



IT Policy

Document Control:

Version	Date Written	Authors	Date Ratified	Judgement of controls/Amendments
Draft V.0.1	05/12/2024	L. Gleed & S. Bear		
Draft V.0.2	21/01/2025	S.Bear	12.03.25	Check password change info with Lucas given suggestion on training.
Draft V.0.3	01/03/2026	S.Bear	11.03.26	Amended 01.06.26 to reflect individual responsibility for deleting data as per data retention schedule. KB
Date of Review:		1 year or sooner if required.		

Table of Contents

1. Purpose	2
2. Scope.....	2
3. Roles and Responsibilities	2
4. Acceptable Use of IT Resources	2
5. Data Protection and Privacy.....	3
6. Passwords and Access Control.....	3
7. Device Management.....	4
8. Internet and Email Use.....	5
9. Cybersecurity.....	6
10. Remote Working.....	6
11. Incident Reporting	6
12. Policy Enforcement and Consequences	7
13. Policy Review.....	7

1. Purpose

This IT policy outlines the standards and guidelines for the acceptable use and security of IT resources, data, and systems within Wiltshire Treehouse. Its purpose is to ensure that all technology resources are used responsibly, data is protected, and the organisation's mission is supported securely and efficiently.

2. Scope

This policy applies to all employees, volunteers, contractors, and anyone who has access to Wiltshire Treehouse's IT resources, including computers, mobile devices, software, internet, network, and data. This policy should be used in conjunction with the AI policy.

3. Roles and Responsibilities

- **IT Administrator/Manager:** Manages IT resources, enforces this policy, and ensures data security.
- **Employees and Volunteers:** Understand and comply with this policy, report any incidents, and ensure responsible use of IT resources.
- **Board of Trustees:** Oversees the policy and ensures it aligns with the organisation's mission and legal requirements.
- **All users:** It is the responsibility of all employees, Trustees, Volunteers and contractors to follow policy. This includes securely destroying in a timely manner any Wiltshire Treehouse data held upon their devices. All data should be held and destroyed in accordance with the charities data retention schedule.

4. Acceptable Use of IT Resources

All users must use IT resources in a manner that supports Wiltshire Treehouse's goals and maintains the security and integrity of our data. The following guidelines apply:

I. Permissible Use: IT resources should be used for organisational activities. Limited personal use is permitted, provided it does not interfere with duties or consume excessive resources.

II. Prohibited Use

- a. Accessing, creating, or distributing offensive or inappropriate content.
- b. Engaging in activities that could harm the organisation's reputation.
- c. Conducting personal business or political activities.
- d. Using unauthorised applications or services that could compromise security.

5. Data Protection and Privacy

Wiltshire Treehouse is committed to safeguarding data in compliance with data protection regulations (e.g., GDPR). This policy ensures that all personal, sensitive, and organisational data is processed lawfully, securely, and transparently.

Wiltshire Treehouse best practice is to store all data within Microsoft SharePoint system; any downloaded information should be regularly reviewed and deleted after use - this includes emails including attachments. It is the responsibility of all employees, Trustees, Volunteers and contractors to securely destroy in a timely manner any Wiltshire Treehouse data held upon their devices. All data should be held and destroyed in accordance with the charities data retention schedule.

I. Data Collection and Storage:

- a. Collect only necessary data for the organisation's operations.
- b. Store personal and sensitive data securely using encryption, passwords, or other appropriate methods.

II. Data Access and Sharing:

- a. Only authorised personnel can access or share data.
- b. When sharing data, ensure compliance with relevant data protection laws.
- c. All sensitive data must be accessed via a Wiltshire Treehouse Microsoft 365 portal/account. This applies to staff, Trustees and volunteers.
- d. Where sensitive data must be shared outside of the organisation, e.g. for safeguarding concerns – ensure the data being provided is password protected (Password to be shared via a separate means of communication/email).
- e. Any documents that are downloaded must be deleted into the recycle bin and then the recycle bin emptied when no longer in use. All documents should be stored on the shared drive.

III. Data Retention and Disposal:

- f. Retain data only as long as required by law or organisational need.
- g. Securely delete data that is no longer needed.

6. Passwords and Access Control

I. Password Standards: In order to keep data stored on all devices safe the following standards must be adhered to. All users must:

- Set strong passwords and avoid reusing passwords across different accounts. Best practice is to use 3 words plus additional numbers (not replacing letters with numbers) and special characters. Passwords should meet the following criteria:
 - a. At least 12 characters in length and include letters, numbers, and special characters.
 - b. Changed every 90 Days.
 - c. Unique pin/password to gain access across devices and platforms.
- Have 2 factor authentication set up where offered the opportunity to do so. This is commonly a password plus a code sent by text or email.
- Have 2 layers of security to gain access to data (e.g. one password to unlock device, a separate password to unlock One Drive and Outlook app). Note: for this purpose, emails should be accessed via the Outlook app, not via the phone's built in email facility
- Have 'find my device' function set up that enables us to find, lock and erase a lost device

II. Access Control:

- User access is granted based on role and job requirements.
- Wiltshire Treehouse will regularly review access rights to ensure appropriate levels of access.

7. Device Management – Staff/volunteers/Trustees.

I. Use of Charity-owned Devices:

- Use Wiltshire Treehouse-owned devices only for official purposes.
- Report lost or stolen devices immediately to your line manager, copying in admin@wiltshiretreehouse.org.uk so that all actions to reduce the leak of sensitive data can be made.
- Ensure devices used for charity work meet security standards (e.g., updated OS, password-protected, antivirus).
- Use of Intune can support with password management where needed.

II. Personal Devices (BYOD):

- When using personal devices to access organisational data, install security software and follow data protection guidelines. Wiltshire Treehouse recommend McAfee as their preferred standard of security software.
- Ensure the firewall is turned on and that you are accessing the internet through a secure medium. This could be your home internet connection that is password protected or a mobile device providing a hotspot via 4G/5G.
- Ensure personal devices used for charity work meet the recommended security standards. E.g. update operating systems, password-protected, antivirus software installed and updated and 2-

factor authentication where available. Personal devices no longer supported by the manufacturer **must not** be used for charity purposes. If a device is a necessity to your role, please discuss this with your line manager immediately.

III. Agreed Security Standards for Devices:

These standards apply to both devices owned by Wiltshire Treehouse and any personal devices used for work purposes. It is the responsibility of the staff/volunteer/Trustee to maintain the following:

- Devices must remain maintained/supported by the manufacturer – Devices can be checked here:
- **Apple:** <https://www.compareandrecycle.co.uk/blog/how-long-will-my-iphone-be-supported#:~:text=Is%20My%20iPhone%20Supported%3F>
- **Android:** <https://www.howtogeek.com/797200/how-long-will-my-android-phone-be-supported-with-updates/>
- Latest versions of security software (McAfee) **must** be installed and updated within 5 working days of the new release.
- Devices **must** use the most up to date web browser – this is to ensure the highest level of cyber security available to the charity. Automatic updates for web browsers should be turned on. Wiltshire Treehouse **recommended web browsers are Edge and Chromium.**
- 2-factor authentication should be used where available for all devices and software.

IV. Device Management – Organisational responsibilities

- A hardware replacement schedule will be set and maintained by the charity. Devices must be replaced before the expiration of their support by manufacturer.
- New hardware will be set up initially by the charity administrator, then signed out to staff/volunteers/Trustees by their line manager/administrator. New hardware must be signed for and the asset number/serial number recorded against the asset register by the administrator. Once signed for, the item remains the responsibility of the named individual.
- Old hardware will be returned to the charity administrator, where the hard drive will be wiped clean, logged on the inventory and asset register, and device(s) no longer used/maintained will be taken to Curry's for secure recycling.

8. Internet and Email Use

I. Internet Use: Internet resources should be used primarily for organisational purposes. Avoid accessing sites that could pose a security risk.

II. Email Use:

- Use organisational email accounts for all charity-related communications.

- Avoid clicking on suspicious links or attachments in emails. Report any suspicious links or Phishing attempts to admin@wiltshiretreehouse.org.uk as soon as possible – however, **do not forward the email**.

9. Cybersecurity

I. Antivirus and Malware Protection: All devices must have updated antivirus software to protect against malware.

II. Security Updates: Regularly update software, applications, and operating systems to the latest versions to mitigate security risks.

III. Phishing Awareness: Be cautious of phishing attempts. Do not share personal or sensitive information in response to unsolicited emails, phone calls, or messages.

IV. Training – All staff, Trustees and Volunteers that use devices for work purposes must complete a basic introduction into cybersecurity. This must be completed as part of your induction.

<https://www.ncsc.gov.uk/training/v4/Small+organisations/Web+package/content/index.html#/>

10. Remote Working

When working remotely, employees and volunteers must:

- a) Ensure a secure internet connection using mobile data. Provided devices should come with ample data allowance. However, please discuss this with your line manager if you are notified of exceeding this.
- b) **Do not use public Wi-Fi for accessing sensitive information.**
- c) Store organisational data only on approved platforms; Microsoft 365 and **do not download sensitive data to any personal devices**. For support in using MS365 most effectively please see your line manager.

11. Incident Reporting

I. Data Breach: Report any suspected data breach to your line manager who will then pass this onto the relevant support parties. Follow established procedures to contain, investigate, and mitigate the breach.

II. Guidance on phishing email response:

a. Immediately change all passwords for your devices – this will be both laptop/phone and any other devices you use to access work. Also change the password for your Wiltshire Treehouse Email. You can access the password changing element using this link:

<https://passwordreset.microsoftonline.com/passwordreset>

b. Forward the email to National Cyber Security Centre - **report@phishing.gov.uk**

c. Report this incident to your line manager and copy in admin@wiltshiretreehouse.org.uk

Guidance on Email sent with personal attachments to the wrong recipient:

- If an internal email – recall the email with immediate effect.
- For external emails - send an email request for the incorrect recipient to delete the previous email without reading.

Technical Incidents:

Report any issues with devices, software, or network access to your line manager as soon as possible.

12. Policy Enforcement and Consequences

- Violation of this policy may result in disciplinary action, including access restrictions, suspension, or termination of roles and access privileges.
- Severe breaches may also lead to legal action where necessary.

13. Policy Review

This policy will be reviewed annually, or as needed, to ensure compliance with legal and regulatory requirements and alignment with Wiltshire Treehouse's mission and needs.

Acknowledgement

By accessing Wiltshire Treehouse's IT resources, you agree to follow this policy and understand that any violation may result in disciplinary action.
