MUCH HOOLE PARISH COUNCIL

Information Technology (IT) Policy

Approved at the Council's Annual Meeting on 12TH May 2025 for use during year 2025-2026

1. Introduction and purpose

The purpose of this policy is to ensure that all employees, councillors and any third parties using Much Hoole Parish Council information technology (IT) have a clear understanding of what is and is not permitted. This IT Policy sets out the principles and rules governing the use of information technology by Much Hoole Parish Council and applies to:

- The Clerk and Responsible Financial Officer as the sole paid staff member using Council-provided IT equipment,
- All Councillors who access council IT systems or data using their own devices.

The policy ensures IT systems are used securely, lawfully, and in a way that protects Council data and reputation.

2. Definitions

Users – Councillors, employees and third parties acting on behalf of the Council.
Data – digitally stored information including (but not limited to) documents, copyrighted / copyrightable text, images, personal information and accounting information including banking information/access.
IT hardware/software – includes, but is not limited to computers, internet access, remote access connections, email servers, file storage, webmail, smart phones, telephones, website, mobile phones, etc.

3. Scope

This policy covers the use of IT, both hardware and software, for all councillors, employees and third parties acting on behalf of the Council (Users).

4. IT Equipment

This policy applies to:

- Council-provided devices (e.g. laptop and wireless printer used by the Clerk)
- Personal devices used by Councillors for Council duties
- Council email accounts (e.g. @muchhoole-pc.gov.uk),
- The Council's website and services provided by its IT provider, Easy Websites

5. Responsibilities

- **The Clerk** is responsible for maintaining awareness of this policy, overseeing compliance, and liaising with Easy websites on any IT-related issues.
- All users must follow this policy when accessing Council systems or handling Council information.

6. Acceptable Use

- Council IT equipment and services are to be used strictly for Council business.
- Personal use of the Council-issued laptop is not permitted.
- Councillors using personal devices must take reasonable precautions (e.g. antivirus software, strong passwords) to protect all Council data.

7. Passwords and Access

- All devices and accounts must be password protected.

- Passwords should be complex, not shared, and changed if compromised at any point.
- The Council reserves the right to access the Clerk's Council laptop if required (e.g. sickness or emergency) and the Chair retains a sealed envelope with all logins and passwords to be opened in the presence of another Councillor only if absolutely required (e.g. emergency).

8. Monitoring and Security

- The Council will review this policy annually at its May Annual meeting.
- The Council may review IT usage for compliance purposes.
- Emails and digital communications may be subject to legal or public access requests (e.g. under FOI).
- Devices must be locked or shut down when unattended.

7. Data Protection

Where users use their own hardware to access Council systems or data they are responsible for ensuring the security of systems and data as per this policy and the Data Protection Policy.

An email address will be provided to all councillors and Council employees and should be the only address used for official or unofficial Council correspondence.

Personal use is not permitted for any Council communication services, software applications (downloaded or software as a service) or data, unless such data is already in the public domain.

Any correspondence undertaken on behalf of the Council on Council provided or personal devices or services, must be provided upon request to the Clerk or Chair, particularly, but not limited to the case of a Freedom of Information request.

Users must:

- comply with the UK GDPR and the Council's Data Protection Policy.
- Store Council emails only on .gov email addresses.
- not leave their user accounts logged in on an unattended and unlocked device.
- use suitable secure methods for storing and accessing data and services;
- not perform any unauthorised changes to the IT systems. Changes must only be made with agreement from the Chair and at least one other councillor, or at full Council where applicable;
- not attempt to access or use data or software that they are not authorised to use or access;
- not give or transfer Council data or software to any person or organisation outside the Council without the appropriate authority and reason to do so;
- comply with all relevant policies, procedures and UK legislation with respect to the use of IT software. If unsure users should check with the Clerk or Chair.

8. Use of Personal Devices

Councillors are permitted to use their personal devices for Council communications but must:

- Use their official @muchhoole-pc.gov.uk email address for Council business.
- Ensure the device is not shared where access to the Council emails is available.

9. Email and Internet Use

- Council emails must be used in a professional and appropriate manner.
- Abusive, discriminatory, or unlawful content is prohibited.
- Caution should be taken to avoid unintentionally entering into contracts or agreements via email.

10. Software and Downloads

- No unauthorised software may be downloaded on to the Council laptop.

11. Misuse and Disciplinary Action

Misuse of IT systems may result in disciplinary or other action, including:

- Attempting to circumvent security,
- Sharing passwords,
- Loss of Council data,
- Inappropriate or unauthorised use of systems.

12. Risk management relating to Council IT equipment

- As part of its risk management the Council maintains insurance on the equipment provided.
- All equipment must be secured from theft or unauthorised use as far as is practical. When travelling with equipment, it should not be left in an unattended vehicle unless there is no other option, in which case it should be secured out of sight.
- Any loss of, or damage to equipment should be reported as soon as possible to the Clerk and Chair and any criminal damage will be reported to the Police by the Clerk.
- Any loss of personal data as the result of loss or theft of equipment shall be reported to the Clerk and Chair and Information Commissioner's Office (ICO).
- An annual risk assessment should be undertaken regarding use and security of Council IT hardware, software, and stored data.

13. Policy Review

This policy will be reviewed annually at the annual governance meeting or as needed in response to legal or technical developments.