Birchanger Parish Council

IT and E-mail Policy

Adopted	2nd September 2025
Reviewed	
Date of next review	Autumn 2028

Document history	
July 2025	Version 1.0 policy devised

1. Introduction

Birchanger Parish Council (BPC) recognises that internet, mobile and digital technologies provide positive opportunities and are of particular importance in supporting BPC's business, operations, and communications.

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

2. Scope

This policy applies to all individuals who use BPC's IT resources. This includes computers, software, devices, data, and email accounts.

It is linked to other BPC policies and documents, in particular -

- Subject Access
- Data Breach
- Risk Management

3. Acceptable use of IT resources and email

BPC 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

Authorised devices, software, and applications will be provided by BPC for work-related tasks for the Chair and Clerk.

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

5. Data management and security

All sensitive and confidential BPC 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. Internet usage

internet connections, when using BPC devices, should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

Whilst using BPC devices users must not:
Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent imaging of children actually or apparently under the age of 18 or images of child
  abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring BPC or any individual within it into disrepute e.g. promotion of violence, gambling, libel and/or disrespect

7. Email communication

Council members and employees should use a BPC email account for all official communications to ensure everyone is protected through the traceability. Emails created or received will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted. **Users must not** send emails which are offensive, embarrassing or upsetting to anyone.

It is important to be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

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. 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 and GDPR.

10. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. It is important to regularly review and delete superfluous emails to maintain an organised inbox.

11. Reporting security incidents

All suspected security breaches or incidents should be reported to the designated IT point of contact[1] for investigation and resolution. This includes any email-related security incidents or breaches.

12. Training and awareness

BPC will provide the opportunity for regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive information on email security and best practices[2].

13. Compliance and consequences

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

14. Policy review

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

[1] Ken Wheatley
[2] Via EALC News bulletin