NHS
South Central Ambulance Service
NHS Foundation Trust

Social media guidance

March 2022

1. Introduction

The guidance sets out the principles which Trust employees and volunteers should follow when using social media, whether they are using a Trust-approved corporate account and/or using personal accounts.

The intention of this guidance serves to highlight those areas in which problems can arise for both individuals and the Trust, threatening someone's role or position and the reputation of them and the organisation.

Because of the nature of emerging digital changes and new platforms coming on board annually, it is impossible to cover all circumstances but the social media controls in the Acceptable Use of Information and Technology Policy must always be followed and this guidance should be followed.

2. Scope

This guidance applies to all SCAS employees and volunteers (encompassing the references employees, workers, non-executive directors, governors and volunteers).

Individuals who are undertaking work placements with the Trust, such as university students, or observers must also follow the controls set out in the Acceptable Use of Information and Technology Policy and the guidelines set out in this document in conjunction with their own institute or employer's social media policies and frameworks.

3. Aim

This guidance aims to ensure that employee or volunteer use of social media does not damage the Trust's reputation, that patient confidentiality is adhered to at all times and that it is an environment where individuals are treated with dignity and respect.

This guidance encompasses use of social networking in both a professional and personal capacity and aims to enable employees and volunteers to protect themselves while using social media.

4. Roles and responsibilities

4.1 Communications Department, Information Technology and Human Resources

This guidance has been developed and is reviewed by the Communications Department in conjunction with the wider Acceptable Use of Information and Technology Policy (AUP) developed by Information Technology.

The Human Resources Department advises on employment legislation in relation to the policy and guidance, best-practice people management principles and NHS guidelines.

5. Definitions

Social media – for the purposes of this guidance, social media is any type of interactive online media which includes platforms that enable users to communicate their thoughts, opinions or observations with other people for a variety of reasons. See more below in **section 7. The scope of social media**.

Trolling – Where a social networking user communicates a deliberately provocative posting with the aim of inciting a response, usually with contents that are hurtful and/or personal.

6. Development

6.1 Prioritisation of work

This document has been developed to offer guidance to everyone about the expected level of conduct when using social media alongside the controls which must be adhered to as outlined in the AUP.

6.2 Responsibility for document's development

The Communications Department is the author of this guidance.

7. The scope of social media

Social media platforms include, but are not limited to:

- Facebook
- Twitter
- Instagram
- TikTok
- LinkedIN
- Google Plus

- Snapchat
- YouTube
- Flickr
- Blogs
- Podcasts
- Message Boards
- Chat Forums
- Information sharing sites (e.g. Wikipedia)

These allow people to network, build communities, and collaborate on ideas and work. For instance, Facebook provides what has become an integral way for people to keep in touch with friends and colleagues.

This does mean, however, through the potentially public nature of such sites it is also possible for third parties to collate vast amounts of information.

When someone clearly identifies their association with SCAS and/or discusses their role, they should behave appropriately and in ways consistent with the Trust's values, expected conduct, and their individual responsibility as an employee or volunteer. This expectation applies whether the communication can be seen by the public or whether it is via direct communication with an individual(s) available through the social media site.

Relevant professional codes of conduct also apply to some roles including healthcare professionals and NHS managers. If you are a paramedic, we would strongly recommend that you read the guidance documents issued here by the Health and Care Professions Council (HCPC):

https://www.hcpc-uk.org/globalassets/resources/guidance/guidance-on-social-media.pdf
https://www.hcpc-uk.org/registration/meeting-our-standards/guidance-on-confidentiality/
https://www.hcpc-uk.org/standards/standards-of-conduct-performance-and-ethics/

The College of Paramedics and Nursing and Midwifery Council have also produced guidance on social media:

https://www.collegeofparamedics.co.uk/socialmedia

www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/social-media-guidance.pdf

Any member of staff registered with a professional body is advised to review and follow the guidance available to them via these organisations.

We would also advise all users to read and follow guidance set out by the National Cyber Security Centre here: Social Media: how to use it safely - NCSC.GOV.UK

7.1 Privacy

All employees and volunteers should be mindful of the personal information they disclose on social media platforms, to reduce the risk of identity theft and data breaches. Making information such as your date of birth, your place of work, and other personal information publicly available is high-risk. As an example, your date of birth can be identified by referencing that it is your birthday and referring to how old you are.

In relation to privacy there is a perception, for example, that because Facebook users can limit access to their Facebook profile to 'friends', that the information within their profile is confidential. However, when a photograph is uploaded to Facebook, they have a royalty-free, sub-licence, and worldwide licence to use it, subject to its terms of service which you agree to when you sign up.

7.2 Trust access

Social media users can post a great deal of information which can be circulated rapidly at the touch of a button and become instantly accessible to other users.

In other words, this information enters the public domain and the subject loses control of its ownership; it also means it could be used as evidence in potential disciplinary cases. The information shared on social media can also be exploited by other users – not necessarily for negative reasons, but often because of this – and individual names are easily searchable. Anyone with an 'open' account (i.e. easily accessible through searches) should consider these two examples as a means of helping SCAS protect its employees and volunteers.

7.3 Third party access

Information shared on social media can be used and possibly exploited by other users, but also individual names can be easily searched for.

Examples could include:

Journalists wishing to gain information about SCAS or patient-facing incidents by reviewing social networking entries (a hashtag on Twitter might lead them to an individual's account) or searching for names on sites. Any attempts from journalists making contact, should be referred to the Communications Department, unless you are running a personal event or are the subject of a feature they're running on you in your personal capacity and have given reporters express permission to be contactable on social media.

Clinicians who receive contact from a patient or their representative via social networking sites following an incident should be politely referred to the Patient Experience team to make formal contact.

8. Employee and volunteer conduct online using social media

8.1 Everyday use

Everyone has the right to be digitally-engaged and use social media platforms, and SCAS acknowledges that people do so because there are benefits and advantages when using these platforms appropriately. Because social media has become integral to people's day-to-day activities and thus there is potential to reach more audiences, SCAS has long-established Facebook, Twitter, Instagram and YouTube accounts to engage with stakeholders. There are also internal-only engagement tools including private Facebook and WhatsApp groups (SCAS staff/volunteer-only membership on private groups) and it should be noted here that the internal communications forum, Yammer, forms part of this.

The Communications Department is responsible for running the Trust's main social media accounts under the corporate banners of @SCAS999 and a small number of other teams and departments, such as Education, Recruitment and the Hazardous Area Response Team (HART), manage their own social media channels with arm's length guidance and oversight from the central Communications Department.

Other Facebook and social media groups have been set up and run by other members of staff (e.g. to support charity fundraising efforts) and volunteers.

8.2 Expected standards

Hundreds of employees and volunteers regularly engage on social media and it is expected that they should use any platform and channel responsibly and with regards to the content in this guidance and the controls in the Acceptable Use of Information and Technology Policy.

Employees and volunteers should always verify any information for accuracy when using social media, and expressly state that the views and comments made are personal ones and are not related to SCAS when using public-facing channels. However, just doing this alone doesn't protect a person from consequences – no-one can act with impunity and have no repercussions because of this disclaimer. An account holder will be held accountable for those statements/comments and this can affect you in employment tribunals and/or regulatory enquiries.

Governors should also refer to Governor Code of Conduct and Charter of Behaviours with additional information on social media responsibilities contained within the Governors' handbook.

Employees and volunteers have a duty to conduct themselves in a professional manner, and to post or withhold information in accordance with the following:

- Only patients who have given express verbal and written consent to share images or information can be featured in posts and only then if the individual posting the content knows the patient has capacity to agree to the terms of sharing their image/information e.g. ambulance ride-outs, insight days, public-facing events. This information, consent and the right to withdraw consent must be managed and processed in accordance with current Data Protection Legislation and it is the individual's responsibility to ensure the consent is retained on file.

- No confidential or personal information about other employees or volunteers should be shared without their express consent. This information, consent and the right to withdraw consent must be managed and processed in accordance with current Data Protection Legislation. An example is a photo celebrating a career milestone (training, award, etc.); the individuals / group involved must give their express consent for it to be shared before a photo is taken. Should someone not wish to give their consent, this is their individual choice and you should instruct them to stand aside whilst a photo is taken.

- The Trust does not proactively report on incidents. Media enquiries about incidents are handled and recorded via the Trust press officers, as well as enquiries made on social media by journalists. Therefore, staff and volunteers must not post publicly about incidents or respond to posts giving more details. For those who run Trust corporate accounts and therefore who have been given additional guidelines on engagement on social media, any reactive information about incidents should be redacted to: geographic area, responses dispatched and, where appropriate, brief outcome for patients involved. Photos should not contain any information or imagery that can lead to the identity of the people at the scene. This includes non-SCAS vehicle registrations, distinctive vehicles and branded vehicles.

- Posting any information must adhere to the Terms of Use of the relevant platform, as well as copyright, defamation, discrimination, harassment and other applicable laws.

- Employees and volunteers should be aware that posts may bring the Trust into disrepute in circumstances where they contain slurs, demeaning or inflammatory comments regarding individuals and/or SCAS as an organisation. If this is found to be the case this can result in disciplinary and/or regulatory action. This includes posts relating to another NHS organisation, third party, regulatory body or voluntary organisation.

- Accounts and/or postings should not be created and/or used as a means of attacking or abusing employees, volunteers, patients, anybody connected to the work of SCAS or any member of the public.

8.3 Disclosing employment and volunteering at SCAS
Employees and volunteers using channels which require users to confirm their employer name, professional qualifications and experience (e.g. LinkedIn) must consider the principles set out above before making any entries and adhere to the controls as stated in the Acceptable Use of Information and Technology Policy. Ensure that professional and personal uses are not confused; this can include disclosing employment indirectly, posting photos/videos from vehicles or in uniform.

Jigsaw identification – separate items of information that create a 'data' picture about someone – will leave you open to security issues if on separate profiles there is different information about you that together builds a picture of where you live, your DOB, your place of work, etc.

8.4 Contact from a third party
If employees or volunteers are contacted by a third party (e.g. media, former patient, partner organisation/stakeholder) about comments or entries they have on social media which are connected with SCAS and are unsure of what action to take, they should inform their line manager before responding. The line manager may wish to consult the Communications Department, Human Resources or Information Management and Technology department for advice and/or guidance. If the contact is from a patient or their family, they should be directed to the Patient Experience Team.

8.5 Mental health and wellbeing
If employees or volunteers post on social media when feeling either upset and/or angry, it can attract unwanted and inappropriate comments.

Therefore, it is strongly advised not to post any contentious or emotive work-related issues – even with strict privacy settings – as there is no guarantee how the information may be quoted, copied or shared by others who may or may not have been the intended recipients.

Even deleting a comment after it has been made may not prevent it from having been circulated early on – screen shots of comments can be, and are, taken of posts which are then separately shared for legitimate purposes or inappropriately.

The Trust's HR department has a number of well-established support mechanisms available to staff if they are feeling frustrated, overwhelmed or angry.

8.6 Potential outcomes

Breach of the controls outlined in the AUP will be managed in line with the SCAS' Disciplinary and Conduct Policy for employees and in line with NHS Volunteers' guidance and SCAS Volunteers' Operational Manual. Employees and volunteers must maintain both patient and colleague confidentiality as outlined in this document.

9. Personal profiles/blogging

9.1 Attributing profiles to the Trust

If employees or volunteers plan to write in a personal capacity online e.g. blogging, they must decide whether they wish to expressly mention SCAS. In the case of blogging or other forms of writing online which directly or indirectly references SCAS, permission should be sought from the Communications Department. It is advised that even if a decision is made not to disclose working or volunteering for SCAS, it may still be possible for users to link comments/disclosures with SCAS through jigsaw identification.

9.2 Managing your social media profiles

Employees and volunteers are responsible, liable and accountable for everything that they post online. This includes posting on their own social media and comments and responses made to other blogs and social media posts.

If a third party posts something in your profile which could breach the principles set out within the controls outlined in the AUP and Section 8 above, you must take a screen shot of the entry, remove the whole post or hide responses where applicable and contact your line manager/reporting lead to make them aware. If applicable, it is advisable to report the breach to the platform itself to take appropriate action.

If an employee or volunteer account becomes compromised i.e. hacked, then they have a responsibility to resolve the matter as soon as they are aware of the situation which may include removing all entries not made by themselves and taking steps to ensure the security of their account.

Employees and volunteers are responsible for maintaining the security and integrity of any passwords and access to social media platforms.

All users are reminded to respect copyright, fair use, data protection, defamation, libel and financial disclosure laws.

10. Photos, artwork and other imagery

10.1 Sharing/posting of photos, artwork and other imagery

- Employees and volunteers must not post anything which depicts any SCAS-identifiable uniform, ID badges, vehicle, crest or other branding in a negative light and/or may bring SCAS into disrepute, reveals confidential information about a patient or colleague or knowingly compromises any ongoing investigation by SCAS or a third party.

Any of the above may result in disciplinary and/or regulatory action.

Additionally, photos may not be posted which depict the day-to-day activity of SCAS in any form without prior consent of an appropriate manager and the Communications Department.

10.2 Production of photos or videos

Photographs may only be taken during work or volunteer time for social media posts which are for the benefit of SCAS and are in line with the terms of the AUP and this guidance. Photographs taken for the benefit of SCAS by individuals during work or volunteer time should primarily be used through official social media streams (@SCAS999). When not used through official social media streams (i.e. sent to the Communications Department), users should share with official social media streams (i.e. tag @SCAS999) to ensure activity can be monitored and they should seek the permission of their line management before doing so.

11. Respecting others on social media

Whilst there is an expectation by many colleagues, stakeholders and members of the public that SCAS employees and volunteers will share positive work-related information on social media that they are involved in, no assumptions should be made that everyone is comfortable with their image or information being put out in the public domain.

For example, there may be an expectation that photographs taken at a private SCAS event will not appear publicly on social media, both from those present and perhaps those not at the event. Employees and volunteers should be considerate to their colleagues in such circumstances and should not post information when they have been asked not to. They should also remove information about a colleague if that colleague asks them to do so.

Under no circumstance should offensive comments be made online about any colleagues, patients or members of the public as this may amount to cyber bullying and could be deemed a disciplinary offence.

12. Accessing social media using the SCAS IT system and for SCAS-related work

Under SCAS' AUP, no employee has automatic access to all social media using a device such as Trust PCs, phones or tablets. Where employees can access a platform, they must note that engaging in any kind of online activity which is not work related is strictly prohibited.

It may be necessary for some staff to engage in social networking due to the nature of their role e.g. Communications, and those managing or contributing to other SCAS corporate social media accounts (such as @SCASJOBS). In cases where staff believe they require access, they need permission from their line manager and only then use social media for justifiable business activities. In addition, any new SCAS social media accounts need to be approved for use by the Trust's Communications Department.

Anyone accessing social media on a SCAS device, particularly if it is a shared PC or used in an open work space, must logout to reduce the risk of your profiles being accessed by unauthorised people.

Exiting the browser or turning the machine off will not be enough.

13. Identifying individuals

Employees and volunteers must not attempt to gain information about individuals and/or organisations through social media. This is to protect themselves and/or the Trust from any assertion that they have gained information about a third party which could compromise any SCAS process. This is particularly the case for:

- recruitment - unless an applicant specifically directs the recruiter to a site or area for the purposes of making their application
- procurement - unless a tender process requires the Trust to review information held online in a legitimate manner.