

Broadclyst Parish Council IT Policy

1. Introduction

Broadclyst 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. It is adapted from the NALC template released in July 2025 to help local councils comply with Assertion 11 in the 25/26

2. Scope

This policy applies to all individuals who use Broadclyst parish council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Broadclyst 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 Broadclyst parish council for work-related tasks. Where personal devices are used for council business, users should comply with the BYOD policy in Appendix A and complete / return the form in Appendix B.

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 Broadclyst 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.

5A. Cloud Services and Data Residency

Cloud Storage and Processing

All cloud services used by the Council must:

- Be pre-approved by the Clerk or Responsible Finance Officer.
- Comply with UK GDPR, ensuring data is stored within the UK or the European Economic Area (EEA) unless adequate safeguards are confirmed.
- Be subject to a written agreement that includes appropriate data processing and security provisions.

Reference: Information and Data Protection Policy, "Data Security" and "Information Security" sections.

5B. Accessibility Requirements

Accessibility of Digital Content

All digital communications, including email, documents, and web content, must comply with the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018. This means information should be:

- Perceivable and usable by people with disabilities.
- Provided in accessible formats upon request.

Staff and councillors must seek advice from the Clerk where assistance is needed to ensure accessibility.

6. Network and internet usage

Broadclyst 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 Broadclyst 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.

7A. Social Media and Email Integration

Use of Social Media

When using Council email or IT systems to communicate via social media, users must comply with the Social Media Policy (Adopted May 2023) and the Media Communications Policy (Reviewed May 2023). Personal opinions must not be presented as the official view of the Council.

All posts must be respectful, accurate, and compliant with the Council's Code of Conduct.

8. Password and account security

Broadclyst 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.

8A. Password Management (Updated)

Password Standards

In line with National Cyber Security Centre guidance, users must:

- Use long, unique passphrases.
- Avoid password reuse.
- Change passwords only if compromise is suspected or advised by the Clerk.
- Use multi-factor authentication where available.

9. Mobile devices and remote Work

Mobile devices provided by Broadclyst 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

Broadclyst 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.

12A. Incident Reporting and Response Timescales

Incident Response

All IT security incidents must be reported to the Clerk and Data Protection Officer within 24 hours of discovery. The Council maintains an Incident Response Procedure that includes:

- Assessment of risk to individuals and the Council.
- Containment and mitigation measures.
- Reporting obligations to the Information Commissioner's Office (where required).

Reference: Information and Data Protection Policy, Section "Rights of a Data Subject".

13 Training and awareness

Broadclyst 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.

14A. Records Retention and FOI

Freedom of Information and Retention

All records (including emails and electronic files) are subject to the Freedom of Information Act 2000 and may be disclosed if requested. Information must be retained according to the Council's Records Management and Retention Policy. Any uncertainty about disclosure should be referred to the Clerk. Reference: Information and Data Protection Policy, "Making Information Available" section.

15. Policy review and cross-references

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

- Data Protection: Refer to Information & Data Protection Policy
- Media: Refer to Media Communications Policy
- Social Media: Refer to Social Media Policy

16. Contacts

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

16A. Policy Ownership and Review

This Policy is owned by the Clerk as the Responsible Officer. It will be:

- Reviewed annually.
- Version controlled.
- Approved by Council Resolution¹.

Version Control Table:

Version	Date	Approved by	Summary of Changes
1.0	21.07.25	Finance Committee	Initial adoption

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

Date: _____

Signature: _____

Print: _____

(Signed copy held on file)

¹ Or an appropriate committee in line with LGA 1972 s101