IT Policy

Date of adoption: 30th September 2025

---

1. Introduction

Tickhill Town 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 council members, employees, volunteers, and contractors.

2. Scope

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

3. Acceptable use of IT resources and email

Tickhill council IT resources and email accounts are to be used for official council-related activities and tasks. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

All email communications regarding council business must be conducted using official council email accounts only.

4. Device and software usage

Where possible, authorised devices, software, and applications will be provided by Tickhill Town council to employees for work-related tasks.

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

Software updates should be installed promptly to maintain security.

5. Data management and security

All sensitive and confidential Tickhill Town 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

Tickhill Town council's network and internet connections should be used responsibly and efficiently for official purposes. Tickhill Town Council files must not be accessed over open or unsecured Wi-Fi networks including public Wi-Fi. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

Email accounts provided by Tickhill Town 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.

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

Tickhill Town council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong, unique and not shared with others. A password secure document is held in line with the Business Continuity Plan both on the OneDrive and in the Council safe.

All councillors and staff using their own devices for Tickhill Town Council business should have adequate up to date anti-virus protection and not leave their account logged on when away from their device. Utilise the shortcut 'windows L' to lock your screen if away for just a short time as an alternative to logging out.

9. Mobile devices and remote Work

Mobile devices provided by Tickhill Town council should be secured with passcodes and/or biometric authentication and no-one other than those with the authority to do so should use them. When working remotely, users should follow the same security practices as if they were in the office.

If using your own mobile device for email and access to Tickhill Town Council files, the device must be password protected and you must not permit anyone else to use the device to avoid accidental access to confidential files.

10. Email monitoring

Tickhill Town council reserves the right to monitor email communications and IT use 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 and the Tickhill Town Council Retention Policy. Regularly review and delete unnecessary and spam emails to maintain an organised inbox.

12. Reporting security incidents

All suspected security breaches, email-related security breaches or incidents should be immediately reported to the Clerk for investigation and resolution or the Chair, in the event of the Clerk being unavailable. These will then be reported to the IT support provider, ESP Projects.

Any loss of theft of council equipment or devices containing confidential council information must be reported to the Clerk or Chair immediately.

Report any email-related security incidents or breaches to the IT administrator immediately

13 Training and awareness

Tickhill Town council will provide regular training and resources where necessary to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

14. Compliance and consequences

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

15. Contacts

For IT-related enquiries or assistance, in the first instance please report any issues to the Clerk, users can also contact Tickhill Town Council's IT provider;

ESP Projects
Support@espprojects.co.uk
Tel: 0330 2020 118 option1

All staff and councillors are responsible for the safety and security of Tickhill Town council's IT and email systems. By adhering to this IT and Email Policy, Tickhill Town council aims to create a secure and efficient IT environment that supports its mission and goals.

16. Policy review

This policy will be reviewed annually or following any change in legisaltion to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

Date of adoption: 30th September 2025

Adopted by Full Council

Review Date: September 2026

(Source:) 2025 Practitioners Guide