

WINGHAM PARISH COUNCIL IT POLICY

1. Introduction

Wingham Parish Council (WPC) 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 WPC's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

WPC 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 WPC 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 WPC 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. [Ref: WPC Retention and Disposal of Documents Policy]

6. Network and internet usage

WPC'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 WPC 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 password encrypted, with the password provided under separate communication.

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

WPC 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 WPC 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. Council members are encouraged to use passcodes and/or biometric authentication on any personal devices used to access WPC information and emails. Devices should have an active mechanism in place to protect against viruses, phishing and malware.

10. Email monitoring

WPC 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. [Ref: WPC Retention of Documents Policy]

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact (the Clerk) for investigation and resolution. Report any email-related security incidents or breaches to the Clerk immediately. [Ref: WPC Internal Data Protection Policy – Draft]

13 Training and awareness

WPC will provide regular training and resources to educate users about IT security best practices. All employees and councillors will receive regular training on email security and best practices. [Ref: WPC Training, Learning And Development Policy]

14. Compliance and consequences

Breach of this IT policy may result in the suspension of IT privileges and further consequences in relation to the Code of Conduct.

15. 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.

16. Contacts

For IT-related enquiries or assistance, users can contact the Parish Clerk in the first instance.

All staff and councillors are responsible for the safety and security of WPC's IT systems. By adhering to this policy, WPC aims to create a secure and efficient IT environment.