IT POLICY

Chiddingly Parish Council

Adopted in September 2025
Amended and approved March 2026

Julie O'Donnell

Clerk@chiddingly.gov.uk

1. Introduction

Chiddingly 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 Chiddingly Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Chiddingly 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 Chiddingly 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 Chiddingly 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

Chiddingly 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 Chiddingly Parish Council are for official communication only. All council communications must be conducted via official email addresses hosted on a council-owned domain (e.g., **xxx@chiddingly.gov.uk**).

Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

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

Chiddingly 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 Chiddingly 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. Email monitoring

Chiddingly 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.

11. 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.

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

13. Training and awareness

Chiddingly 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.

14. Compliance and consequences

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

15. **Ex-Councillor Email Accounts**

- When a councillor leaves office, the Clerk will notify the council's IT provider within 5 working days to arrange closure of their council email account.
- The IT provider will disable access promptly and apply a short auto-reply (if needed) for up to 30 days, directing the public to the Clerk's office.
- The closed account will be retained in archive form for 12 months for audit, FOI, or legal purposes. Access is limited to the Clerk and IT provider.
- After 12 months, the IT provider will permanently delete the mailbox and confirm deletion to the Clerk.
- If the mailbox is needed for an active complaint, legal matter, or investigation, the Clerk may instruct the IT provider to pause deletion until the matter is concluded.
- All actions must comply with the parish council's data protection and records-retention requirements.

16. 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.

17. Contacts

For IT-related enquiries or assistance, users can contact the Clerk or the Council's IT Provider.

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