IT Policy

EWERBY AND EVEDON PARISH COUNCIL IT POLICY

1. Introduction

EEPC 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 EEPC's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

EEPC 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

Authorised devices, software, and applications may be provided by EEPC 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 EEPC 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

EEPC'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

The email account provided by EEPC is provided 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.

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

EEPC 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. Email monitoring

EEPC 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, via the Clerk. Report any email-related security incidents or breaches to the Clerk immediately.

13 Training, awareness and compliance

EEPC will use available training and resources to educate users about IT security best practices, privacy concerns, and technology updates and refer staff and Councillors to online sources such as **https://www.ncsc.gov.uk/collection/phishing-scams**

14. Contacts

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

Adopted by the Clerk 11th February 2026