



Image by Sheila Ashton

CLIFTON PARISH COUNCIL Information Technology Policy

Adopted at the Full Council meeting on 11th September 2025

Introduction.

Clifton Parish Council ("the Council") recognises the importance of effective and secure information technology ("IT") usage in supporting its business, operations and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources by Council members, employees, volunteers and contractors.

Scope.

This policy applies to all individuals who use the Council's IT resources, including computers, networks, software, devices, data and email accounts.

Acceptable Use of IT Resources.

The Council IT resources, where provided, are to be used for official council-related activities and tasks. Personal use should be limited and should not interfere with the Council's work responsibilities.

All users must adhere to ethical standards, respect copyright and intellectual property rights and avoid accessing inappropriate or offensive content.

Device and Software Usage.

Where possible, authorised devices, software and applications will be provided by the Council for work related tasks.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

Data Management and Security.

All sensitive and confidential Council data should be stored and transmitted securely using approved methods.

Regular data backups should be performed to prevent data loss and secure data destruction methods should be used when necessary.

Network and Internet Usage.

The Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited. The following is deemed unacceptable use or behaviour:

- Visiting sites that contain obscene, hateful, pornographic or illegal material.

- Perpetrating any form of fraud or software, film or music piracy.
- Using the internet to send offensive or harassing material to other users.
- Downloading commercial software or any copyrighted materials belonging to third parties, unless the download is covered or permitted under a commercial agreement or other such licence.
- Hacking into unauthorised system, sites or files.
- Publishing defamatory and/or knowingly false information about the Council, colleagues, members and/or customers on social networking sites, blogs, wikis, or any online publishing format.
- Revealing confidential information about the Council in a personal online posting, upload or transmission. Including financial information and information relating to customers, business plans, policies, employees, members and/or internal discussions.
- Undertaking deliberate activities that waste Council effort or networked resources.
- Introducing any form of malicious software into the Council network.

Email Communication.

Email accounts provided by the Council are for official communication only. Email signatures should be used and emails should be professionally and respectful in tone.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking the links.

Password and Account Security.

The Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

The Clerk will regularly update their passwords, these are written down and sealed in an envelope and kept by the current Chair to use in case of emergencies.

Mobile Devices and Remote Work.

Mobile devices provided by the Council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

Reporting Security Incidents.

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution.

Retention and Archiving.

Emails should be retained and archived in accordance with legal and regulatory requirements, as per the Council's Document Retention Policy. Users should regularly review and delete unnecessary emails to maintain an organised inbox.

Training and Awareness.

The Council will provide regular access to resources to educate users about IT security best practices, privacy concerns and technology updates.

Compliance and Consequences.

Breach of this IT policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

Policy Review.

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

Contacts.

For IT-related enquiries or assistance, users can contact in the first instance, The Clerk.

All staff and Councillors are responsible for the safety and security of Clifton Parish Council's IT resources. By adhering to this IT policy, Clifton Parish Council aims to create a secure and efficient IT environment that supports its functions.

Signed: The Clerk/RFO. Date:

Policy Details.

Date of Adoption: 11th September 2025

Review Period: *Annual (to be reviewed Full Parish Council Meeting in September)*

Version: 01