Cholsey Parish Council
IT AND EMAIL POLICY

21st January 2026

1. Introduction

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

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

2. Scope

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

3. Acceptable use of IT resources and email

Cholsey Parish Council IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

4. Device and software usage

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

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

5. Data management and security

All sensitive and confidential Cholsey Parish 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.

6. Network and internet usage

Cholsey Parish 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.

7. Email communication

Email accounts provided by Cholsey Parish Council are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

Council-provided email accounts must be used for all official communication. This ensures sensitive information is handled in a controlled environment with appropriate security measures. It provides a clear record of communications, which is essential for transparency and accountability.

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

8. Password and account security

Cholsey Parish 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.

9. Mobile devices and remote work

Mobile devices provided by Cholsey Parish 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.

10. 'Bring Your Own Device' policy

Cholsey Parish Council recognises that members and employees may sometimes use personally owned devices (e.g. smartphones, tablets, laptops) to conduct Parish Council business.

All users of personal devices for council business must:

- Ensure devices are secured with strong passwords or biometric authentication, and auto-lock after a short period of inactivity;
- Keep devices updated with the latest security patches and antivirus software;
- Use encrypted connections (e.g. VPN or secure Wi-Fi) when accessing council data;
- Avoid using public Wi-Fi unless protected by a secure connection;

- Enable remote wipe capabilities where possible;
- Immediately report any loss, theft, or suspected breach to the Clerk;
- Only access or process personal data for legitimate council purposes;
- Cooperate fully with audits or investigations related to data protection;
- Permanently delete all council-related data from personal devices and email accounts once no longer required or upon leaving the Council.

The council reserves the right to restrict access to council systems from any device that does not meet security standards.

11. Email monitoring

Cholsey Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

12. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

13. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Parish Council Clerk for investigation and resolution. Report any email-related security incidents or breaches to the Clerk immediately.

14. Training and awareness

Cholsey Parish Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

15. Council Property

All hardware and software issued by Cholsey Parish Council remains the property of the Council. When using such equipment:

- You are responsible for all equipment and software until you return it.
- It will be insured by the Parish Council against loss and damage in accordance with the terms and conditions of the Council insurance but must be always kept secure.
- You are expected to take reasonable care of the equipment, and it should be returned in good, clean condition. When travelling it should not be left unattended. If left in a motor vehicle it should be locked in the boot out of sight.

- You are the only person authorised to use the equipment and software issued to you.
- If you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the Council's attention.
- Upon the request of the Council at any time, for any reason, you will immediately return any laptop, equipment, and all software to the Council.

16. Compliance and consequences

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

17. Related Polices

This policy should be read in conjunction with the Council's Social Media Policy.

18. 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.

19. Contacts

Cholsey Parish Council contracts the professional services of ASAP Computer Services to provide IT services including security, support, mailboxes, Microsoft licenses, backups, and advice. Employees experiencing technical issues should report these to the Parish Council Clerk providing as much detail as possible. The Clerk is the Data Controller.

All staff and councillors are responsible for the safety and security of Cholsey Parish Council's IT and email systems. By adhering to this IT and Email Policy, Cholsey Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

Date: _____

Signature: _____

Role: _____