Information Technology Policy

1. Introduction

Towcester 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 the Council's IT resources, including computers, networks, software, devices, data, and email accounts.
This IT Policy should be read alongside the Council's other adopted policies and procedures, including but not limited to:

- Communications Policy
- Data Protection Policy
- Email Communication Policy
- Social Media Policy
- Staff Handbook: Section 26: Internet Policy and Procedure

Together, these documents form the Council's approach to responsible digital governance and legal compliance.

3. Roles and Responsibilities

The Town Clerk is responsible for managing and enforcing this policy, ensuring IT resources are used appropriately and securely. Councillors and staff are responsible for complying with the policy and reporting any breaches and incidents immediately. External IT support providers and contractors must adhere to the standards set out in this policy when handling council information.

4. Acceptable Use of IT Resources and Email

The Council's IT resources and email accounts are to be used for official council-related activities and tasks. Personal use is discouraged and, where permitted, must not interfere with work responsibilities or violate any part of this policy. The use of personal email accounts for council business is prohibited. All council correspondence must be conducted through official email addresses. Users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

5. Device and Software Usage

Where possible, authorised devices, software, and applications will be provided by the Council for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

6. Data Management and Security

All sensitive and confidential 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. Staff and councillors must not disclose confidential council information to any unauthorised person, either during or after their term of office or employment.

7. Network and Internet Usage

The Council'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

Towcester Town Council provides all staff and Councillors with an official email address which is to be used for council business purposes. Email accounts provided by the 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. Users are to 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

Individuals, whether using their own device or one provided by the Council, 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. All Council-provided email accounts must have Two-Factor Authentication (2FA) enabled.

10. Mobile Devices and Remote Work

Mobile devices provided by the Council 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. Use of Own Devices

Councillors and staff may use their own devices for Council-related activities, provided that the following security requirements are met:

11.1 Device Security

- Devices must be protected with strong passwords and/or biometric authentication.
- Operating systems and applications must be kept up to date.
- Up-to-date antivirus software and operating system must be installed and active.
- An automatic screen lock should activate after a short period of inactivity (recommended: 5 minutes).

11.2 Data Protection

- Council documents should not be stored locally unless password-protected or encrypted.
- Sensitive or confidential information must only be accessed via secure cloud services (e.g. OneDrive, SharePoint) or encrypted email platforms.
- Personal data should be kept separate from Council data wherever possible.
- Ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device.

11.3 Network Security

- Only use secure Wi-Fi networks when accessing Council data or systems. Avoid public or unsecured networks.

12. Email Monitoring

The Council 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.

13. Third-party Access and Security Standards

Any contractors or third-party software providers accessing Council data or systems must do so under a formal agreement. This access must be limited to the data or systems necessary for their role, logged appropriately, and revoked as soon as work is completed.

14. Use of CCTV and Surveillance

Where the Council operates CCTV or similar surveillance systems, they will be used solely for the purpose stated at the time of installation (such as crime prevention or public safety). All systems must comply with the ICO's CCTV Code of Practice. Signs must be clearly displayed in areas under surveillance. Data must be stored securely, retained only for the legally allowed duration, and accessed only by authorised personnel.

15. Digital Inclusion and Accessibility

The Council recognises the importance of digital inclusion. Support and training will be offered to councillors and staff who are less confident using technology. Residents who are digitally excluded will be offered alternative methods of accessing council information and services, such as paper notices or telephone enquiries. The Council's website and online documents must comply with accessibility regulations and offer downloadable content in accessible formats.

16. Retention and Archiving

Emails should be retained and archived in accordance with legal and regulatory requirements and the Council's Retention and Disposal Policy.

17. Reporting Security Incidents

All suspected security breaches or incidents should be reported immediately to the Town Clerk for investigation and resolution.

18. Training and Awareness

The Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates.

19. Compliance and Consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges and may also result in disciplinary action, reporting to the Monitoring Officer, or other action in line with the Council's Code of Conduct or HR procedures.

20. 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.