov.uk email domain.
- Sensitive information must be shared only through secure Microsoft 365 tools.
- Meeting papers must be distributed via SharePoint or email, not personal storage.
- Video meetings (Teams/Zoom) must be held in private spaces.

7. Passwords and Access Control

- Passwords must be strong (minimum 12 characters, mix of types).
- Multi-factor authentication (MFA) must be enabled on all Microsoft 365 accounts.
- Passwords must not be shared.

Access rights must be reviewed annually and after any change in role.

8. Data Storage, Backup, and Retention

- All council documents must be stored in Microsoft 365 SharePoint/OneDrive, organised according to the Council's filing structure.
- Backups are handled through Microsoft 365's built-in redundancy and versioning.
- Retention periods follow NALC/SLCC guidance (e.g., minutes permanent, financial records 7 years).
- Personal data must be minimised and deleted when no longer required.

9. Cybersecurity Measures

Halling Parish Council will:

- Maintain antivirus and anti-malware protection on all devices
- Apply security patches promptly
- Use secure Wi-Fi networks for council business

- Conduct periodic cybersecurity reviews (at least annually)
- Provide training to councillors and staff on phishing and data protection

Users must:

- Report suspicious emails immediately
- Avoid clicking unknown links or attachments
- Lock screens when away from devices
- Avoid public Wi-Fi unless using a secure VPN

10. Remote Working

- Given that the Clerk and councillors often work from home:
- Devices must not be left unattended in shared spaces
- Confidential papers must be stored securely
- Public Wi-Fi must not be used for council work unless protected
- Conversations involving confidential matters must not be overheard

11. Incident Reporting and Breach Management

- Incidents must be reported to the Clerk immediately, including:
- Lost or stolen devices
- Suspected data breaches
- Malware infections
- Unauthorised access attempts

The Clerk will:

- Assess the incident
- Take remedial action
- Report breaches to the ICO within 72 hours if required
- Notify affected individuals where necessary
- Report significant incidents to Council

12. Procurement and Asset Management

- All IT purchases must be approved by the Council.
- The Clerk maintains the IT asset register, including serial numbers, warranties, and software licences.
- Devices must be securely wiped before disposal or reuse.

13. Monitoring and Audit

- The Council may monitor IT systems for security, compliance, and performance.
- Logs may be reviewed for investigations or audits.
- Monitoring will always comply with UK GDPR and employment law.

14. Policy Review

- This policy will be reviewed annually by Halling Parish Council or sooner if:
- Legislation changes
- New systems are introduced
- A significant incident occurs

Policy adopted 10th March 2026

Next Review 1st March 2028