Axminster Town Council

IT Policy

1. Introduction

Axminster 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 Axminster Town Council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Axminster Town Council's IT resources and email accounts are to be used primarily 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

Wherever possible and practicable, authorised devices, software, and applications will be provided by Axminster Town Council 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 Axminster 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

Axminster Town 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.

7. Email communications

Email accounts provided by Axminster 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. Always 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

Axminster Town Council 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 working

Mobile devices provided by Axminster Town Council should be secured with passcodes and/or biometric multi-factor authentication. When working remotely, users should follow the same security practices as if they were in the Council offices.

10. Email monitoring

Axminster Town 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. In the event of a SAR or a FOI request, email users will be obliged to allow full access to their emails in order for the Council to ensure compliance with Data Protection and Disclosure regulations.

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.

12. Reporting security incidents

All suspected or actual 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 IT administrator immediately.

13. Training and awareness

Axminster Town Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates.
All employees and Councillors will receive regular training on email security, cyber security and best practices

14. Compliance and consequences for non-compliance

Breach of this IT Policy may result in the suspension of IT privileges and further consequences as deemed appropriate, as laid out in the employee Disciplinary Policy and the Member Code of Conduct Policy.

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.

The Town Council has adopted this policy to comply with the requirements laid down in the template issued by the UK Government Digital Service (GDS) and in accordance with the requirements for AGAR Assertion Ten. It is subject to periodic update no later than five years from adoption, or earlier as indicated above, or in the event of published legislative amendment.

16. Contacts

For IT-related enquiries or assistance, users can contact the Town Clerk or Deputy Town Clerk.

17. Policy Purpose

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

First Adopted	Review Schedule	Current Revision	Last Adopted	Minute Reference	Date of Next Review
March 2026	Annual	Version 1	30/03/2026	EFC 26/101.i	March 2027