Bingham Town Council Information Technology (IT) Policy

1. Introduction & Scope

Bingham Town Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications. This policy sets out how the Council will use, manage and protect its information technology systems and digital assets.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

This policy applies to all IT resources, including computers, networks, software, devices, data, and email accounts.

This policy should be used alongside the Council’s other adopted policies and procedures, including but not limited to:

- Data Protection Policy
- Data Breach Policy
- General Privacy Notice
- Privacy Notice for Councillors and Staff
- GDPR Compliance Checklist
- Staff Handbook
- Record Retention Policy

2. Roles and Responsibilities

- The **Clerk** is responsible for managing and enforcing this policy, ensuring IT resources are used appropriately and securely.
- **Councillors and staff** are responsible for complying with the policy and reporting any breaches or incidents immediately to the Clerk.
- **External IT support providers and contractors** must adhere to the standards set out in this policy when handling council information.

3. Acceptable use of IT resources and email

IT systems, council issued devices and email accounts are to be used for official council-related activities and tasks. Personal use is discouraged and where permitted must not interfere with work responsibilities or compromise the Council's security or reputation. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

The use of personal email accounts for Council business is prohibited. All Council correspondence must be conducted through official Council email addresses.

Misue of Council owned IT systems or equipment will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.

4. Device and software usage

Where possible, authorised devices, software, and applications will be provided by the council for work-related tasks.

Unauthorised installation of software on authorised Council devices, including personal software, is strictly prohibited due to security concerns.

A record of Council owned Hardware will be reviewed and PAT tested annually and obsolete equipment will be removed from the asset register.

Regular updates and security will be applied and managed by the Council's IT support providers.

Obsolete or faulty equipment must be securely wiped before disposal, and hardware will be securely disposed of by the Council's IT support providers.

5. Mobile devices and remote work

Mobile devices provided by the 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.

Staff and Councillors working remotely must ensure that they use a secure internet connection and do not leave devices unattended in public or shared spaces.

Devices that can access data must be locked when not in use and must not be shared with family members or others.

Staff must not download Council documents onto personal devices unless approved by the Clerk.

6. Data management, confidentiality and security

All sensitive and confidential 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.

All Council devices used to access data must be password-protected. Multi-factor authentication (MFA) should be enabled for cloud-based systems and emails.

Documents containing personal data or sensitive information must be stored securely, in encrypted cloud-based storage. Any transfer of such data must use secure sharing tools.

Staff and Councillors must not disclose confidential Council information to any unauthorised person, either during or after their term of office or employment.

Personal disks, USB stick, CD, DVD or data storage devices must not be used unless with the express permission of the Clerk and only used when data cannot be transferred by another secure measure.

Councillors using personal devices should maintain a clear a separation between the personal data processed on the council's behalf and that processed for their own personal use. If the device supports multiple profiles, a work profile should be used for Council related purposes.

Councillors leaving the Council will be asked to confirm that all identifiable data is deleted and assistance with personal devices will be provided by the Council's IT providers if required.

7. Network and internet usage

The 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.

8. Email communication

Email accounts will be provided by the council and are for official communication only. Emails should be professional, respectful in tone, and must not contain defamatory or offensive material.

Email accounts must include a standard disclaimer regarding data protection.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

9. Email monitoring

The 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.

Monitoring of an employee's email and/or internet use will only be conducted in the council’s legitimate interests and is to ensure that this policy is being complied with.

The Council reserves the right to access email communications on Council devices and email accounts to meet its obligations for freedom of information and subject access requests or in relation to any legal proceedings.

10. Password and account security

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.

Passwords must not be shared, and any breach of account or password security must be reported to the Clerk.

Multi-Factor Authentication (MFA) is enabled for all Council email accounts and on all Council owned devices.

All user accounts must be protected by strong, secure passwords. The council recommends the National Cyber Security Centre (NCSC) recommendations for creating passwords using three random words (e.g. PurpleCandleRiver). This method helps create passwords that are both strong and easy to remember

GDPR compliance checklists are completed by all Councillors prior to data being shared to their Council provided email address. Data will not be shared to personal email accounts.

11. Third-party Access and Security Standards

Any contractors or third-party software providers accessing Council data or systems must adhere to this policy and ensure compliance with the Data Protection Act 2018.

Access will be limited to the data or systems necessary for their role, logged appropriately, and revoked as soon as work is completed.

12. Social Media

Personal use of social media/networking/media are not permitted on Council owned devices. Use of social media on Council owned devices, on behalf of the Council, as part of the individuals position is acceptable and must be authorised by the Clerk.

13. Digital Inclusion and Accessibility

The Council recognises the importance of digital inclusion. Support and training will be offered to Councillors and staff who are less confident using technology. Residents who are digitally excluded will be offered alternative methods of accessing Council information such as paper.

The Council's website and online documents comply with accessibility regulations and offer downloadable content in accessible formats.

14. Disaster Recovery and Backup

Council documents and emails are backed up at least weekly using a secure and encrypted cloud-based service provided by the Council's IT provider. The backup system includes the ability to restore data in the event of accidental deletion or system failure. The Council's IT providers will notify the Clerk of any failed backup procedures.

15. Reporting security incidents

Any data breach, loss of equipment, or suspected cyber incident must be reported immediately to the Clerk, who will investigate and determine whether the breach needs to be reported to the Information Commissioner's Office (ICO).

The Council will follow procedures outlined in its Data Protection Policy and maintain an incident log.

All Councillors and staff must remain vigilant against phishing attempts and other online threats.

Passwords must be changed immediately if a compromise is suspected.

16. Health and Safety

Staff working in council offices with council devices will be provided with an appropriate workstation and a DSE check will be completed for all users.

Eye tests are offered to all staff and councillors using display screen equipment for continuous periods of one hour or more.

If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the Clerk.

17. Training and awareness

The Clerk will provide training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All new councillors will be offered training on email security and best practices.

Staff and Councillors are encouraged to familiarise themselves with National Cyber Security Centre (NCSC) guidance on staying safe online.

18. Compliance and consequences

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

19. 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.

This IT Policy was considered by the Finance, Policy and Resources Committee on 03 March 2026 minute reference 10 and was approved by the Full Council on 17 March 2026, minute reference 7c.

POLICY REVIEW	DATE	MINUTE REF