
For Information

IT Policy

Adopted:

Chairman: Cllr. L Street

Minute Ref.: 260119/___

*Administered by Clerk and Responsible Financial Officer
to Barrow Parish Council.*

IT POLICY

Introduction

Assertion 10 is a new requirement for Parish Councils, starting with the 2025/6 Annual Governance and Accountability Return (AGAR), that mandates compliance with digital and data governance standards. Key requirements include operating with a council-owned domain email and website, ensuring the website meets WCAG 2.2 AA accessibility standards, having a comprehensive IT policy, and demonstrating compliance with data protection laws like the UK GDPR and Data Protection Act 2018.

Barrow Parish Council's website and email services are provided by EasyWebsites who ensure the website is compliant with accessibility standards and who recently upgraded the Council's email accounts to gov.uk addresses to ensure compliance with Assertion 10 requirements.

The adoption of this IT policy forms the final strand in Barrow Parish Council's overall compliance with the new Assertion 10 requirements.

Barrow Parish Council IT Policy

1. Introduction

Barrow 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.

2. Scope

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

3. Acceptable use of IT resources and email

Barrow Parish Council 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 Barrow Parish Council 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 Barrow Parish 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.

6. Network and internet usage

Barrow 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.

7. Email communication

Email accounts provided by Barrow Parish 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.

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

Barrow 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.

9. Mobile devices and remote Work

Mobile devices used for Parish Council activities 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.

10. Email monitoring

Barrow 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.

11. 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.

12. 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.

13 Training and awareness

Barrow Parish Council 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.

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

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

16. Contacts

For IT-related enquiries or assistance, users can contact the Clerk or contact the Easywebsites support team direct (01995 917972 Option 1, between 9am and 5pm Monday to Friday (for out of hours support call 07900 993874).

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

Signed:



Chair, Barrow Parish Council

Date:

19th January 2027

Adopted: January 2026

Reviewed:

Next Review: January 2027