The Shrublands Trust

Information Security and Social Media Policy

This policy aims to set out the processes and procedures that must adhered to by all trustees and volunteers of The Shrublands Trust in relation to the use of trust computer facilities and the actions and precautions that are to be taken to ensure the confidentiality and security of both client and trust data. In addition it is the responsibility of all trustees and volunteers to ensure the prevention of unauthorised access, disclosure or deletion of trust or client data in whatever format it is stored and held by The Shrublands Trust.

1.) **Confidentiality**
All trustees and volunteers of The Shrublands Trust have a duty to protect information/data from breaches, unauthorised disclosures, unauthorised viewing and to ensure the integrity of the information/data by not allowing it to be modified or deleted whether maliciously or accidentally.

2.) **Availability**
To maintain the availability and integrity of the trust and client information/data it is essential that it is protected from cyber-attacks, destruction, disruption and denial of service. In addition information security also relates to the protection of The Shrublands Trust reputation should any of these principles are breached.

"Information/data" can be held in digital form, but also covers information/data held in printed form and hand-written. It is The Shrublands Trust policy to ensure that the use of documents, computers, mobile computing, mobile communications, portable storage devices, mail, voice mail, voice communications in general, multimedia, postal services must be controlled to prevent unauthorised use and to reduce security risks.

3.) **Social Media**
Social media is the term used for internet-based applications and web sites which help people keep in touch and enable them to interact. It allows people to share information, ideas and views.
Social media can affect communications amongst volunteers, donors and clients; how organisations promote and control their reputation; and how colleagues treat one another. Misuse of Information Technology (IT) and social media can create issues such as, defamation, loss of reputation, cyber-bullying, freedom of speech and the invasion of privacy.

4.) **Legal Considerations**
The Human Rights Act 1998 Article 8 gives a 'right to respect for private and family life, home and correspondence'. Case law suggests that employees have a reasonable expectation of privacy in the workplace.
General Data Protection Regulations (GDPR) May 2018 which describes how organisations must collect, handle and store personal information.
The Regulation of Investigatory Powers Act 2000 covers the extent to which organisations can use covert surveillance.
Computer Misuse Act 1990 made it an offence to access any computer to which a person does not have an authorised right to use. The Act introduced three criminal offences:
Unauthorised access to computer material.
Unauthorised access with intent to commit or facilitate commission of further offences.
Unauthorised modification of computer material

5.) **IT Support Roles and Responsibilities**
The trustees of The Shrublands Trust have responsibility for the overall management of information security, together with the day-to-day management by the trust manager, who should ensure that all volunteers understand, implement and maintain the security objectives set out in this policy.

6.) **Trustees and Volunteers Responsibilities**
Information Security is the responsibility of all trustees and volunteers, who are expected at all times to act in a professional and responsible manner whilst conducting The Shrublands Trust business. All trustees and volunteers have a responsibility not to compromise The Shrublands Trust, e.g. by sending defamatory or harassing electronic mail, or by making unauthorised purchases, and must also be aware that the confidentiality and integrity of information transmitted by email may not be guaranteed.
Access by trustees and volunteers to the Internet via computing facilities provided by The Shrublands Trust is restricted to trust use only.

Trustees and volunteers granted access to The Shrublands Trust information systems must keep passwords private and changed if it is thought they have been compromised in any way. Trustees and volunteers should ensure that they understand their role and responsibilities, and that failure to comply with this policy may result in the withdrawal of access rights and/or disciplinary action.

7.) **Securing Data**
Whenever possible The Shrublands Trust will utilise “cloud” based resources and rely on the provider of those resources to guarantee industry-wide best practice on the reliability and frequency of their data backup and recovery procedures.

8.) **Backing up digital information**
Any other computer-based data which is not be being supported by the cloud based storage, will be backed up at least once a week, on either a USB memory stick, a separate drive or a separate computer to mitigate the loss of data. Ideally backup copies of data will be held off-site. Access to essential data will only be available to those trustees and volunteers which require access in the running of The Shrublands Trust activities.

9.) **Lost or stolen devices**
If possible, remotely lock access to the device, to prevent other people using it remotely and erase the data stored on the device. Retrieve and restore a back-up copy of the data stored on the lost or stolen device.

10.) **Protection from Malware**
Install and activate antivirus software on all trust computers, laptops and tablets.
The Shrublands Trust volunteers undertaking business on behalf of the trust are not allowed to connect to the Internet using unknown or unsecured Wi-Fi hotspots, unless using an installed Virtual Private Network (VPN).

In order to protect against malware (i.e. malicious software or web content that can harm the charity, usually through the deployment of viruses that infect legitimate software), the following steps should be followed to prevent the download or installation of any unauthorised software applications from unknown vendors sources.

Third party applications downloaded onto The Shrublands Trust computers must be approved by the Board of Trustees and only downloaded from manufacturer-approved stores, such as Google Play or Apple Store.

11.) **Online Representatives**
Just as with traditional media, The Shrublands Trust have an opportunity and a responsibility to effectively manage The Shrublands Trust reputation online and to selectively engage and participate in social media. The following principles guide how authorised spokespeople should represent The Shrublands Trust in an online, official capacity when they are speaking on behalf of The Shrublands Trust.

Those posting on behalf of The Shrublands Trust must follow the Code of Conduct and all other trust policies, i.e. as a representative of The Shrublands Trust they must act with honesty and integrity in all matters. Be mindful that they are representing The Shrublands Trust as an official representative, it is important that all posts be respectful of all individuals in accordance with the Equality and Diversity policy and associated legislation.

12.) **Keeping records**
It is important that online representatives keep records of their interactions in the online social media space and monitor the activities of those with whom they engage. Because online conversations are often fleeting and immediate, it is important to keep track of them when officially representing The Shrublands Trust. Representatives must be aware that The Shrublands Trust online statements can be held to the same legal standards as traditional media communications, when in doubt, do not post.

Trustees and volunteers are personally responsible for their words and actions, wherever they are. Online spokespeople must ensure that their posts and emails are completely accurate and not misleading, and that they do not reveal non-public information of The Shrublands Trust.

Representatives must not use the copyrights, trademarks, publicity rights, or other rights of others without the necessary permissions of the rights-holder(s).
The Shrublands Trust copyright: any content generated by or on behalf of The Shrublands Trust will remain the copyright or The Shrublands Trust.

Equality and Diversity
Monitoring and Compliance - The Shrublands Trust is committed to ensuring that the way it provides services to the public and the way volunteers are treated reflects their individual needs and does not discriminate against individuals or groups on any grounds. This policy has been appropriately assessed. The Shrublands Trust will maintain effective monitoring systems to ensure implementation of this policy.

Further security guidance is contained in the National Cyber Security Centre ‘Cyber Security for Charities’ handbook which is available at https://www.ncsc.gov.uk/files/Charity-Guide-v3.pdf. The following infographic summarises the guidance contained in the guide.

Approved: 13/12/2023

Reviewed: 13/12/2024
Review Date: 13/12/2025

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Charity Guide

This advice has been produced to help charities protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/charity** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

Identify what needs to be backed up. Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.

Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.

Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

Switch on PIN/password protection/fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be **tracked**, **remotely wiped** or **remotely locked**.

Keep your **devices** (and all **installed apps**) **up to date**, using the '**automatically update**' option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

Use antivirus software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.

Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.

Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.

Scan for malware and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).

Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/ PIN protection** or **fingerprint recognition** for mobile devices.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.

Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

Do not enforce regular password changes; they only need to be changed when you suspect a compromise.

Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

For more information go to www.ncsc.gov.uk @ncsc

The Shrublands Trust
7 Broom Road, Croydon CR0 8NG
Charity number: 1093186