Alcester Town Council IT and Email Policy

1. Introduction

Alcester Town Council (ATC) 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 ATC's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

ATC 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. 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

Where possible, authorised devices, software, and applications will be provided by ATC 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 ATC 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
ATC'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 communication
Email accounts provided by ATC are for official communication only and should follow the following guidelines:

a. Use appropriate language to avoid unintentional misunderstandings;
b. Respect the confidentiality of information contained within emails, even if encountered inadvertently;
c. Check with the sender if there is any doubt regarding the authenticity of a message;
d. Do not open any attachment unless certain of the authenticity of the sender;
e. Only copy emails to others where appropriate and necessary;
f. Emails which create obligations or give instructions on behalf of the Council must be sent by officers only, not councillors or other individuals;
g. Emails must comply with common codes of courtesy, decency and privacy.

Care must be taken when addressing emails, particularly those including sensitive, confidential or restricted information, to avoid accidentally sending them to the wrong people. Particular care must be taken when software auto-completes an email address.

Personal email accounts should not be used for Council business due to potential data breaches, issues surrounding Freedom of Information or Subject Access Requests.

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

Council email addresses must not be used for:

a. Any political activities;
b. Commercial or personal profit-making purposes or other form of financial gain (e.g. in connection with any employment other than that associated with the Council);
c. Activities that lead to unauthorised expenditure for the Council (e.g. excessive printing or photocopying that is not Council business);
d. Activities that are contrary to Council policies or standards;
e. Personal interest group activity outside of a user's role;
f. Activities that may cause damage, disruption, fines, penalties or negative media attention for the Council;
g. Excessive email conversations that may be interpreted as misuse.

Email accounts must have an appropriate email signature and the relevant email disclaimer at the bottom of all emails written. Appropriate disclaimers will be provided by the Town Clerk.

8. Communication via social media or text messages
Councillors should avoid replying to residents via social media or text message particularly if the issue raised is a request for information or might be a complaint. Whenever possible, Councillors should respond to messages received via their Council email account or refer the correspondent to the Town Clerk**.**

9. Password and account security
ATC 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.

10. Mobile devices and remote Work
Mobile devices provided by ATC 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
ATC 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
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
All suspected security breaches or incidents should be reported immediately to the Town Clerk for investigation and resolution. Report any email-related security incidents or breaches to the Town Clerk immediately.

14. Training and awareness
ATC 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 and best practices.

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

16. Policy review
This policy will be reviewed regularly to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

17. Contacts
For IT-related enquiries or assistance, staff users can contact Davis Ground IT Services Ltd via their helpdesk.

All staff and councillors are responsible for the safety and security of ATC's IT and email systems.

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

Approved by Finance and General Purposes Committee – 27th May 2025

Adopted by Full Council – 3rd June 2025

Review due May 2027