

CABUS PARISH COUNCIL

Information Technology Policy

1. Introduction

Cabus 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 employees and council members.

2. Scope

This policy applies to all individuals who use Cabus Parish Council's IT resources and email accounts.

3. Acceptable use of IT resources and email

Cabus 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. Data management and security

All sensitive and confidential Cabus 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.

5. Email communication

Any email accounts provided by Cabus Parish Council are for official communication only. Emails should be professional and respectful in tone. Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

6. Password and account security

Cabus Parish Councillors and staff are responsible for maintaining the security of their IT accounts and passwords (whether they are provided by Cabus Parish Council or not). Regular password changes are encouraged to enhance security.

7. Mobile devices and remote Work

Any mobile devices provided by Cabus Parish Council should be secured with passcodes and/or biometric authentication.

8. 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.

9. Reporting security incidents

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

10. Training and awareness

Cabus Parish Council will keep abreast of IT and email security best practices and will share training opportunities with all employees and councillors.

11. Policy review

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