E-Safety Policy

SURVIVORSUK
male rape and sexual abuse

Contents

Introduction
What digital and social media do SurvivorsUK use?
1. Digital and social media use for trustees, paid staff & volunteers
    1.1 Policy statement
    1.2 Who is covered by the policy
    1.3 The scope of the policy
2. Basic principles
3. General policies and procedures
4. Specific protective guidelines for trustees, paid staff and volunteers
5. Rules for use of social media
6. Passwords
7. Email and SMS (texts)
8. Publishing service-users' images and names
9. Staff use of digital and social media at work
10. Monitoring use of social media websites and moderation rules
11. Comment and post moderation
12. Responsibility for implementation of the policy

Introduction

Purpose
We need to ensure that **SurvivorsUK** is using digital and social media in safe, appropriate, inclusive and creative ways.

Scope
Service-users, trustees, paid staff and volunteers, technical advisors and digital visitors - all who are using digital social media at or via **SurvivorsUK** are subject to the guidance provided in this policy.

Authority
This document has been adopted by the **SurvivorsUK** Board of Trustees.

What digital and social media do SurvivorsUK use?

Website
Our *address* is **https://www.survivorsuk.org/**

Facebook
Profile page called **https://www.facebook.com/agnesesurvivorsuk**
Like page called **https://www.facebook.com/SurvivorsUK/**

Twitter
Our username *(profile page) is* **@SurvivorsUK**

YouTube
Our *profile page* is called **https://www.youtube.com/SurvivorsUK**

LinkedIn
Profile page called **https://www.linkedin.com/in/survivorsuk**
Company page called **https://www.linkedin.com/company/survivorsuk**

Pinterest
Our *profile page* is called **www.pinterest.com/survivorsuk**

Instagram
Our username *(profile page) is* **SurvivorsUKcharity**

Tumblr
Our *profile page* is called **www.survivorsuk.tumblr.com**

1.

Digital and social media use for trustees, paid staff & volunteers

1.1 Policy statement

- This policy is intended to help staff make appropriate decisions about the use of social media such as blogs, wikis, social networking websites, podcasts, forums, message boards, or comments on web-articles, such as Twitter, Facebook, Instagram, YouTube, LinkedIn or any other social media platform that SurvivorsUK may choose to enter and participate within.

- This policy outlines the standards we require staff to observe when using social media, the circumstances in which we will monitor your use of social media and the action we will take in respect of breaches of this policy.

- This policy does not form part of any contract of employment and it may be amended at any time.

1.2 Who is covered by the policy

- This policy covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as **staff** in this policy).

1.3 The scope of the policy

- All staff are expected to comply with this policy at all times to protect the privacy, confidentiality, and interests of our charity and our services, employees, partners and clients.

- Breach of this policy may be dealt with under disciplinary procedures outlined in our Employee Handbook and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

2.

Basic principles

All staff must keep a professional distance online, just as they would in the offline world. Compared with a conversation in the offline real world, technology increases the potential for messages to be taken out of context, misinterpreted or forwarded to others.

All staff must bear in mind that once they place something in the public domain, it is there permanently for people to access, change and share it with others.

The Key principles in digital and social media use are the same as in any professional interaction:

- All staff working with service-users should reflect the positive messages they give service-users through their public behaviour.
- All staff must be clear about where the boundaries are in the support they offer to service-users, and must avoid setting up false expectations.
- All staff must ensure they are not put in the position of having to deal with information or situations that they are not confident or comfortable to deal with.
- **SurvivorsUK** must ensure that they do not create situations in which staff could cause harm to service-users.

- Any *moderators* or *administrators* whether trustees or staff with permitted unsupervised access to *Social Network Sites (SNS)* must be DBS checked.

- All staff working with service-users must not use their personal social networking account to communicate with service-users.

3.

General policies and procedures

Service-users who become trustees, other trustees, paid staff or volunteers

- If staff have their own personal *SNS profile*, they must ensure that service-users cannot access any content, media or information from that *profile page* that relates to **SurvivorsUK** or which would undermine their position as a professional, trusted and responsible adult working or volunteering with service-users at **SurvivorsUK** either as trustees, paid staff and volunteers.

- Staff who are currently or who have been service-users must moderate their use of SNS to reflect their status at **SurvivorsUK** accordingly just as they would moderate their behaviour in the offline world to reflect their responsible, role modelling status.

- All other staff who use their own personal SNS must ensure that service-users from **SurvivorsUK** cannot access any content, media or information from their personal *profile page*. All staff must check their privacy settings regularly to ensure this.

- Only **SurvivorsUK** official pages, profiles, groups and sites can be used to share information relating to **SurvivorsUK**. This boundary must not be confused by the use of personal SNS to convey information about **SurvivorsUK** by member of staff. For example, staff must not message service-users from their personal Facebook profile as this will blur boundaries between their professional and personal lives.

- All staff must review regularly that they have no *'Friend'* connections on their personal *SNS profile* with the service-users they work with. They should not accept *'Friend'* requests from service-users they work with to their personal *profile page(s)*. Paid staff and trustees who have been or are currently service-users are exempt from this clause.

- When entering into social media discussions outside work where a member of staff might be seen to be representing **SurvivorsUK** when in fact they are speaking as a private individual, they must make this clear with an explicit statement to this effect.

- Staff may only set up pages for events, activities or groups for which they are responsible and have *'officer'* or *'admin'* responsibilities for. The staff member with key responsibility in any context must always be the *administrator* or *officer* of these spaces.

- If, on behalf of **SurvivorsUK**, staff create a *group*, host *discussions* or encourage *media-sharing*, then the *Moderation Rules* (in Section 10) must be adopted. These provide rules for service-user engagement. Staff must create a group agreement with these ground rules about the kind of language, *discussions* and *media sharing* allowed. Staff must make sure these guidelines are created with service-users in mind and are accessible.

- Even with stringent *privacy settings*, the nature of *social networking sites* like *Facebook* means it is difficult to avoid seeing content from service-users which a trustee, worker, or volunteer may not wish to see/should not see outside their paid/voluntary role. Staff must not post or comment on the status, wall or photos of any service-users. Staff who have been or are currently service-users are exempt from this clause but their comments must nevertheless reflect their responsible and role modelling status at **SurvivorsUK**.

- Staff engaged in promotional or campaigning activities for **SurvivorsUK** will be encouraged and offered support to make maximum use of digital and social media as part of their work.

- Staff must not bring the organisation into disrepute in their use of digital and social media.

4.

Specific protective guidelines for trustees, paid staff and volunteers

- All staff must ensure they have clear understanding on who to contact if they have any concerns about service-users safety online. They must use the same chain of authority and advice (e.g. Director and/or Chair) as used in the generic Safeguarding Policy. If in doubt, they should go up a management level and consult.

- In all contexts, staff must conduct themselves in an appropriate way as they would face to face - be hyper aware of what they say and how they say it.

- All staff must be mindful that even if a comment is deleted straight away, someone might have already seen it. *SNS* sites happen in real time and some service-users are often constantly online and will see things as they happen.

- Staff must not provide personal details about service-users on the website, *SNS or social networking group* (this includes full name, email address, etc).

- All staff must ensure that they have permission to use any photos of service-users and only use their first names on any caption. *Tagging* of service-users in photos/videos will remain the responsibility of the individuals themselves and not trustees, paid staff or volunteers.

- Staff must only use appropriate photos, the sort that they would be happy putting on a public notice board – they must remember that everyone can view them.

- If staff would like to use a quote from a service-user which has been said during one-to-one contact, they must ask for permission before they use it and clarify how the person wants the quote attributed.

- If staff are concerned about the way a service-user is attempting to contact them, they must report it immediately to their line-manager (or other trustees in the case of a trustee).

- **The Digital Communications Officer** has overall responsibility for monitoring social media interaction on *Timelines, discussion boards, blogs*, comments on photos/videos, *tagging* of pictures/videos and *'Group'* or *'Fan Pages'* and *Twitter* mentions.

- All staff must ensure they do not infringe copyright. If they use photos taken by someone who is not part of **SurvivorsUK**, then they must ensure they credit the images or use images which are free of copyrights. The same practice applies for any other content that has not been created originally by **SurvivorsUK**.

- **SurvivorsUK** intellectual property rights and copyright must be asserted when publishing online.

5.

Rules for use of social media

Whenever you are permitted to use social media in accordance with this policy, you must adhere to the following general rules:

- Staff must not upload, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.
- Any member of staff who feels that they have been harassed or bullied, or are offended by material posted or uploaded by a colleague onto a social media website should inform the Chief Executive Officer.
- Staff must never disclose commercially sensitive, anti-competitive, private or confidential information. If staff are unsure whether the information they wish to share falls within one of these categories, they should discuss this with the Chief Executive Officer.

- Staff must not upload, post or forward any content belonging to a third party unless they have that third party's consent.

- It is acceptable to quote a small excerpt from an article, particularly for the purposes of commenting on it or criticising it. However, if staff think an excerpt is too big, it probably is. Staff must quote accurately, include references and when in doubt, they must link, don't copy.

- Before staff include a link to a third party website, they must check that any terms and conditions of that website permit them to link to it. All links must be done so that it is clear to the user that they have moved to the third party's website.

- When making use of any social media platform, staff must read and comply with its terms of use.

- Staff must not post, upload, forward or post a link to chain mail, junk mail, cartoons, jokes or gossip.
- Staff must be mindful of the impact their contribution might make to people's perceptions of SurvivorsUK as a company. If they make a mistake in a contribution, they must be prompt in admitting and correcting it.
- Staff are personally responsible for content they publish into social media tools – staff must be aware that what they publish will be public for many years.
- Staff must not escalate heated discussions and should be conciliatory, respectful and quote facts to lower the temperature and correct misrepresentations.

- If staff note a conversation which calls the organisation into dispute or in which someone is acting in a way that they believe may be harmful to them (e.g. stating they are suicidal etc) then they should try to take the conversation "off-line" and into a private messaging space where issues can be resolved and the person supported.

- If staff feel even slightly uneasy about something they are about to publish, they should discuss it with the Chief Executive Officer or the Director of Clinical Services first.

- Staff must always consider others' privacy and avoid discussing topics that may be inflammatory e.g. politics and religion.

- Staff must avoid publishing their contact details where they can be accessed and used widely by people they did not intend to see them, and never publish anyone else's contact details.

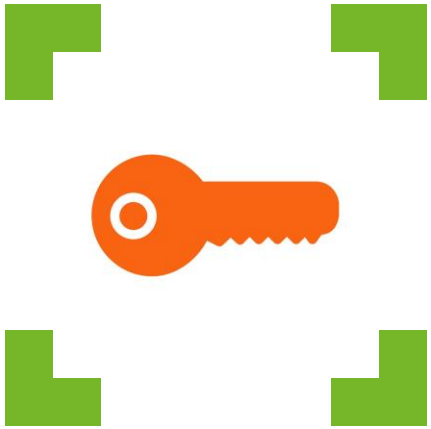
- Activity on social media websites during office hours should complement and/or support staff's roles and should be used in moderation.

- If staff notice any content posted on social media about SurvivorsUK (whether complementary or critical) they should report it to the Chief Executive Officer.

- Staff should not access, view, receive, download, send or store material from sites such as those relating to pornography, racism, terrorism, cults, hate speech, illegal drugs or other inappropriate sites. To do so may be considered an act of gross misconduct. The only possible exceptions to this are for employees who need to access such sites in relation to work. For example, someone in the helpline service may need to go to a site about gambling addiction or a member of staff may have good reason to go to a site about the effects of illegal drugs. Visits to such sites however should be limited strictly to work-related issues.

6.

Passwords



Staff must keep **SurvivorsUK** account and password details in a safe place. They must ensure that the **Digital Communications Officer** has overall access to e-mail accounts and networking sites for when they are on leave, absent or no longer working with the project. When staff leave the project, passwords must be changed.

7.

Email and SMS (texts)

- Emails sent to external organisations should be written carefully in the same way as a letter written on **SurvivorsUK** headed paper.
- When sending emails to groups of service-users, staff must use the 'BCC' facility to avoid sharing e-mail addresses.
- Staff may only use **SurvivorsUK** e-mail accounts to contact service-users.
- Staff must not reveal personal details of themselves or others in e-mail and SNS communication, or arrange to meet anyone without specific permission.
- If a text is sent to a service-user, it must be sent from an official work mobile.

8.

Publishing service-users' images and names

- In case of any photographing/videoing in which service-users take part, they will be informed that if they would not like to be used in **SurvivorsUK** publicity they must make themselves known to staff at the time of photographing/videoing. When images/videos are posted of service-users, no names should be mentioned and no-one should be tagged, unless you have specific approval to the contrary.

- Service-users full names will not be used anywhere on the website or *SNS*, particularly in association with photographs and videos, unless you have specific approval to the contrary. *Tagging* of service-users in photos/videos will remain the responsibility of the individuals themselves.

9.

Staff use of digital and social media at work

- Staff may not use email or social media for unofficial or inappropriate purposes, including

  - any messages that could constitute bullying, harassment or have any other detrimental impact, as well as *flaming* (deliberately provocative communications)
  - on-line gambling
  - accessing or transmitting pornography
  - transmitting copyright information and/or any software available to the user
  - posting confidential information about other employees, the charity or its clients or suppliers
  - contact with extremist groups or political parties

- The use of digital and social media at work using **SurvivorsUK** equipment and internet connections to access and/or distribute any kind of offensive material, inappropriate sites considered pornographic or those of extremist organisations will lead to disciplinary action.

- **SurvivorsUK** permit the incidental use of social media websites for personal use subject to certain conditions set out below. However, this is a privilege and not a right. It must neither be abused nor overused and SurvivorsUK reserve the right to withdraw the permission at any time at our entire discretion.

- The following conditions must be met for personal uses to continue :

  - Use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before 9:30 am or after 5.00 pm);
  - Use must not breach any of the rules set out in section 5
  - Use must not interfere with business or office commitments

10.

Monitoring use of social media websites and moderation rules

- Staff should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored and, where breaches of this policy are found, action may be taken.

- **SurvivorsUK** reserve the right to restrict or prevent access to certain social media websites if we consider personal use to be excessive. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

- Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against staff and **SurvivorsUK**. It may also cause embarrassment to **SurvivorsUK** and to our clients.

- In particular uploading, posting forwarding or posting a link to any of the following types of material on a social media website, whether in a professional or personal capacity, will amount to gross misconduct (this list is not exhaustive):

  - pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
  - false and defamatory statement about any person or organisation;
  - material which is offensive, obscene, criminal discriminatory, derogatory or may cause embarrassment to us, our clients or our staff;
  - confidential information about us or any of our staff or clients (which you do not have express authority to disseminate);
  - any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or
  - material in breach of copyright or other intellectual property rights, or which invades the privacy of any person.

Any such action will be addressed under the procedures outlined in the Employee Handbook and is likely to result in summary dismissal.

- Where evidence of misuse is found SurvivorsUK may undertake a more detailed investigation in accordance with our Employee Handbook, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the investigation.

- If staff notice any use of social media by other members of staff in breach of this policy they should report it to the Chief Executive Officer.

11.

Comment and post moderation

- **SurvivorsUK** encourage and welcome open, lively debate on our social media accounts, but we take no responsibility for any content posted or interactions by third parties on our social media accounts. The view expressed by any third parties are solely theirs and are not necessarily endorsed by SurvivorsUK.

- All **SurvivorsUK** channels and communities are monitored regularly and we reserve the right to suspend comments at any time, and remove comments older than six months.

- **SurvivorsUK** will review and possibly delete any comments or messages that:

- **SurvivorsUK** will review and possibly delete any comments or messages that:

  - incite hatred on the basis of race, religion, gender, nationality or sexuality or any other personal characteristic;
  - are off-topic or unrelated;
  - are disrespectful, malicious or offensive;
  - could constitute a personal attack on a person's character;
  - impersonate or falsely claim to represent a person or organisation;
  - are party political;
  - include swearing or obscenity;
  - are not persistent or repetitive negative messages which aim to provoke a response and/or don't constructively add to the conversation;
  - don't impersonate or falsely claim to represent a person or organization;
  - are illegal – including libel or breaking copyright;
  - could be considered spam;
  - contain personal information like phone numbers, address details, etc;
  - advertise commercial activity or make requests for donations or money, unless agreed in advance with SurvivorsUK.

- Enquiries or concerns about comments and posting can be emailed to info@survivorsuk.org
- SurvivorsUK aim to update and monitor its social media accounts daily and during regular office hours: Mon-Fri, 09.30 – 17.00, GMT. However, due to limited staff capacity, this may not always be possible.
- SurvivorsUK will read all replies and direct messages sent to us and, when possible, will respond to them.

12.

Responsibility for implementation of the policy

- The Chief Executive Officer has overall responsibility for the effective operation of this policy.
- The Chief Executive Officer is responsible for monitoring and reviewing the operation of this policy and making recommendations for changes to minimise risks to our operations.
- The Chief Executive Officer is responsible for reviewing this policy annually to ensure that it meets legal requirements and reflects best practice.
- All staff are responsible for their own compliance with this policy and for ensuring that it is consistently applied. All staff should ensure that they take the time to read and understand it. Any breach of this policy should be reported to the Chief Executive Officer.

- Questions regarding the content or application of this policy should be directed to the Chief Executive Officer.

SURVIVORSUK

E-Safety Policy
Policy Date: May 2016
Policy Renewal Date: May 2019

Prepared by Agnese Manfrin
Digital Communications Officer
SurvivorsUK
communications@survivorsuk.org

SurvivorsUK

11 Sovereign Close
London
E1W 3HW

02035983898

info@survivorsuk.org