



Brockham Parish Council

IT and Email Policy

Date of Policy: 14th July 2026

Approving Committee: Full Council

Date of Council Meeting: 14th July 2026

Date for Next Review: July 2028

1. Introduction

Brockham Parish Council recognises the importance of effective, secure and responsible use of information technology (IT) and email systems in supporting the Council's operations, communications and statutory responsibilities.

This policy sets out the standards and responsibilities for the appropriate use of IT resources and email by councillors, employees, volunteers and contractors acting on behalf of Brockham Parish Council.

2. Scope

This policy applies to all users of Brockham Parish Council's IT resources, including:

- Computers and laptops
- Mobile devices
- Networks and internet connections
- Software and applications
- Cloud-based services and storage systems
- Data and records
- Council email accounts

The policy applies whether equipment is owned by the Council or used for Council business under approved arrangements.

3. Acceptable Use of IT Resources and Email

Council IT resources and email accounts are provided primarily for Council business.

Limited personal use is permitted provided that it:

- Does not interfere with Council duties.
- Does not incur additional costs for the Council.



- Does not compromise security.
- Does not contravene any Council policy or legal requirement.

Users must:

- Act professionally and responsibly.
- Comply with copyright and intellectual property laws.
- Avoid accessing, viewing, storing or transmitting inappropriate, offensive or unlawful material.
- Use Council systems in a manner that protects the reputation of Brockham Parish Council.

4. Device and Software Usage

Where practical, authorised devices, software and applications will be provided or approved by Brockham Parish Council for Council business.

Users must not:

- Install unauthorised software.
- Alter security settings without approval.
- Use unlicensed software.
- Connect unauthorised devices to Council systems.

Any software required for Council business should be approved by the Clerk before installation.

5. Data Management and Security

All Council information must be handled appropriately and securely.

Users must:

- Store Council information using approved storage locations and systems.
- Protect confidential and personal data in accordance with UK GDPR and the Data Protection Act 2018.
- Share information only with authorised recipients.
- Ensure data is backed up where appropriate.
- Dispose of electronic and physical records securely when no longer required.

6. Network and Internet Usage



Council internet and network facilities must be used responsibly and primarily for Council purposes.

Users must not:

- Download copyrighted material without appropriate permission.
 - Access malicious, illegal or inappropriate websites.
 - Use Council resources for personal commercial activities.
 - Engage in activities that may compromise network security.
-

7. Email Communication

Council email accounts are the official channel for Council business.

Users must:

- Use professional and courteous language.
- Ensure correspondence reflects the standards expected of a public authority.
- Take care when sending personal or confidential data.
- Verify recipients before sending sensitive information.
- Be vigilant regarding phishing emails, suspicious links and attachments.
- Where residents correspondence is being shared, all steps to maintain GDPR are taken.

Confidential or sensitive information should only be transmitted using appropriate security measures.

8. Password and Account Security

Users are responsible for safeguarding their accounts and credentials.

Users must:

- Use strong passwords.
 - Keep passwords confidential.
 - Enable multi-factor authentication (MFA) where available. (This will be worked towards)
 - Report any suspected account compromise immediately.
 - Avoid using the same password across multiple services.
-

9. Mobile Devices and Remote Working



Council-owned and authorised devices used for Council business must be secured by:

- Passwords or PINs.
- Biometric authentication where available.
- Automatic screen locking.

When working remotely, users must maintain the same security standards as when working from Council premises and take reasonable steps to prevent unauthorised access to Council information.

10. Monitoring and Security

Brockham Parish Council reserves the right to monitor the use of its IT systems and email services where necessary:

- To maintain security.
- To investigate suspected misuse.
- To ensure compliance with legal and regulatory obligations.

Any monitoring will be proportionate and undertaken in accordance with data protection legislation.

11. Retention and Archiving

Electronic records and emails must be retained and managed in accordance with:

- The Council's Retention Policy.
- Data protection legislation.
- Legal and audit requirements.

Users should regularly review records and delete information that is no longer required in accordance with approved retention periods.

12. Reporting Security Incidents

Any actual or suspected security incident must be reported immediately to the Clerk.

Examples include:

- Loss or theft of devices.
- Disclosure of confidential information.
- Suspected phishing attacks.



- Malware infections.
- Unauthorised access to Council systems.

Prompt reporting assists in minimising potential risks and ensuring compliance with legal obligations.

13. Training and Awareness

Brockham Parish Council will seek to promote good information security practices through training, guidance and awareness activities.

Councillors and staff are expected to:

- Familiarise themselves with this policy.
- Complete any relevant training provided.
- Keep up to date with emerging security risks and good practice.

14. Compliance and Consequences

Failure to comply with this policy may result in:

- Restriction or withdrawal of access to Council IT systems.
- Investigation by the Council.
- Disciplinary action where appropriate.
- Referral to relevant authorities where legal obligations have been breached.

15. Policy Review

This policy will be reviewed every two years, or sooner if required due to:

- Changes in legislation.
- Changes in technology.
- Identified security risks.
- Changes to Council operations.

16. Contact

For IT-related enquiries, support, or to report a security concern, users should contact:

The Clerk to Brockham Parish Council



Adoption

This IT and Email Policy was adopted by Brockham Parish Council at a meeting of the Full Council held in **July 2026**.

Signed: _____

Chairman

Date: _____

Review Date: July 2028.