11/6/2025

IT Policy

Jane Smith
LATHOM SOUTH PARISH COUNCIL

LATHOM SOUTH PARISH COUNCIL — IT POLICY

Adopted by Lathom South Parish Council 11th June 2025

1. Introduction

This policy sets out the responsible use of IT systems, devices, data, and communication channels by Councillors and employees of Lathom South Parish Council ("the Council"). Its purpose is to:

- Prevent inappropriate use of Council IT resources.
- Protect personal and confidential data.
- Minimise the risk of malware or virus infection.
- Ensure compliance with software licensing laws.
- Promote responsible use of devices, including personal ones used for Council business.
- Support Councillors and employees in delivering services effectively and securely

The policy is intended to be proportionate to the size and structure of the Council and recognises that not all users have access to dedicated Council-owned equipment.

2. Scope

This policy applies to all individuals using the Council's IT resources, including email, data, documents, software, and devices—whether Council-owned or personal (BYOD).

3. Email (Internal and External Use)

3.1. All Councillors and relevant employees will be issued a Council email account, which must be used for Council-related correspondence.

3.2. Email is not inherently secure. Avoid sending sensitive information in the body of an email; use password-protected attachments where appropriate.

3.3. Emails should be treated like paper records: retain those which form part of the official record.

3.4. Avoid forwarding emails without checking the chain for relevance and sensitivity. Consider copying and pasting content rather than forwarding to remove header data.

3.5. Emails relating to Council business—even if sent from a personal account—may be subject to Freedom of Information or subject access requests.

3.6. Do not forward Council emails containing personal or confidential information to personal accounts. However, public information (e.g. road closures, public notices) may be shared with residents, provided no personal data is included.

3.7. Councillors should check their Council email regularly to stay informed.

3.8. Communications should be professional and respectful. Avoid language that could reasonably be interpreted as offensive or misleading. Users are not expected to police common usage, slang, or harmless ambiguity.

3.9. Disseminating material that could reasonably be considered obscene, racist, sexist, or harassing is prohibited.

3.10. The impact of communication on the recipient is what matters; users should exercise care and courtesy in their tone.

3.11. Upon leaving the Council, Councillors and employees must surrender access to Council email accounts and all related content.

4. Use of Equipment (Laptop & Smartphone)

4.1. Devices owned by the Council or used for Council business are subject to this policy.

4.2. When using Council-owned devices;

- 4.2.1. You are responsible for its care and security.
- 4.2.2. Only the assigned Councillor or employee should use Council-provided equipment.
- 4.2.3. Report any hardware or software issues to TBC
- 4.2.4. Council may request return of equipment or data at any time.
- 4.2.5. Do not install unlicensed software or transfer data without checking for viruses.
- 4.2.6. Keep logins secure and do not share them.
- 4.2.7. Confidential information must be protected during use and transfer.
- 4.2.8. Council data should only be used for Council business and not for personal purposes.
- 4.2.9. Good practice includes:
    - Running antivirus software.
    - Using only approved USB or external devices.
    - Avoiding obvious passwords (e.g., birthdays).

- Backing up important data regularly.
- Logging out of devices when unattended

4.3 When using personal devices;

4.3.1. Ensure reasonable precautions are taken—e.g., antivirus software, screen locks, and password protection.

4.3.2 Publicly available information stored on personal devices may be used for Council purposes, provided it does not breach data protection laws.

5. Internet Use

5.1 Posting online is equivalent to publishing.

5.2 Any statements made on forums, websites, or social media platforms that appear defamatory or inappropriate could result in liability for the individual and the Council. Follow the same professional standards online as in email.

6. Social Media

6.1. Only the Clerk or authorised individuals may post to official Council social media accounts.

6.2. Posts must be factual, respectful, and non-political.

6.3. Personal social media accounts should clearly distinguish personal views from official Council positions.

6.4. Campaigning or advocacy on local issues is permitted, but should remain respectful, accurate, and not bring the Council into disrepute.

7. Monitoring

7.1 The Council reserves the right to monitor IT usage to:

- Detect misuse or harassment.
- Protect Council data and equipment.
- Comply with legal obligations.
- Support the well-being and security of Councillors and employees.

7.2 Monitoring will be proportionate and compliant with data protection law. The Clerk may support the process administratively, but oversight rests with the Council, not the Clerk individually.

8. Reporting Security Incidents

8.1 Report suspected breaches or data loss immediately to TBC and Chair of the Council. This includes:

- Lost or stolen devices containing Council data.
- Suspected virus infections or unauthorised access.
- Accidental disclosure of personal information.

9. Acceptable Use Acknowledgment

9.1 All users must confirm they have read and understood this policy by signing an Acceptable Use Statement. This affirms:

- Understanding of responsibilities and legal duties.
- Commitment to responsible IT and data use.
- Awareness of consequences for misuse.

10. Data Classification Guidance

10.1 Users must handle data according to its sensitivity:

- Public: Free to distribute (e.g. meeting agendas, published plans).
- Confidential: Internal working documents, supplier details.
- Personal: Identifiable individual data, protected under UK GDPR.

10.2 Confidential and personal data must not be shared without authorisation and must be stored securely.

11. Bring Your Own Device (BYOD)

11.1 Personal devices may be used for Council business, provided users:

- Maintain basic protections (passwords, antivirus software).

- Avoid storing sensitive Council data unless necessary and encrypted. - however data in the public domain is exempt from this clause.
- Use discretion when transferring or sharing files - password protect if possible, sharing the password via a separate method (e.g. via text message to the recipient).

11.2 The Council will not require separate devices unless risk or legislation demands it.

11.3 BYOD use reflects practical realities and is permitted where sensible precautions are followed.