

West & Middle Chinnock Parish Council

IT POLICY

1. Introduction

West & Middle Chinnock Parish Council (the 'PC') 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 ('User' or Users).

2. Scope

This policy applies to all individuals who use the PC's IT resources, including but not limited to computers, networks, software, devices, data and email accounts.

3. Acceptable use of IT resources and email

The PC's IT resources and email accounts are to be used for official council-related activities and tasks only.

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 the PC 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

The PC's sensitive and confidential 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 PC'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 PC are for official communication only. Emails will be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted. Users should be cautious with attachments and links to avoid phishing and malware. Users should verify the source before opening any attachments or clicking on links.

8. Password and account security

Users are responsible for maintaining the security of their email 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

If any mobile devices are provided by the PC, these should be secured with passwords and/or biometric authentication. If working remotely, Users should follow the same security practices as if they were in the office.

10. Email monitoring

The PC 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. Emails should be regularly reviewed and unnecessary emails deleted to maintain an organised inbox.

12. Reporting security incidents

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

13. Training and awareness

The PC will arrange regular training and resources to educate employees and councillors about IT and email security best practices, privacy concerns, and technology updates.

14. Compliance and consequences

Breach of this IT Policy may result in the suspension by the PC of User(s)' IT privileges and further consequences as deemed appropriate.

15. Policy review

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

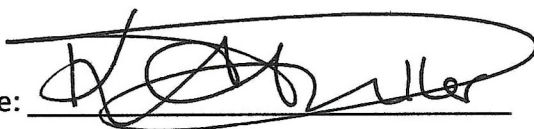
16. Contacts

For IT-related enquiries or assistance, Users can contact the Clerk to the PC. Kdullerpheme@gmail.com
All employees and councillors are responsible for the safety and security of the PC's IT and email systems.

By adhering to this IT Policy, the PC aims to create a secure and efficient IT environment that supports its mission and goals.

Date: 11th February 2026

Reference: 26/1412

Signature: 

Role: Clerk & RFO