South East Coast Ambulance Service NHS
NHS Foundation Trust

Social and Digital Media Policy

Contents

1. Statement of Aims and Objectives

1.1 South East Coast Ambulance Service NHS Foundation Trust (the Trust) is committed to maintaining the highest possible standards of practice and to ensuring that all its dealings and activities are ethical, transparent, and compliant. To that end, this policy sets out clear, reasonable guidelines for employees on acceptable and appropriate use of social networking and social media platforms.

1.2 The policy sets out the actions the Trust will take where behaviour falls below the expected standards and helps to ensure that the Trust's patients, employees, and reputation are protected, and the Trust is not exposed to legal and/or governance risk.

2. Principles

2.1 In order for the Trust to maintain a good social media and digital reputation and to avoid detrimental impact on individual staff members (which could result in disciplinary or other action inside or outside of the Trust), it is critical that employees act appropriately in their personal and/or professional use of social media. This applies equally to internal social media platforms used by the Trust, as well as external platforms used in a personal capacity.

2.2 It is not the intention of this policy to prevent employees from enjoying normal and appropriate use of social media technologies and the Trust fully appreciates the rights of employees to privacy and to freedom of expression. However, the Trust must also ensure these rights are balanced with its legal responsibilities and employees' responsibilities and duties to patients, employees, partners, and the public.

2.3 Social media use by employees, either privately or professionally, is covered by the same principles as any other media. Social media is a public forum, and the same considerations should be applied to it as would be applied to speaking in public, speaking to the media, or writing an item for publication either officially or outside of work.

2.4 Whether officially authorised to speak on behalf of the Trust or not, employees may be seen by people outside of the Trust as representatives of the Trust and should also be aware that they are often held in high regard externally as employees of the NHS and of the emergency services. Employees should represent the Trust values and core values in the NHS Code of Conduct and other relevant registering bodies whenever they choose to make social media comments.

2.5 The policy recognises that social media is used extremely widely, both personally and professionally. It affords significant positive opportunities for two-way communication and engagement and can enable the rapid and widespread communication of key messages, including with those who may be considered 'harder to reach' through other media.

2.6 Employees should always be respectful of every individual's legal right to express their opinion. When using social media, employees must adhere to the Trust's Equality, Diversity, and Inclusion Policy - anything containing ageist, racist, sexist, homophobic, transphobic, sexually explicit, threatening, abusive, disrespectful, or other unlawful comments must not be published.

2.7 Inappropriate comments relating to protected characteristics (for example age, sex, race, disability, religion, sexual orientation, nationality, or any personal characteristic of the individual) as set out in current equality legislation, must not be posted. There must also be proper consideration of privacy and of topics that may be considered or perceived to be objectionable or inflammatory or that have the potential to offend, such as strong views on politics and religion.

2.8 It is illegal to comment on or undertake behaviours on social media which could cause harassment, malicious communications, stalking, threatening violence and incitement or crimes. This behaviour and any breaches of privacy, confidentiality or information security will be investigated in line with the Trust's Disciplinary Policy and Procedure.

2.9 Whilst appreciating the rights of employees to privacy and to freedom of expression, employees should be aware, beforehand, of the impact of sharing or supporting information that directly contradicts national NHS or Trust policy and the potential impact on patients and members of the public.

2.10 The Trust will not actively seek to monitor employee activity on social media where this is conducted outside the workplace. However, if the Trust is alerted to inappropriate social media activity undertaken by any employee, it reserves the right to investigate the matter fully and to act if necessary.

2.11 The Trust does not use social media to vet or gather further information on candidates in its recruitment process.

2.12 Breaches of this policy will be investigated if necessary and addressed in accordance with the appropriate Trust's policy and procedure.

2.13 The Trust will ensure that employees are made aware of this policy, during induction of new employees and by regular reminders, particularly about any changes or updates.

3. Scope

3.1 This policy applies to all employees of the Trust regardless of level or length of service, as well as those holding bank contracts and all volunteers, contractors, students, and apprentices who are operating on behalf of or working closely with the Trust,

3.2 Any social media issues regarding third parties will be referred to the employing agency/company and will be resolved under the contractual arrangements in place.

3.3 This policy applies to all content types such as images, posts, videos or audio recordings on social networking sites, personal web pages, blogs, personal space, and mobile phone apps provided by internet providers and all social media platforms that are current and that may be developed in the future.
These include but are not limited to:

- Facebook
- Google+
- Twitter
- YouTube
- TikTok
- Vimeo
- Flickr
- LinkedIn
- Myspace
- Snapchat
- Instagram
- Bebo
- WhatsApp
- Telegraph
- Tumblr
- Whisper
- Pinterest
- Yelp
- OnlyFans

3.4 This policy applies equally to all externally accessible social media platforms, as well as Trust and local internally accessible social media sites, including those available Trust-wide as well as individual team or area sites.

3.5 Social media must not be used to conduct formal Trust business, including matters relating to patient care or staff employment, as our governance polices do not cover this use.

3.6 The Trust acknowledges there are several professional social media services or platforms that are used for both professional and private social use, for example LinkedIn and Yelp. Employees may wish to identify themselves as Trust employees for the purposes of professional networking, however the same principles of appropriate conduct apply.

4. Responsibilities

4.1 All employees have a responsibility to always act in a professional manner and the Trust expects and trusts employees and all those covered by this policy as referenced in 3.1 above, to act professionally and exercise personal responsibility whenever they use social media.

4.2 In addition to Trust responsibilities, those employees who hold professional/clinical registration should ensure that they are familiar with the relevant guidance and/or Code of Conduct provided by their professional body and the standards expected regarding social media use.

4.3 All employees are encouraged to report any concerns to the Trust regarding inappropriate or illegal social media activity as soon as they become aware of it.

4.4 Employees are responsible for making sure their social media activities do not interfere with fulfilling their job requirements or their commitments to the Trust, patients, and colleagues. They must:

- not share information which puts patient confidentiality at risk, or which could bring the Trust, the NHS, or their profession, into disrepute or is in any way derogatory to the patients we serve
- ensure that their social media activities are in line with the Trust values
- refrain from sharing photos of Trust equipment or estate, without permission from the Communications Team, as this could present a security threat
- take care to avoid revealing confidential information or information they hold in trust, including about their colleagues
- refrain from publishing or republishing material that may cause injury to the Trust, another person, organisation, association, or company's reputation - any such activity may result in disciplinary action and/or legal proceedings for posts, sharing of posts or retweets aimed at named individuals or an organisation, that are considered to harm their reputation
- take care not to speak or act in a way that could be seen by their colleagues or by external stakeholders as deliberately or accidentally bringing the Trust into disrepute or otherwise damaging its reputation: this includes using social media to criticise, attack, undermine, embarrass, or air grievances about the Trust, its positions, programmes, employees, or leadership, as well as comments about individual Trust employees

- consider the impact of any negative references to the Trust or any of its partner agencies by friends, colleagues and other contacts and remove any such posts on their own social media as soon as they become aware of them

- reserve caution if contacted by a journalist or an unknown individual who is asking questions about the Trust, and should speak to their line manager or seek guidance from the Trust's Communication team

- not set up sites which resemble an official Trust site, without the knowledge or explicit consent of the Trust's Communication team

- not engage in activities which may constitute copyright infringement, for example use the Trust's logo or crest or other professional Trust images, without the express consent and explicit approval of the Trust Communications Team; this includes the unauthorised use of uniform or Trust equipment

- review and where appropriate enable security settings to ensure that social media activities are compliant with this policy

- ensure they present a professional image and are compliant with the Uniform Policy when appearing in photos

4.5 Employees must maintain up to date knowledge of the implications of social media use and be aware that:

- their own safety and security, and that of others, may be at risk when images are disclosed or displayed that reveal personal information such as home address, date of birth, street name, car number plate or other similar information

- even if the highest level of privacy settings is established on social media pages, there is still the potential for posts to show on friends and family pages or for information to be forwarded on indefinitely

- once an item has been posted on any social media platform, it is then in the public domain indefinitely - comments made on social media sites are public and searchable even if they are deleted

- when posting on social media, information is neither private nor temporary and disclosures live online indefinitely, and posts may be visible to a broad audience

- they may be identified online as Trust employees, either through their own direct declaration on their social media pages, or through a general understanding within their online network of family, friends and associates – and must always consider this association in their social media activity and act appropriately; employees should also

be aware of the potential of 'jigsaw identification' i.e. where separate items of information, potentially across different social media profiles, can be pieced together to create a 'data' picture

- posting on social media when feeling either upset and/or angry can attract unwanted and inappropriate comments; deleting a comment after it's been made may not prevent it from having been circulated previously. Employees are advised not to post any contentious or emotive work-related issues - even with strict privacy settings - as there is no guarantee on how the information may be quoted, copied, or shared by others who may or may not have been the intended recipients – and to seek support elsewhere as needed e.g., via the Trust's Wellbeing Hub.

- when appearing in any images on social media in the uniform associated with the Trust, they are representing the Trust, even if not naming it explicitly

- if they disclose that they work for the Trust, they must make clear that opinions shared on their social media platform are their own views only; however, this does not negate the need to adhere to the points contained in 4.4 above.

5. Confidentiality

5.1 Social media can provide employees with a space in which they can discuss their experiences within clinical and professional practice and enhance learning and study.
However, staff should exercise extreme caution when discussing any details relating to specific incidents that they or their peers have attended.

5.2 All employees have a legal and ethical duty to protect patient privacy and confidentiality. Disclosing any identifiable information about patients without the consent of the patient on medical forums or any social networking sites would constitute a breach of confidentiality. Presenting clinical experiences, even hypothetically, on online forums or on social media platforms can be a direct breach of patient confidentiality as posts may be geo-located and inadvertently identify patients.

5.3 Staff must not, in any circumstances, share photographs or details of any incidents or patients, regardless of whether consent has been given by those involved. Please contact the Trust's Communication Team if guidance is required.

5.4 Individual pieces of information may not on their own breach patient confidentiality, however the culmination of published information could be sufficient to identify a patient, their relatives, or the location of their incident.

5.5 With awareness and caution, employees can avoid intentionally or unintentionally disclosing confidential or private information about patients.

To minimise the risks of using social media in relation to patient confidentiality, all employees must:

- not share, post, or otherwise disseminate any patient information they have learned because of providing care on behalf of the Trust
- safeguard all such information and only disclose data to colleagues for the purpose of providing care or liaison for the patient on a suitable Trust system or platform
- follow Trust policies for taking photographs or videos of patients for treatment or other legitimate purposes using trust-provided, not personal, devices

6. Privacy and Information Security

6.1 Employees must comply with the Trust's policies on information governance and security, which are readily available on the Intranet.

6.2 Individuals have a right to their personal privacy. They have the right to keep their personal opinions, beliefs, thoughts and emotions and anything else they wish as private. Therefore, employees should not share anything via social media channels that could violate a patient's or colleague's right to privacy.

6.3 Examples of social media disclosures that may compromise a person's right to privacy include, but are not limited to:

- pictures, video, or audio recording that are shared through social media channels without the permission of any single individual featured
- the public disclosure of private facts, or information that is likely to identify individuals
- the disclosure of information gained through privileged access or unreasonable intrusion

6.4 Employees must seek permission from anyone before posting personal details or images that may link them with the Trust and must not post anything about someone if they have been asked not to. Employees must always remove information about someone if they have been asked to do so.

7. Bullying and Harassment

7.1 The Trust's Bullying and Harassment policy and procedure applies to social media as well as in the physical workplace. Workplace bullying and harassment includes any bullying or harassing comments or behaviour employees make or participate in, even on their own private social media networks or out of working hours.

7.2 All employees are expected to treat their colleagues with respect and dignity and must ensure their behaviour does not constitute bullying and/or harassment - see the Trust's Bullying & Harassment Policy and Procedure for more information.

7.3 Abusive, harassing, threatening, or defaming postings are in breach of the Trust's Bullying and Harassment Policy, and may result in disciplinary action being taken.

8. Raising Concerns at Work

8.1 The Trust encourages employees, volunteers, and others with serious concerns about any aspect of its work to come forward and express those concerns. However, it should be recognised that social media, whether internal or external, is not the appropriate channel to do this.

8.2 There are several channels through the Trust's normal procedures that colleagues can use to raise concerns or complaints such as the mechanisms for resolving grievances and disciplinary matters, as well as Freedom to Speak up and the Trust's regonised Trade Unions. Employees should refer to the Trust's Raising Concerns at Work (Whistleblowing) Policy for further information.

9. Audit and Review (evaluating effectiveness)

9.1 Adherence to this Policy, as far as is practicable, will be monitored by the Trust Communications Team, as well as via incidences highlighted via the complaints and grievance policies, via Freedom to Speak up, other channels used by employees to raise concerns and by individual staff members.

9.2 Non-compliance with the Policy will be dealt with, as appropriate, via existing Trust mechanisms, including the Disciplinary procedure where needed.

9.3 This document will be reviewed in its entirety every three years or sooner if new legislation, codes of practice or national standards are introduced, or if feedback from employees indicates that the policy is not working effectively. In addition, given the changing nature of social and digital media, an annual review will be undertaken with relevant stakeholders.

9.4 All changes made to this policy will go through the governance route for development and approval as set out in the Policy on Policies.

11. Financial Checkpoint

11. 1 This document has been confirmed by Finance to have no unbudgeted financial implications.