



Brereton Parish Council

IT Policy

1. Introduction

Brereton 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 and the Clerk.

2. Scope

This policy applies to all individuals who use Brereton Parish Council's IT resources, and/or personal devices used for Parish Council work, including computers, networks, software, devices, data and email accounts.

3. Acceptable use

Brereton 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, increase the risk of introducing malware 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. Downloading and sharing copyrighted material without proper authorisation is prohibited.

Any communications shared via social media should be succinct and respectful in tone and limited for the purposes of information sharing to the general public, and to promote/highlight the parish. Members should ensure they are adhering to the Council's code of conduct when using social media.

Members using social media in their capacity as councillors must make it clear they are speaking in a personal capacity and not representing the view of the council. In the event of 'flaming' or a war of comments breaking out, further engagement should be

restricted to requesting the parties bring any issues to the Parish Council's attention via the normal channels.

4. Device and software usage

Where possible, authorised software, and applications will be provided by Brereton Parish Council for work-related tasks.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited.

If personal devices are used during Brereton Parish Council work, they must meet minimum security standards as stipulated in this policy.

Members and the Clerk must ensure that:

- Devices are password-protected and kept secure at all times.
- Devices are regularly updated with the latest software and security patches.
- Devices run antivirus or other protective software.

Static data (non-email) ideally should not be downloaded to the local, personal device. If, however data is downloaded it should be deleted immediately after use on the personal device. It should be noted that version control may be needed where copies of data are being made and manipulated.

5. Data management and security

All sensitive and confidential Brereton Parish Council data should be stored and transmitted securely using approved encryption standards.

Any USB storage device must be scanned for malware using high grade security software, we currently use McAfee.

An annually review and audit should be undertaken to understand where static data and email is/has been stored, and reviews should be undertaken to delete data that is not required, in line with data retention policy and GDPR.

6. Retention and Archiving

Emails and Parish Council data must be managed in line with legal and regulatory requirements. The Clerk will ensure records are archived for as long as required and securely deleted once they are no longer needed. Users should review their inboxes regularly and remove unnecessary emails but must not delete material that could form part of a Freedom of Information (FOI) or Subject Access Request.

7. Email communication

Email accounts provided by Brereton Council are for official communication only. Emails should be professional and respectful in tone. Brereton 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.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links. If in doubt, seek guidance from the Clerk.

8. Password and account security

All employees, members and other users should be aware of the increasingly sophisticated scams and risks posed to cybersecurity. As a general rule, users will never be asked to share passwords by email and users should be aware of odd language used in emails which may indicate a fraudulent email.

Brereton 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. A strong password is long (8-12+ characters), uses a random mix of uppercase and lowercase letters, numbers, and symbols, and contains no personal information or common dictionary words.

Screen locks on devices should be set to automatically invoke after a reasonable idle time e.g., 5 mins

Members must ensure that any personal devices used to access council systems (including email, websites and data) are password protected with unique, strong passwords and access is restricted solely to the member.

Mobile devices used for Brereton Parish Council work 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.

Public Wi-Fi should not be used for Parish Council work unless a secure virtual private network (VPN) or mobile hotspot is used.

12. Reporting security incidents

All suspected security breaches or incidents must be reported immediately to the Clerk for investigation and resolution.

This includes but is not limited to:

- Lost devices
- Potential risk arising from phishing emails/websites
- Passwords having been shared
- Unauthorised access to systems
- Accidental sharing of personal data
- Suspected malware

13. Training and awareness

Brereton Parish Council will arrange regular training and resources to update members about IT security best practices, including email security and best practices, privacy concerns and technology updates.

15. Websites

The Clerk shall ensure that any websites operated by the council are regularly reviewed to ensure content is accurate, accessible and up to date. Websites shall also be monitored for unauthorised access and abuse.

Websites will comply with WCAG 2.2 AA accessibility standards and the Public Sector Bodies Accessibility Regulations 2018. The Clerk will ensure that all required documents (e.g. FOI Publication Scheme, Transparency Code documents, AGAR) are published and updated.

16. Compliance and consequences

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

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.

18. Contacts

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

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