Technology and Communication Policy

Version No.	1.0	Date Ratified	21/10/2025	Review Date	June 2026

The purpose of this policy -

- to ensure the best interests of Mill House are preserved
- to avoid misuse of data
- to the optimise the use of automation within budgeted constraints
- to avoid conflicts of interest
- to protect confidentiality

Objectives -

- to clarify when Committee approval is required
- to clarify limits of delegation to the Manager
- to prevent hacking of internet or external systems
- to prevent unauthorised use of internet or external systems
- to prevent systems to be used for illegal purposes
- to prevent systems being used to bully or harass people
- to ensure confidentiality of staff and Committee emails
- to ensure passwords and pins are handled correctly
- to ensure back up and recovery processes of systems are in place

Preferred Suppliers of Technology -

- the Committee must authorised suppliers of Technology before they are added to the authorised suppliers list
- the Committee will maintain a list of authorised suppliers of Technology
- before adding a new supplier to the list of authorised suppliers, the Committee will consider factors including: reputation, value for money, risks, ongoing support, ongoing costs and if the supplier is prepared to sign a confidentiality agreement when needing access to any of the technology systems (Accounting, Electronic Documents, Emails, Website, Alarm)
- it is a preference to maintain IP rights and ownership of systems developed for Mill House.
- Mill House will retain ownership of the data

The Committee may approve one off purchases of Technology from suppliers not on the authorised list.

Policy Guidelines

1. The Committee is the employer of the Manager/Co-ordinator. This relationship means that some Committee correspondence may be confidential and would be inappropriate for other staff or volunteers and or their partners had access them. It therefore follows that the administration of the email system and file storage needs to remain with the Committee or may be delegated to third party suppliers that do not create a conflict of interest and that are prepared to execute the Confidentiality Agreement.
2. Passwords should be complex, of at least 8 characters, contain upper and lower case, contain at least 1 number and 1 symbol, when permitted. Two factor authentication should use when available.
3. Passwords should never be shared or written down and left in shared areas
    a. An exception is the shared Internet access code and password
4. Communication must not defame people or disclose confidential information to unauthorised people.
5. Systems are not permitted to access illegal material or material that harms people.
6. Systems are not permitted to create illegal material or material that harms people.
7. Screens should be locked when not in use.
8. Computers must be backed up to prevent loss of data, at least monthly, however ideally weekly.
9. Computers must have current comprehensive anti-virus software.
10. Modern technology developments should be considered where there is a clear business case that improve efficiency and are with budget.
11. On going support and costs and training need to be factored into any decisions to implement new technology.
12. No remote access is permitted unless authorised by the Manager or President.
13. Users are required to attend training to avoid scams and prevent hacking.
14. Technology assets must be recorded in the asset register.
    a. Acquisition Date
    b. Description of goods
    c. Cost
15. If Technology is loaned out, this must be recorded in the loan register
    a. Date
    b. Full name of person
    c. Description of goods
    d. Return date