Ash Parish Council

IT Policy

Ash Centre
Ash Hill Road
Ash
Surrey
GU12 5DP
Tel: 01252 328287
Fax: 01252 319338
E-mail: office@ashpcsurrey.gov.uk

Adopted by Ash Parish Council	13 April 2026
Review Date	12 April 2027

Ash Parish Council

IT Policy

Introduction

Ash Parish Council ("the 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.

Scope

This policy applies to all Councillors who use the Council's IT resources, including computers, networks, software, devices, data, and email accounts. It is aligned to the Email & Internet Policy in the Employee Handbook.

Acceptable Use Of IT Resources & Email

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. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

Device & Software Usage

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

Data Management & 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.

Network & Internet Usage

The Council's network should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

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.

Councillors must use their .gov email address for Council business and never their personal email addresses.

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

Password & Account Security

The 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.

Tablets, Laptops & Remote Working

Tablets and laptops 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.

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.

Retention & Archiving

On leaving the Council, access to emails will be kept until operationally necessary, after resetting password. Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

Reporting Security Incidents

All suspected security breaches or incidents should be reported immediately to the Clerk for investigation and resolution. Report any email-related security incidents or breaches to the Clerk immediately.

Training & Awareness

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

Compliance & Consequences

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

Cyber Security

The Council acknowledges the evolving nature of cyber threats, including but not limited to :

- Phishing and social engineering
- Malware and ransomware
- Unauthorised access or data breaches
- Insider threats
- Denial-of-service attacks

The Council will implement and maintain the following technical safeguards :

- Firewalls and antivirus software
- Multi-factor authentication (MFA) for system access

- Regular software updates and patch management
- Secure configuration of devices and systems
- Encrypted communications and secure data storage
- Cyber security controls will be reviewed annually or following a significant incident
- The Council will stay informed of best practices and regulatory changes

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.

Contacts

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

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