



Clifton Campville with Thorpe Constantine Parish Council

INFORMATION TECHNOLOGY (I.T.) POLICY

1. Purpose

This policy establishes the standards, responsibilities, and procedures for the secure and effective use of information technology (IT) within the Parish Council. It ensures compliance with legal, regulatory, and data protection requirements while supporting efficient council operations.

2. Scope

This policy applies to:

- All Councillors and staff using council-owned or personal devices for council business.
- All IT systems, software, networks, cloud services, and communication platforms used for council activities.
- All data created, stored, processed, or transmitted as part of council operations.

3. Roles and Responsibilities

Councillors and Staff

- Use IT systems responsibly and in accordance with this policy.
- Protect council data from unauthorised access or disclosure.
- Report IT incidents, data breaches, or suspicious activity immediately.

Parish Clerk

- Acts as the primary administrator for council IT systems.
 - Ensures secure storage and management of council records.
- Oversees compliance with data protection and retention requirements.

IT Support (internal or external)

- Provides technical support and maintenance.
- Ensures systems are secure, updated, and backed up.

4. Acceptable Use

- Council IT resources must be used only for legitimate council business.
- Personal use of council devices must be minimal and not interfere with council operations.
- Users must not engage in illegal, offensive, or inappropriate activities.
- Users must not install unauthorised software or alter system configurations.

5. Devices and Security

Council-Owned Devices

- Must be password-protected and encrypted where possible.
- Must have up-to-date antivirus and security patches.
- Must be used in accordance with council data protection requirements.

Personal Devices

- May be used for council business only with Clerk approval.
- Must have secure passwords and updated software.
- Must not store council data permanently unless authorised.

6. Data Protection and Privacy

- All personal data must be handled in accordance with UK GDPR and the Data Protection Act 2018.
- Confidential or sensitive information must not be shared via unsecured channels.

- Data must be stored only in approved locations (e.g., council cloud storage, Clerk's official email).
- Users must ensure documents are shared only with authorised recipients.

7. Email and Communication

- Official council business must be conducted using council-approved email accounts.
- WhatsApp or similar messaging platforms may be used only for operational coordination, not decision-making.
- Confidential matters must not be discussed on messaging apps.
- Important information shared via messaging must be forwarded to the Clerk's official email for record keeping.

8. Passwords and Authentication

- Passwords must be strong (minimum 12 characters, mix of letters, numbers, symbols).
- Passwords must not be shared.
- Multi-factor authentication (MFA) must be used where available.

9. Cybersecurity

- Users must complete basic cybersecurity awareness training annually.
- Phishing emails or suspicious links must not be opened.
- Devices must be locked when unattended.
- Security incidents must be reported immediately to the Clerk.

10. Software and Systems

- Only approved software may be installed on council devices.
- Cloud services must be approved by the Clerk.
- System updates must be applied promptly.

11. Records Management

- Electronic records must be stored in approved council repositories.

- WhatsApp messages may constitute official records and must be retained appropriately.
- Data retention schedules must be followed.

12. Backups

- Council data must be backed up regularly.
- Backups must be stored securely and tested periodically.

13. Incident Reporting

- Any data breach, loss of device, or cybersecurity incident must be reported immediately.
- The Clerk will assess the incident and take appropriate action, including notifying authorities if required.

14. Policy Review

This policy will be reviewed annually or when significant changes occur in legislation, technology, or council operations.

15. Approval

This IT Policy was approved by the Parish Council on: 9 September 2026

To be reviewed as and when required eg if legislation changes.