Bromeswell Parish Council

IT Policy

1. Introduction

- Bromeswell Parish Council (BPC) 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.
- This policy defines how BPC manages its use of IT in line with the Transparency Code for Smaller Authorities (2015) and the 2025 edition of the Practitioners' Guide. It ensures the Council's digital operations are transparent, secure, and compliant with data protection laws.

2. Scope

- This policy applies to all individuals who use BPC's IT resources: Councillors, employees, volunteers, and contractors who access or manage the Council's IT resources. This is including but not limited to:
    - Desktop and laptop computers, tablets and smartphones
    - Email and cloud-based systems
    - Council website, social media, and digital publication tools
    - Video conferencing and messaging platforms
    - Personal devices used under Bring Your Own Device (BYOD) provisions

3. Acceptable use of IT resources and email

- BPC's 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. Governance and Oversight

- The Clerk is the designated Data Protection Officer (DPO) and IT systems operator. All Councillors oversee implementation, security and compliance.

5. Device and software usage

- Where possible, authorised devices, software, and applications will be provided by BPC for work-related tasks.
- Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

6. Data management and security

- All processing of personal data will comply with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.
    - **Privacy Policy:** All data collection, processing, and subject rights are governed by the Council's Legal and Privacy Statement, available on the Council website. All users will familiarise themselves with this.
    - **Access and Storage:** Data is stored securely, with access granted only to authorized personnel based on necessity.
    - **Retention:** Personal data will be retained in accordance with the Council's Data Protection Statement and securely deleted when no longer needed.
- All sensitive and confidential BPC data will be stored and transmitted securely using approved methods. Regular data backups will be performed to prevent data loss.

7. Email Communication

- Email accounts provided by BPC are for official communication only. Emails will be professional and respectful in tone. Confidential or sensitive information will not be sent via email unless it is encrypted.
- BPC will be cautious with attachments and links to avoid phishing and malware and will verify the source before opening any attachments or clicking on links.

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

8. Password and account security

- BPC 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 BPC will be secured with passcodes and/or biometric authentication. When working remotely, users will follow the same security practices as if they were in the office.

- Mobile devices should not be accessed while abroad.

10. Email Monitoring

- BPC 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 2018 and GDPR.

11. Retention and archiving

- Emails will be retained and archived in accordance with legal and regulatory requirements. BPC will regularly review and delete unnecessary emails to maintain an organised inbox.

12. Data Breach Process and Protocols

- All suspected security breaches or incidents should be reported immediately to the Clerk, who is the designated IT point of contact for investigation and resolution. Any breaches or incidents must be reported immediately to minimise risk and comply with UK GDPR requirements.

- A data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include:
    - Loss or theft of devices containing personal data

- Unauthorised access to Council email accounts or files
- Sending personal data to the wrong recipient
- Malware or ransomware attacks compromising Council systems

- Any Councillor, employee, or contractor who becomes aware of a data breach must report it immediately to the Clerk in their role as Data Protection Officer.

- The Clerk will assess the severity and scope of the breach and determine if mitigation steps are required (e.g. changing passwords, disabling access).

- A full investigation will be conducted by the Clerk or designated officer within 72 hours of the breach being discovered.

- The breach will be logged, including:
  - Date and time of breach
  - Type and volume of data affected
  - Cause and extent of the breach
  - Actions taken to address the breach

- If the breach is likely to result in a risk to the rights and freedoms of individuals, the Council must notify the Information Commissioners' Office (ICO) within 72 hours.

- If the breach poses a high risk to the individuals affected, those individuals will also be informed without undue delay, outlining:
  - The nature of the breach
  - Likely consequences
  - Measures taken to mitigate the risk
  - Contact information for further support

- The Clerk will ensure lessons are learned and policies, procedures, or training are updated as necessary. Technical fixes or security upgrades will be prioritised to prevent recurrence.

13. Training and awareness

- BPC 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 training on email security and best practices.

14. Compliance and consequences

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

15. Policy review

- This policy will be reviewed annually, or sooner if legislation changes, to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

16. Contacts

- For IT-related enquiries or assistance, users can contact the Clerk.
- All staff and Councillors are responsible for the safety and security of BPC's IT and email systems. By adhering to this IT Policy, BPC aims to create a secure and efficient IT environment that supports its mission and goals.

This Policy was adopted by the Council at its meeting held on: 23 March 2026

Signed:

Chair Clerk

Version Control

Date	Details	Next Review
V.1	Agreed	March 2027