WHITEHILL
TOWN COUNCIL
Serving Whitehill & Bordon

IT POLICY

Date of adoption: 26.06.2021 Review date: 06.11.2025 Next Review: 05.11.2026

1. Introduction

1.1. Whitehill Town Council (WTC) recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

1.2. This policy outlines guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers and contractors.

1.3. The Town Clerk is responsible for the implementation and monitoring of this policy but may delegate that responsibility to another officer.

1.4. Line managers have a responsibility to ensure that staff they supervise comply with this policy.

2. Scope & General Principles

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

2.2. All employees, members and other users should be aware of the increasingly sophisticated scams and risks posed to cybersecurity and when in any doubt should seek guidance from the Town Clerk

2.3. As a rule users will never be asked to share passwords by email and users should be aware of odd language used in emails which may indicate a fraudulent email.

2.4. All employees, members and other users of council IT equipment must be familiar with and abide by the regulations set out in the council's 'Data Protection & Retention Policy'.

2.5. All council devices will have up-to-date antivirus software installed and this must not be switched off for any reason without the authorisation of the Town Clerk.

2.6. All users are reminded that deliberate unauthorised use, alteration, or interference with computer systems, software or data is a breach of this policy and in some circumstances may be a criminal offence under the Computer Misuse Act 1990.

2.7. All software installed on council devices must be fully licensed and no software should be installed without authorisation from the Town Clerk.

3. Acceptable use of IT resources and email

3.1. WTC's 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.

3.2. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

4. Training and guidance

4.1. Employees and volunteers will be provided with regular cybersecurity training as is appropriate for their role and level of systems access.

4.2. Members will be provided with a brief overview of cybersecurity measures as part of induction and may be provided with more in-depth training as required.

5. Device and software usage

5.1. Where possible, authorised devices, software, and applications will be provided by WTC for work-related tasks.

5.2. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

6. Data management and security

6.1. All sensitive and confidential WTC 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.

7. **Network and internet usage**

7.1. WTC's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

8. Email communication

8.1. Email accounts provided by WTC 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.

8.2. Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

9. Password and account security

9.1. WTC's users are responsible for maintaining the security of their accounts and passwords.

9.2. All council computers and systems must be password protected to prevent unauthorised access.

9.3. Users should ensure that unattended devices are password protected, and the computer has been locked.

9.4. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

10. Mobile devices and remote Work

10.1. Mobile devices provided by WTC 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.

11. Email monitoring

11.1. WTC 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.

12. Retention and archiving

12.1. Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

13. Reporting security incidents

13.1. 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.

14. Compliance and consequences

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

15. Policy review

15.1. This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technological trends and security measures.

16. Contacts

16.1. For IT-related enquiries or assistance, users can contact the Clerk or Deputy Clerk. All staff and councillors are responsible for the safety and security of WTC's IT and email systems.

16.2. By adhering to this IT and Email Policy, WTC's aims to create a secure and efficient IT environment that supports its mission and goals.