INFORMATION TECHNOLOGY POLICY

POLICY APPROVAL

Adopted by: Ashendon Parish Council

Meeting date: 9th March 2026

Minute reference: [Item 9]

Next review date: May 2027 for AGM

1. Introduction

Ashendon 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:-

Applies to all individuals who use the Council's IT resources, including computers, networks, software, devices, data, and email accounts.

Applies to all individuals who use the Council's IT systems for Council business, including computers, networks, software, devices, data, and email accounts. Regardless of whether they are using council-owned or personal devices.

Outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

The Council meets the Governments digital communication requirements - SAAPP 2025 for email communication and website accessibility (WCAG)2.2AA.

2. Acceptable Use of IT Resources and 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.

3. 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.

4. 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. See the Councils Data Policy for further information.

Council laptops must not have software installed without prior consent and no personal data should be stored unencrypted on any devices or cloud platforms without Council approval.

5. 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.

6. 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.
The Council must be cautious with attachments and links. It must verify the source before opening any attachments or clicking on links to avoid phishing and malware.

7. Password and Account Security

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.

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. To protect devices from being accessed All devices must lock after 3 attempts to log in and after a short period of time lock if no activity is detected.

8. 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. To protect devices from being accessed All devices must lock after 3 attempts to log in and lock after a short time of inactivity.

9. 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.

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

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

13. Compliance and Consequences

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

14. Responsibilities

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

15. Social and Digital Communication

Website www.ashendon.org.uk is used by the Council for its digital communication. Only the Clerk, Chair and Vice Chair is authorised to post on the Council's official social media pages.

16. Contact and Assistance

For IT-related enquiries or assistance, users can contact the parish clerk at:-
INSERT NEW EMAIL

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.