This policy will be reviewed bi annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

Amber Hill Parish Council IT and email Policy

1. Introduction

Amber Hill Parish 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.

This policy applies to all individuals who use Amber Hill Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

2. Acceptable use of IT resources and email

The Council recognises that some councillors, staff, and other authorised users may wish to use their own smart phones, tablets, laptops etc to access our servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the council's cloud services or to store data on the council's server(s) or access data in other services. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (Microsoft Windows, Mac OS X, Linux - in commercial configurations) will normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

However, the same security precautions apply to personal devices as to the council's desktop equipment. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

Wherever possible, the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

Councillors, staff, and other authorised users who intend to use their own devices via the council's infrastructure must ensure that they:

- use a secure passcode, passphrase or biometrics to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after 10 failed login attempts
- configure their device(s) to automatically prompt for a password after a period of inactivity
- always password protect any documents containing confidential information that are sent as attachments to an email, and notify the password separately (preferably by a means other than email)
- for smartphones and tablets, activate the automatic device wipe function (where available). Note that use of the remote wipe function may also involve the removal of the individual's personal data. Councillors, staff, and other authorised users are therefore advised to keep personal data separate from council data where possible;
- ensure secure WiFi networks are used;
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device;

- inform the Clerk if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

3. Device and software usage

Where possible, an authorised device,(laptop computer), software, and applications will be provided by Amber Hill Parish Council for work-related tasks undertaken by the Clerk (this will remain the property of the Council at all times). Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

4. Data management and security

All sensitive and confidential Amber Hill Parish Council's 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.

5. Network and internet usage

Amber Hill Parish 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.

6. Email communication

Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted. Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

7. Password and account security

Amber Hill Parish 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.

8. Mobile devices and remote Work Mobile devices provided by

Amber Hill Parish 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 an office.

9. Email monitoring

Amber Hill Parish 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.

10. 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.

11. Reporting security incidents.

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email related security incidents or breaches to the IT administrator immediately.

12. Training and awareness

Amber Hill Parish Council can 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 access to training on email security and best practices.

14. Compliance and consequences

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

15. Policy review

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

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

Adoption date: 16/03/2026

Agenda Reference: 10.