

Tywyn Town Council

Information Technology Policy

1. Introduction

Tywyn 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 councillors, 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. It also applies to those using their own devices for Council business.

3. Acceptable use of IT resources and email

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

The Council'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 or General Data Protection Regulations (GDPR).

All users must adhere to ethical standards and in line with Council's Code of Conduct, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

Documents and emails containing confidential data must not be forwarded to unauthorised parties or saved to unsecured platforms.

Councillors and staff must not download or save documents outside of the Council's secure environment (SharePoint) unless authorised by the Business Manager. Councillors may save documents to personal devices if the requirements in section 11 are met.

4. 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.

5. Use of Artificial Intelligence (AI)

AI may be used for low level tasks such as efficiency and automation (e.g., customer service chatbots), data analysis, and drafting assistance with documents such as letters or reports. However, there must always be a sense check edit performed by a competent member of staff and this must include a bias and fairness check.

AI must not be used for automated decision-making on services that affect residents' rights or on subjects where the staff member or Councillor does not have the expertise to be able to weigh up the appropriateness and validity of outputs.

You must not load confidential data into any AI platform.

Any document produced using AI must carry a disclaimer stating “Portions of this document have been drafted using AI tools. The final document has been signed off by a competent person.”

Officers and Councillors should be aware of the current concerns globally regarding the amount of power and water being used to support AI platforms and usage. Usage should be kept to a minimum in recognition of the environmental impacts.

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 are required to comply with the Council’s Retention and Disposal Policy and the Council’s Data Protection and Privacy Policy.

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

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 devices or not, 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.

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 personal devices

Councillors and staff may use their own devices for Council business, provided they meet the following requirements:

- Devices must be password protected and locked when not in use
- Up-to-date antivirus and security software must be installed
- Automatic screen lock must activate after a short period of inactivity
- Council documents should not be stored locally unless password-protected or encrypted
- Sensitive or confidential information must only be accessed via secure cloud services or encrypted email platforms

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. Retention and archiving

Emails, documents, and other information should be retained and archived in accordance with legal and regulatory requirements and the Council's Retention and Disposal Policy. Regularly review and delete unnecessary emails and documents is strongly suggested to ensure compliance.

14. Reporting security incidents

All suspected security breaches or incidents related to IT and emails should be reported immediately to the Clerk for action, including investigation and resolution.

15. Training and awareness

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

16. Compliance and consequences

Breach of this IT and any other relevant Council policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

17. 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 at any point.

If you need any specific help or general guidance about the Council's procedures, please contact the Clerk.

In writing to The Town Clerk, Tywyn Town Council, The Council Office, High Street, Tywyn, LL36 9AD

By telephone 01654 712411

By Email clerk@tywyntowncouncil.org.uk

Adopted by Tywyn Town Council on 10 June 2026

Minute CI 048. 10.6.26

To be reviewed annually