

Cotesbach Parish Council

IT Policy

1. Introduction

Cotesbach Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its operations and communications. This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees and contractors.

2. Scope

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

3. Acceptable use of IT resources and email

Cotesbach 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

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 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

The 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 the 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.

Caution should be taken with attachments and links to avoid phishing and malware. The source should be verified before any attachments or links are opened.

8. Password and account security

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. Working Remotely

Mobile devices provided by the Parish Council should be secured with passcodes and/or biometric authentication.

10. Email Monitoring

Cotesbach Parish Council reserve 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. Emails should be regularly reviewed and unnecessary ones deleted to maintain an organised inbox.

12. Reporting of Security Incidents

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

13. Compliance and consequences

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

14. 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.

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

Approved by the Parish Council at the Parish Council meeting dated 1st September 2026, item 12