SP-UK

SUICIDE PREVENTION UK

Suicide Prevention UK

Charity Device and Acceptable Use Policy

2024

Introduction and Purpose

In today's IT-driven world, with devices on almost every desk, virtually all staff can surf the internet and use email.

Few organisations, however, appreciate the potential problems this can bring.

This policy aims to protect the Charity's technological assets from misuse and security threats such as malware and breaches, ensuring that these resources are used safely, ethically, and legally.

The purpose of having these controls in place is to minimise the risk of:

- Unintentional sharing of organisational, personal, or sensitive personal information.
- Data breaches of any of the systems or networks.
- Breaking the law.
- Reputational damage.

Scope

This policy applies to all Suicide Prevention UK (SPUK) staff (including employees, trustees, volunteers and any other individual working for or on our behalf) who have access to Charity devices.

All equipment and information owned and controlled by us fall within the scope of this policy (including all information systems, hardware, software, channels of communication, social media, email, and internet use).

Staff Responsibilities

All staff are required to read and abide by this policy.

Staff are also expected to read our other policies related to acceptable use. These include but are not limited to our:

- Social Media Policy
- Confidentiality Policy
- GDPR Policy

Policy

User IDs and Passwords

Staff must:

- Protect usernames and passwords appropriately.
- Create secure passwords that are not stored in shared folders or written down.
- Not log on to any Charity device or systems using another user's credentials.

Device Security

Staff must:

- Lock the screen when temporarily leaving devices that are in use.
- Log out of all computer devices at the end of the shift.
- Ensure that portable devices are not left unattended or in a vulnerable position.
- Be careful when downloading files or clicking on links. Downloading certain content may enable viruses to attack the device and infiltrate all data stored on it. Remember: Think before clicking on unknown links or engaging with 'pop up' boxes on sites.
- Not remove or disable Antivirus or other security software.
- Ensure that updates and security patches are installed in a timely manner.

Remote Working

Staff must:

- Ensure that devices are kept in a secure place. Devices must not be left in vehicles overnight.
- Ensure that care and attention are paid when home or remote working, including securing devices, particularly when left unattended.
- Not let others (including family members) use their devices.
- Be careful of who can see their device screen. Screens should only be accessible by staff members, particularly when viewing personal, sensitive or confidential information.
- Not use open/unsecured Wi-Fi locations or hotspots when accessing information or systems.

Internet Use

Internet use is permitted where it relates to the staff member's role. Therefore, we encourage our staff to use the internet whenever such use supports the Charity's goals and objectives.

However, the following are not permitted:

- Personal browsing.
- Accessing and/or downloading inappropriate content and/or visiting sites that are obscene, indecent or advocate criminal activity.
- Attempting to bypass our web filters.

In addition, users must not:

- Place any information on the internet related to SPUK, alter any information about the Charity or express any opinion about it unless authorised to do so by the trustees.
- Make official commitments through the internet or email on behalf of SPUK unless authorised to do so by the trustees.
- Share any personal, sensitive or confidential data related to SPUK, its staff or stakeholders on the internet unless authorised to do so by the trustees.
- Use the internet for bullying or harassment.
- Use the internet or email to make personal gains or conduct personal business during working hours (whether using our devices or personal devices).
- Use the internet to gamble during working hours (whether using our devices or personal devices).
- In any way infringe any copyright, database rights, trademarks, or other intellectual property.
- Use the internet to download or install unauthorised personal software, games, or other multimedia to our devices.
- Open attachments that they suspect contain viruses or malware or knowingly install any virus, Trojan, keylogger or other harmful software onto our devices.
- Use our devices or the internet to participate in Distributed Denial of Service (DDoS) attacks or any other illegal activity related to overloading networks or other cybercrimes.

Email Use

Only users who have been authorised to use email at SPUK may do so.

Email Security

Used inappropriately, email can be a source of security issues for any organisation.

Users of the Charity's email system must not:

- Open email attachments from unknown sources (they may contain a virus, Trojans, spyware or other malware).
- Disable email security software.
- Send confidential data via email unless it is encrypted.
- Access another user's email account.

Any user who receives an email they consider to be potentially harmful or otherwise notices that this section has been breached should immediately report this to a trustee.

Inappropriate Email Content and Use

Our email system must not be used to send or store inappropriate content or materials. Staff must understand that viewing or distributing inappropriate content via email is not acceptable under any circumstances.

Users must not:

- Write or send emails that might be defamatory or incur liability for SPUK.
- Send messages or material that could damage our image or reputation.
- Create or distribute any inappropriate content or material via email. Inappropriate content includes but is not limited to:
    - Pornography.
    - Discriminatory content or material that could reasonably offend someone based on a characteristic protected by law.
    - Information encouraging criminal skills, violence, or terrorism.
    - Materials to promote political ideologies.
    - Materials relating to cults, gambling, or other inappropriate subjects.
- Use email for any illegal or criminal activities.
- Send bullying or harassing emails to others.

Any user who receives an email they consider to be inappropriate should immediately report this to a trustee.

Copyright

Users may not use the Charity's email system to share any copyrighted software, media or materials owned by third parties unless permitted by that third party or to perform any tasks that may involve a breach of copyright law.

Users should keep in mind that the copyright on letters, files, and other documents attached to emails may be owned by the email sender or by a third party. Forwarding such emails to other people may breach this copyright.

Email Disclaimers

The standard SPUK email template should be used when sending emails.

Email Marketing and Bulk Email

All email marketing campaigns must be authorised by the trustees before being shared.

Email Etiquette

Although a relatively informal medium, staff should be aware that each email they send does affect our image and reputation and can be a waste of time and resources.

Therefore, staff must:

- Not forward on chain emails or 'humourous' messages. These clog up people's inboxes and may be inappropriate for the workplace.
- Always use a meaningful subject line rather than leaving it blank or using a single word like 'hello'.
- Only use the 'important message' setting sparingly for messages that are actually important and time-sensitive.
- Not use **ALL CAPITAL LETTERS** or bold text, as this can be perceived as impolite and potentially aggressive.
- Be sparing with group messages, only adding recipients who will find the message genuinely relevant and useful. It is rarely necessary to 'reply all'.
- Think before sending an email:
    - Is it better to have a telephone or face-to-face discussion?
    - Is this the best way to send a document for comment? (Sharing documents via email may lead to multiple copies being available within the system and a lack of order to suggestions or comments.)
- Use the 'CC' (carbon copy) field sparingly. If someone needs to receive a message, they should be included in the 'to' field.
- Maintain their inboxes, ensuring that emails that are no longer required are archived or deleted, especially large emails or those with attachments.

Phone Use, Video Calls and Voicemail

Sensitive information must not be discussed/confirmed over the telephone or on a video call unless the identity of the person on the telephone is confirmed and they have a legitimate right to know the information being communicated.

Staff should take care when discussing sensitive information over the telephone or on a video call; it is easy to be overheard.

No answerphone or voicemail messages are to be left that contain sensitive information. Staff should simply request a callback if they cannot reach the person they need to speak with.

Privacy

Staff should be aware that SPUK has the right to:

- Monitor internet usage and communications on Charity devices and systems.
- Monitor SPUK Wi-Fi usage (whilst we have filters on our Wi-Fi to prevent access to certain websites, we may still collect data on searches and activity).
- Monitor usage of Charity devices (this includes being able to remotely access devices at any time).

Therefore, staff should not consider that their use of Charity devices, software, communication systems, or Wi-Fi is private.

SPUK may retain information that it has gathered on the above for a period of one year.

Non-Compliance

Failure to adhere to this policy may result in disciplinary action, including termination of employment or ending a volunteering or contracting agreement.

In addition, breaches may constitute a criminal offence, which will be reported to the appropriate authorities.

Monitoring and Reviewing

This policy should be reviewed periodically to ensure it remains compliant with current legislation, meets best practices, and is not discriminatory.

Policy Date: November 2020

Review Date: April 2024

Next Review: April 2025

Dated and Signed by the Chair and Founder of Suicide Prevention UK: