

BROADSTONE TOWN COUNCIL

Information Technology (IT)

1. Introduction

Broadstone Town 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 sets out how Broadstone Town Council manages and protects its information technology (IT) systems, electronic communications, and digital data.

It applies to:

- All individuals who use Broadstone Town Council's IT resources including councillors, employees, contractors, and volunteers who use IT systems or devices for council business,
- All council-owned devices, systems, software, and online services, and
- Any personal devices used to access or process council information.

The aim of this policy is to ensure that the council's digital activities are secure, lawful, and transparent, in accordance with the Practitioners' Guide and Assertion 10: Digital and Data Compliance in the Annual Governance Statement.

3. Acceptable use of IT resources and email

Broadstone Town 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

Council-owned equipment (laptops, tablets, printers, etc.) remains the property of the council. Users must not install software or apps without prior authorisation. Equipment must be returned to the council when an individual leaves office or employment. Any loss, theft, or damage must be reported immediately.

5. Data management and security

All sensitive and confidential Broadstone Town 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, internet usage and Social Media

Broadstone Town 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.

The council's official social media accounts are managed by the Proper Officer.

- Councillors should not comment on behalf of the council using personal profiles.
- Posts and comments must be factual, respectful, and non-political.
- Inappropriate or offensive content must be reported to the Clerk for moderation or removal.
- Use of messaging platforms (e.g. WhatsApp, Facebook Messenger) for council business must be limited to administrative coordination and not decision making.

7. Email communication

Email accounts provided by Broadstone Town 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.

- All council business must be conducted through official council email accounts (e.g. firstname.surname@broadstone-tc.gov.uk).

BROADSTONE TOWN COUNCIL

Information Technology (IT)

- Councillors and staff must not use personal email addresses for council work or forward council emails to personal inboxes.
- Passwords must be strong and changed regularly.
- Access to council email accounts will be withdrawn when a councillor or employee leaves their role, and all records must be retained by the council.

8. Password and account security

Broadstone Town 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 provided by Broadstone Town 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

Broadstone Town 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.

- All council devices must have up-to-date antivirus software and system updates installed.
- Two-factor authentication (2FA) should be enabled wherever possible.
- Passwords must be unique to council accounts and not reused across personal accounts.
- Councillors and staff must be alert to phishing emails and avoid opening suspicious links or attachments.
- Any suspected cyber incident must be reported to the Clerk without delay.

13. Training and awareness

Broadstone Town 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. All councillors and staff will receive periodic training on IT security, data protection, and digital governance.

14. Compliance and consequences

Failure to comply with this policy may result in disciplinary action or referral to the Monitoring Officer, depending on the individual's role and the seriousness of the breach.

15. Policy review

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

16. 15. Contacts

For IT related enquiries or assistance, staff and councillors can contact: the Town Clerk on 01202 028480.

For suspected security breaches, staff and councillors can contact: the Town Clerk on 01202 028480.

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