BRANDON
TOWN COUNCIL

Chairman: Cllr Philip Wittam  Town Clerk: Tina Cunnell

# Brandon Town Council IT Policy

(Assertion 10 – Digital and Data Compliance)

## 1. Introduction

The Parish Council recognises the importance of effective, secure, and compliant use of information technology (IT) in supporting its business, operations, and communications. This policy sets out the council's approach to IT, data protection, email, and website management in line with the Annual Governance and Accountability Return (AGAR) Assertion 10 requirements.

## 2. Scope

This policy applies to all Councillors, employees, volunteers, and contractors who use the council's IT resources, including computers, networks, software, devices, data, and email accounts.

## 3. Authority-Owned Email Accounts

All official council business must be conducted using the council-provided email accounts on an authority-owned domain (e.g. clerk@brandon-tc.gov.uk). Personal or free webmail accounts (e.g. Gmail, Outlook) must not be used for council business. Email accounts must be managed in accordance with the council's data protection and retention policies.

## 4. Acceptable Use of IT Resources

IT resources are to be used for official council-related activities. Limited personal use is permitted if it does not interfere with work or breach this policy. Users must not access, store, or transmit inappropriate, offensive, or illegal material. All users must respect copyright and intellectual property rights.

## 5. Device and Software Security

Only authorised devices and software may be used for council business. Personal devices used for council work must comply with this policy and be secured appropriately. Unauthorised installation of software is prohibited.

## 6. Data Management and Security

All sensitive and confidential council data must be stored and transmitted securely using approved methods. Regular data backups must be performed and tested. Secure data destruction methods must be used when data is no longer required.

Data must be processed in accordance with UK GDPR and the Data Protection Act 2018.

## 7. Website and Accessibility

The council's website must meet the Web Content Accessibility Guidelines (WCAG) 2.2 AA standard and the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018. An accessibility statement must be published and regularly reviewed, including reasons for any non-compliance and contact details for alternative formats. All required documents must be published in line with the Freedom of Information Act 2000 and the Transparency Code for Smaller Authorities.

## 8. Password and Account Security

Users are responsible for maintaining the security of their accounts and passwords. Passwords must be strong, unique, and not shared. Accounts must be disabled promptly when a user leaves the council.

## 9. Mobile Devices and Remote Working

Council-provided mobile devices must be secured with passcodes and/or biometric authentication. Remote working must follow the same security standards as office-based work.

## 10. Email and Internet Use

Council email accounts must be used professionally and only for council business. Users must be vigilant against phishing, malware, and suspicious links or attachments.

## 11. Retention and Archiving

Emails and electronic records must be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails and files.

## 12. Reporting Security Incidents

All suspected security breaches or incidents must be reported immediately to the Clerk or designated IT contact. Prompt action will be taken to investigate and resolve incidents.

## 13. Training and Awareness

The council will provide regular training and resources on IT security, data protection, and best practice. All users must participate in mandatory training.

## 14. Compliance and Consequences

Breaches of this policy may result in suspension of IT privileges and further disciplinary action as appropriate.

## 15. Policy Review

This policy will be reviewed annually and updated as necessary to reflect changes in legislation, technology, and best practice.

## 16. Contacts

For IT or data protection queries, contact: Jackie Prior.

## Adoption and Review

Adopted by Brandon Town Council on: 8th December 2025

Review Date: December 2027

Signed: _____ (Chair)

Signed: _____ (Clerk)

References

- AGAR Practitioners' Guide 2025, Assertion 10, paras 1.47–1.54, 5.117–5.128
- The Good Councillor's Guide to Cyber Security 2025
- Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018
- UK GDPR and Data Protection Act 2018