



SP-UK

SUICIDE PREVENTION UK

Suicide Prevention UK

Social Media Policy

2024

Introduction and Purpose

At Suicide Prevention UK (SPUK), we recognise the benefits of social media.

However, if used unwisely, social media may expose us to reputational damage, breaches of confidentiality, legal issues, and a negative impact on workplace relationships.

This policy is intended to help our team members make appropriate decisions about the use of social media such as blogs, wikis, social networking sites, podcasts, forums, message boards, etc.

Scope

This policy applies to all team members of SPUK and applies to the use of the Charity's social media and the use of personal social media where it relates to SPUK.

Definitions

For the purposes of this policy, **social media** is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. Current examples include X (formerly known as Twitter), Facebook, YouTube, Instagram, TikTok, LinkedIn, etc.

This policy also includes the use of Internet message boards, chat rooms, podcasts, blogs, and any other social media platform not named above.

Policy

General Standards

Overarching Principles

Team members must not, in any way, breach this policy when posting to social media. This includes:

- Posting anything that other team members or the users of our services, Charity partners, donors or other stakeholders would find offensive, including discriminatory comments, insults or obscenities.
- Posting anything that is derogatory or defamatory about other team members or the users of our services, Charity partners, donors or other stakeholders.
- Posting anything which breaks the law in relation to data and information security. For example, revealing personal and sensitive information without a lawful basis.
- Posting confidential information relating to the Charity.
- Posting anything which may infringe on copyright or the intellectual property of others.
- Posting anything that may otherwise harm SPUK or our stakeholders, even indirectly.

SPUK Account Usage

- Only Trustees are permitted to post anything anywhere on our behalf.
- Only Trustees are permitted to update or post on our website and social media accounts.
- Trustees will receive training before being allowed to post on our behalf or on our website or social media accounts.
- Passwords to our social media accounts must be kept secure at all times and never be shared.
- Posters who post spam, abusive or otherwise inappropriate content to SPUK social media accounts will be blocked from further posting.
- Team members may be invited to 'like' and/or 'share' SPUK posts from time to time. This is not mandatory.

Personal Usage

- Team members should be aware that when using Charity devices or Wi-Fi to access their personal social media, they must not expect total privacy (see below).
- Team members may only use our logo or post any of our proprietary information with prior written permission from our Trustees.
- Team members should use personal email addresses to register their accounts and not SPUK email addresses.
- When posting:
 - Be mindful of what you are posting:
 - Don't post images of other team members, users of our services, or stakeholders without our express permission (not everyone wants their photos posted online!).
 - Think twice before putting something live, and consider whether it will harm your reputation or the reputation of SPUK.
 - If disclosed in your profile that you are linked with SPUK:
 - State that your views do not represent those of SPUK. For example, "All views posted are my own and do not represent the views of Suicide Prevention UK".
 - Ensure that posts are consistent with the Charity's image. (Remember, team members, donors, potential donors, users of our service and other stakeholders may be able to see what you post!)
- Team members who are contacted via social media for comment about the Charity for publication anywhere, including in any social media outlet, should always direct the request to a manager or Trustee and must not respond to any such request without written approval.

Key Points to Remember

- Even 'private' conversations and posts are potentially damaging and may constitute a breach of our policy and/or the law. Do not assume that because you have high-security settings, your posts are private!
- The internet never forgets! Everything published will be visible to the world for a very long time and can be shared beyond our control.
- If unsure about whether to post something, seek clarification from management.

IT and Data Security

SPUK has the right to monitor internet usage and communications on work devices and systems and will do so at all times to ensure the security of the Charity's systems.

Therefore, team members should have no expectation of privacy when using Charity devices, software or Wi-Fi.

We may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice.

Team members should also be aware of cyber attacks and social engineering scams using social media and should be careful when clicking on links, accepting 'friend requests' from unknown people, sharing too much information, etc.

Reporting Breaches

Team members should immediately report the following to a manager or Trustee:

- Any comments/posts/blogs, etc., referring to SPUK that they feel need to be looked into. This may include, but is not limited to, confidential information being shared or defamatory comments about SPUK, our team members or stakeholders.
- Unauthorised use of the SPUK social media accounts.

Non-Compliance

Any employee who breaches this policy may be subject to disciplinary action up to and including dismissal.

Any non-employee who breaches this policy may be subject to termination of contract or working/volunteering agreement as relevant.

Team members may also be subject to criminal prosecution depending on the nature of the breach.

Monitoring and Reviewing

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

Where evidence or trends indicate that our culture, policy, procedures, or workforce require intervention, an action plan will be initiated.

Policy Date: June 2024

Review Date: June 2025

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