Broughton Parish Council

IT AND EMAIL POLICY

1. Introduction

Broughton 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. Whilst this policy is not specifically about GDPR, the GDPR policy is closely linked and must be followed at all times.

2. Scope

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

3. Acceptable use of IT resources and email

Broughton Parish Council's IT resources and email accounts are to be used for official council-related activities and tasks only. 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 Broughton Parish Council for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited to avoid compromising security.

5. Data management and security

All sensitive and confidential Broughton Parish Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and data destruction methods should be as secure as reasonably possible.

6. Network and internet usage

Broughton 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 Broughton Parish Council are for official communication only. All Council activity must use the approved provided accounts. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is personal information relating to a councillor or employee should not be included in the body of an email but should be sent using a password protected file.

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

Broughton 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. The clerk will remove access to the email account with immediate

effect upon their departure from the Council, unless agreed by the Chairman and Clerk for the purposes of continuity in "handover" of duties by a retiring councillor.

Once that email account is no longer needed the clerk will delete it. Email accounts from retiring Chairs or other councillors with specific duties may need retaining for longer periods of time, in line with our GDPR policy.

9. Mobile devices and remote work

Mobile devices provided by Broughton 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 the office.

10. Email monitoring

Broughton 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 General Data Protection Regulation (GDPR).

11. Retention and archiving

Emails should be retained, archived or deleted in accordance with our GDPR policy and any legal and regulatory requirements, regularly reviewing and deleting 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. Any email related security incidents or breaches must be reported to the IT administrator immediately. In both cases this is the clerk.

13. Training and awareness

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

14. Compliance and consequences

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

Approved: 2nd March 2026 (Minute Ref: 2025/26-83)

For Review: March 2027