East of England Ambulance Service NHS Trust

Social Media Policy

Document Reference:	POL078
Document Status:	Approved
Version:	V2.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author (s)**
Communications Team	17/05/2018	Director of Communications and Engagement
Version	**Date**	**Comments (i.e., viewed, or reviewed, amended approved by person or committee)**
Draft V0.1	24/05/2018	Digital Manager
Draft v0.2	Circulated on 30/05/2018	Circulated to Policy Steering Group and Interim Head of Communications and Engagement for consultation
Draft V0.3	01/06/2018	Review by HR Policy Group and Head of Communications
Draft V0.4	January 2020	Review by HR Policy Sub-group
Draft V0.5	26 February 2020	Sent to SPF and ELT for approval
V1.0	22 April 2020	Approved by ELT
V1.1	16/06/2021	Reviewed and amended by Digital Communications Manager

Draft V1.2	October 2021	Reviewed and amended by Digital Communications Manager
Draft V1.3	November 2021	Reviewed and amended by Head of Governance and Culture Improvement Director
Draft V1.4	November 2021	Reviewed and amended by Head of Information Governance & Security
Draft V1.5	November 2021	Reviewed and amended by IG Team
Draft V1.6	4 March 2022	Policy sent to Browne Jacobson for external review
Draft V1.7	19 May 2022	Reviewed by The People Services team, HR Policy Subgroup including Ops managers
Draft V1.8	4 August 2022	Sent to Unison Regional Branch
Draft V1.9	10 August 2022	Sent to ELT
V2.0	23 August 2022	Approved at ELT
V2.0	19 June 2023	Extension to 31 August 2024
V2.0	29 September 2025	6-month extension approved by CRG
V2.0	26 January 2026	6-month extension approved by CRG

Document Reference	Directorates: Corporate Affairs and People Services
Recommended at Date	HR Policy Sub-Group 29 July 2022
Approved at Date	CRG 19 June 2023 (extension 26 January 2026)
Valid Until Date	July 2026 or until regulatory changes
Equality Analysis	4 March 2022
Linked procedural documents	Dignity at Work Policy Disciplinary Policy Raising Concerns Policy Internet Use Policy Official EEAST Twitter Account Guidance Data Protection Policy Information Governance Policy

	Information Security Policy (Electronic) Social media guidance documents: HCPC Guidance College of Paramedics Guidance AACE Best Practice Guidance Managing Safeguarding Allegations Policy Safeguarding Adults/Children's Policy
Dissemination requirements	To all staff via Trust Intranet and Need to Know article E-learning module on social media utilisation Via the MetaCompliance Policy application
Part of Trust's publication scheme	Yes

The East of England Ambulance Service NHS Trust (the Trust) has made every effort to ensure this policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of: age, disability, gender reassignment, race, religion/belief, gender, sexual orientation, marriage/civil partnership, pregnancy/maternity. The Trust will not tolerate unfair discrimination on the basis of spent criminal convictions, trade union membership or non-membership. In addition, the Trust will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups.

All Trust policies can be provided in alternative formats. Please contact the People Services Department if you require an alternative format.

Contents

1. Purpose of policy

The purpose of this policy is to provide guidance on social media use and to minimise the risks to the Trust and its staff through responsible use of social media. This policy applies to the use of social media in both a professional and personal capacity, where personal use affects the Trust in any way. Using social media responsibly is part of the professional standards that we expect all staff to adhere to.

Social media has blurred the boundaries between a person's private and professional life. Staff who use social media in their personal life should therefore be mindful that inappropriate content could have implications on or damage their own reputation and that of the Trust and its staff, and cause harm to others.

The world of social media changes rapidly and exponentially, it is therefore impossible to cover all circumstances that may occur, but the principles in this policy must be followed. This policy is under regular review to adapt to the evolving changes in social media and its use.

2. Breach of policy

Breach of this policy may result in disciplinary action up to and including dismissal. If the Trust suspects you have committed a breach of this policy, you are required to co-operate with any investigation.

Breach of this policy may also put professionally qualified staffs' registration at risk. Professionally qualified staff must read and adhere to the social media guidelines produced specifically for their registered bodies (e.g. HCPC) in addition to this policy.

You will be required to remove any social media content that the Trust considers to constitute a breach of this policy. Failure to comply with that request may in itself result in disciplinary action.

3. Scope

This policy applies to all individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Trust.

4. Responsibility for policy

4.1 Chief Executive

As the accountable officer for the Trust, the Chief Executive is responsible for meeting all statutory requirements and required to provide assurance that all information risks to the Trust are effectively identified, managed and mitigated. Details of incidents involving data loss or confidentiality breaches must be recorded on Datix and on the NHS Digital Data Security and Protection Toolkit (DSPT) tool. All serious information incidents are reported in the annual quality account report.

4.2 Director of Corporate Affairs and Performance

The Director of Corporate Affairs and Performance is responsible for ensuring, via the Communications and Engagement Team (C&ET) that appropriate training, support, advice and guidance is provided to staff in relation to social media use, and that corporate social media is utilised appropriately.

4.3 Director of People Services

The Director of People Services is responsible for ensuring, via the People Services team, compliance with this policy and ensuring appropriate action is undertaken when staff raise concerns relating to the use of social media.

4.4 *Communications and Engagement Team (C&ET)*

The Communications and Engagement Team (C&ET) are responsible for monitoring and managing corporate social media utilisation content and responses, as well as offering advice, support and training to staff to support this policy's effectiveness. They are responsible for referring any concerns received to the People Services team.

4.5 *The Head of Information Governance and Data Security*

The Head of Information and Data Security is responsible for the provision of expert advice and guidance in relation to social media incidents and potential breaches of relevant legislation.

4.6 *Approved Trust users of EEAST social media accounts*

It is the responsibility of those with authorised access to EEAST social media accounts to:

- Ensure that they maintain both their mandatory social media training and Data Protection & Information Governance Training.
- Highlight to C&ET immediately if they believe that their account has been hacked, cloned or otherwise compromised. This should be followed with an Incident form using the trust Datix system.

4.7 *Managers*

Managers are responsible for providing advice and guidance to staff on the application of this policy and general information governance. They are responsible for acting on any inappropriate social media content. This will include appropriate education and training and potential escalation where necessary.

4.8 *All staff*

All individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other

person associated with the Trust must comply with this policy, at all times.

It is important that everyone feels able to raise concerns and report any breach of this policy,; this should be undertaken through the range of speaking up channels available including through line management, HR, Freedom To Speak Up, and the incident reporting system (Datix).

All staff are required to complete the mandatory social media training on the Trust's on-line training platform.

4.9 *Consultation and Communication with Stakeholders*

This policy has been written in partnership by management and staff side, and in accordance with current employment legislation.

Consultation has included review by the Director of Corporate Affairs and Performance and the wider governance (and Information Governance) team, as well as review by the Culture Improvement Director.

5. Definitions

5.1 The world of social media changes rapidly and exponentially, it is therefore impossible to provide an absolute list of definitions that could apply to social media communications. The following section aims to provide any user with a basic understanding of the terms used by the Trust in regard to social media.

5.2 *Social Media:*

Social media is the term commonly used for internet based and mobile communications technologies that enable users to share dialogue and content with others.

Examples of popular social media platforms include (this list is indicative and not exhaustive):

- Social networking sites (e.g. Facebook, LinkedIn, Yammer)
- Microblogs (e.g. Twitter)

- Messaging boards
- Photo and video content sharing sites (e.g. YouTube, Instagram, TikTok, Flickr)
- Social messaging platforms (e.g. WhatsApp, Facebook Messenger, Microsoft Teams, Snapchat)
- Wikis (e.g. Wikipedia) Zoom

5.3 *Disrepute:*

To bring the Trust into disrepute may be defined as an action, image or statement that lowers the esteem of the organisation in thinking of society generally. An individual may bring the Trust into disrepute in the following ways (this list of examples is not exhaustive):

- posting content that is likely to lose the respect of the public, our partners and our staff and volunteers via its association with your content or actions.
- posting statements or responses to posts that may cause the Trust to lose respect and or damage the Trust's reputation within society.
- taking part in any social media activities that contravene any legislation in the world (e.g. incitement to commit a crime, threats of violence, radicalisation).

5.4 *Inappropriate content:*

The following are examples of inappropriate content (this list is indicative only and not exhaustive):

- sexually suggestive or explicit content
- sexual comments or jokes
- propositions and sexual advances
- making promises in return for sexual favours
- intrusive questions about a person's private or sex life or a person discussing their own sex life
- sexual posts or contact on social media
- spreading sexual rumours about a person
- sending sexually explicit communications
- images of violence/torture
- promoting or inciting hatred
- promoting or engaging with extremist websites

- content that contains or uses profanity and/or vulgar language
- content that could constitute bullying or harassment (including sexual harassment)
- comments and posts that could be perceived to be derogatory to any individual (i.e. the use of 'black face' as an image).
- images that contain graphic content (i.e. images of injuries, the deceased or harrowing scenes)

5.5 Malicious communication:

This may be defined as any communication sent by an individual or group to another person or group a that is, or could be perceived as, indecent, grossly offensive, obscene, threatening, menacing and/or intends to cause the recipient distress or anxiety.

5.6 Trolling:

Where a social network user writes a deliberately provocative post with the aim of inciting an angry response, usually with contents that are hurtful and/or personal.

6. Social Media Principles

Everyone has the right to be digitally engaged and use social media platforms. They also have the right to feel safe and be shown respect when using these platforms and connecting with others digitally. EEAST 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 so offers the potential to reach more audiences, EEAST has established official Facebook, Twitter, Instagram, LinkedIn and YouTube accounts to engage with its stakeholders.

6.1 Expected Standards of Use

The following standards should be applied when using social media. Treat all individuals, other social media users and organisations with respect, care, and courtesy.

- Be respectful to others when making any statement on social media and be aware that you are personally responsible for all

communications which are published on the internet for anyone to see.

- Make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal email address.

- If you disclose your affiliation with the Trust on your profile or in any social media postings, you must state that your views do not represent those of the Trust (unless you are authorised to speak on the Trust's behalf).

- The Trust recognises that social media groups (e.g. WhatsApp) with colleagues can be useful in regard to sharing information and having access to support and advice. However, any data that is shared via these forums must comply with this policy. Employees should consider if the data is appropriate to share via these forums. Administrators of any social media groups should be mindful of the provisions of this policy when selecting contacts and regularly review the contact membership to ensure that contacts should still be receiving data.

- If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your line manager.

- If you see social media content that disparages or reflects poorly on the Trust you should contact the People Services Team.

6.2 Prohibited use of social media

- You should never use social media in a way that breaches our other policies. For example, you are prohibited from using social media to:
  - breach our Dignity at Work policy.
  - breach our confidentiality obligations to patients and service users.
  - breach our Disciplinary Policy.
  - breach our Data Protection Policy.
  - breach any other laws or regulatory requirements.
  - breach of Safeguarding policies

- You must not use social media in a way that could damage the Trust's interests or bring it into disrepute, directly or indirectly.

- You must not use social media in a way that could damage the Trust's commercial interests.

- You must not use social media to:

    - defame or disparage the Trust, its staff, patients, service users or any third party;
    - harass, bully or unlawfully discriminate against staff, patients, service users or third parties;
    - make false or misleading statements about the Trust, its staff, patients, service users or any third party;
    - impersonate staff, patients, service users or third parties; or
    - create a security risk for the Trust.

- You must not publish or make comments on social media that could be considered inappropriate, indecent, obscene, lewd, graphic, slanderous, defamatory, pornographic, violent, abusive, insulting, threatening or malicious.

- You must not use social media for the purposes of trolling.

- You must not use social media to target / engage with children under the minimum requirement age for the social networking site you are using.

- You must not use social media to disclose any personal, sensitive or confidential information relating to the Trust, its patients, services user or staff.

- You must not create, promote or participate in (whether directly or indirectly) any group on social media (including, but not limited to, WhatsApp) which has the purpose of, or is used for, exchanging and/or sharing content which is prohibited under this policy.

- You must not include the Trust's logo, images or written content in any social media posting or in your profile on any social media.

- You must not express opinions on the Trust's behalf via social media, unless expressly authorised to do so by the C&ET.

- You must not imply you are authorised to speak on behalf of the Trust (unless you have the express authorisation of the C&ET).

- You must not use social media to disclose any information in relation to any incident being handled by the Trust without the express authorisation of the C&ET.

- You must not use social media in a way that breaches a platform's terms of use.

- You must not set up (directly or indirectly) any social media account (or attempt) that purports to be an official Trust account without the express authority of the C&ET.

  You must not use social media for publicly raising or escalating concerns. Such concerns should be raised in accordance with the Trust's Raising Concerns Policy.
  FTSU service: 07562 158013 / Direct line: 07729 108696

6.3 *Official EEAST social media accounts*

The C&ET is responsible for the management and governance of the Trust's social media accounts under the corporate banners of:

- @EastEnglandAmb (Twitter)
- EastEnglandAmbulance (FaceBook)
- EastEnglandAmb (Instagram and LinkedIn)

In some cases, social media accounts have been set up and delegated to certain departments and directorates with arm's length guidance and oversight from the C&ET.

To set up an official Trust account or to obtain permissions to post to an official Trust site an application must be submitted to the C&ET and approved (using the application form at Appendix C).

The administrative access (username and password) to these accounts will be held by C&ET. Such usernames and passwords must not be changed without consultation with C&ET. The C&ET have the Trust authority to access any account set up by EEAST, edit and delete as appropriate (either content or site).

No member of the Trust outside of the C&ET has the authority to post content to social media on a Trust account or on behalf of the Trust before they have received notification of approval from C&ET.

Official accounts of the recognised trade union will not fall under this policy, any issues shall be addressed through Staff Partnership Forum.

6.4 *Personal use of social media*

Occasional personal use of social media, including messaging apps (e.g WhatsApp) during working hours (e.g. breaks) is permitted, so long as it does not involve unprofessional or inappropriate content, does not interfere with your responsibilities or productivity and complies with this policy.

6.5 *Monitoring*

The Trust reserves the right to monitor, intercept and review, without further notice, your activities using our IT resources and communications systems, including but not limited to social media postings and activities, for legitimate business purposes which include:

- ascertaining and demonstrating that in using the systems you are meeting expected standards; and
- the detection and investigation of unauthorised use of the systems (including where this is necessary to prevent or detect crime).

All monitoring will be done responsibly and in compliance with information governance guidelines

7. Safe use of Social Media

The below is taken from the Health and Care Professions Council (HCPC) Guidance on Social Media

- Think before you post. Assume that what you post could be shared and read by anyone.
- Think about who can see what you share and manage your privacy settings accordingly. Remember that privacy settings cannot guarantee that something you post will not be publicly visible
- Maintain appropriate professional boundaries if you communicate with colleagues, service users or carers.
- Do not post information which could identify a service user.
- Do not post inappropriate or offensive material. – follow your employer's policy on use of social media. When in doubt, get advice. Appropriate sources might include experienced colleagues, trade unions and professional bodies. You can also contact the HCPC if you are unsure about the standards. If you think something could be inappropriate or offensive, do not post it.

Keep on posting! We know that many registrants find using social media beneficial and do so without any issues. There is no reason why you shouldn't keep on using it with confidence.

Do not engage in conversations with people of a sexual nature, unless you know who they are. Sexual conversations can be dangerous if you do not know who the person is and how old they are.

Be honest and trustworthy (taken from HCPC)
Our standards of conduct, performance and ethics say:
'You must make sure that your conduct justifies the public's trust and confidence in you and your profession' (9.1)

This means you need to think about who can see what you share. Make sure you understand the privacy settings of each social media channel that you use. Even on a completely personal account, your employer, colleagues or service users may be able to see your posts or personal information. It is best to assume that anything you post online will be visible to everyone.

Our standards of conduct, performance and ethics say:

'You must make sure that any promotional activities you are involved in are accurate and are not likely to mislead' (9.3)

If you use social media to advertise or share information related to your professional practice, you must make sure it is fair and true, as far as you know. You may choose to include a disclaimer on your profile that your views are your own, and that they do not represent the views of your employer or anyone who contracts your services.

8. Policy review

This policy will be reviewed on an annual basis or amended in the light of new employment legislation and/or relevant case law

Appendix A: Monitoring Table

What	Who	How	Frequency	Evidence	Reporting arrangements
Social Media casework	Head of HR	Trend reporting, including outcomes	Bi-Monthly	Reports to Group	Raising Concerns Forum
Social Media concerns	FTSU Guardian	Trend reporting	Bi-monthly	Reports to Group	Raising Concerns Forum
Corporate Account monitoring	Director of Communications and Engagement	Team monitoring of corporate feeds	Daily	Escalation reports	To People Services team
Social Media incidents	Director of Corporate Affairs and Performance	Trend reporting, including outcomes	Bi-Monthly	Reports to Group	Raising Concerns Forum

Appendix B: Equality Impact Assessment

EIA Cover Sheet	
Name of process/policy	Social media policy
Is the process new or existing? If existing, state policy reference number	Existing – POL078
Person responsible for process/policy	Director of Corporate Affairs and Performance
Directorate and department/section	Corporate Affairs and performance Communications and Engagement team
Name of assessment lead or EIA assessment team members	Emma de Carteret, Director of Corporate Affairs and Performance and Hein Sheffer, Culture Programme Director
Has consultation taken place? Was consultation internal or external? (please state below):	Internal Consultation taking place in relation to the amendments to the policy, including: • Chair of People Engagement Committee • Information Governance Team • Staff Network leads • Communications and Engagement team • HR policy Group • Staffside representatives • Freedom to Speak Up Guardian
The assessment is being made on:	Guidelines

Equality Analysis
What is the aim of the policy/procedure/practice/event? To standardise the way in which all staff and volunteers utilise social media and digital communication platforms. To clarify responsibilities and ensure that inappropriate use, including harassment and bullying of individuals and groups does not occur.
Who does the policy/procedure/practice/event impact on? Race X Religion/belief X Marriage/Civil Partnership X Gender X Disability X Sexual orientation X Age X Gender re-assignment X Pregnancy/maternity X
Who is responsible for monitoring the policy/procedure/practice/event? Joint monitoring between the Communication and Engagement team and the People Services team
What information is currently available on the impact of this policy/procedure/practice/event? ER casework data on social media cases
Do you need more guidance before you can make an assessment about this policy/procedure/ practice/event? Yes – too early to assess the positive impact of the policy on social media misuse
Do you have any examples that show that this policy/procedure/practice/event is having a positive impact on any of the following protected characteristics? Yes/No, If yes please provide evidence/examples: Please provide evidence: Race, Religion/belief, Marriage/Civil Partnership, Gender, Disability, Sexual orientation, Age, Gender re-assignment, Pregnancy/maternity. Evidence within the ER casework and Freedom to Speak Up that inappropriate utilisation of social media has resulted in detriment and

harm to a range of staff, in particular racial and sexualised content in line with the protected characteristics under the Equality Act. As a result the policy has been strengthened to better define the requirements and responsibilities, including action to be taken in instances of inappropriate utilisation.
Are there any concerns that this policy/procedure/practice/event could have a negative impact on any of the following characteristics? No: Please provide evidence: Race X Religion/belief X Marriage/Civil Partnership X Gender X Disability X Sexual orientation X Age X Gender re-assignment X Pregnancy/maternity X The policy seeks to ensure that discrimination does not occur through social media channels. It supports the dignity at work and disciplinary policies and clarifies the approach to take; as such, the policy should positively impact on protected characteristics
Action Plan/Plans - SMART Specific Measurable Achievable Relevant Time Limited
Evaluation Monitoring Plan/how will this be monitored? Who How By Reported to

Appendix C

EEAST Social Media Account Application Form

Please complete the following application form to submit your interest in having an official EEAST social media account. This will then be reviewed by the Trust's communication team who will determine if there is enough justification for the application to be accepted. If you have any questions, please contact communications@eastamb.nhs.uk.

All Trust social media accounts must have sign off by two directors or heads of department, one from the relevant area and the other will be the director of communications (these will be sourced via the communications team after initial application).

Your details:

Name:

Job Title:

Email Address:

Your application:

About the account	
Intended social media channel	☐ Twitter Sub-Account ☐ Private Facebook Group
Proposed account name / social handle	(e.g. EEAST AOC Virtual Crew Room / @EEAST_AOCs)
Accountability and responsibility	
Department / team	(e.g. AOC)
Account owner (Full name, job title and email address)	(Who is in charge of the account primarily? For group accounts we ask that one member of the team take

	responsibility for the account and its content)
Who will have access to the account? (Full name, job title and email address)	(Who will have access to the account? Will it be a group of people with access to the account or just one person?)
What experience do your intended social media users have on a 0-10 scale (10 being the most efficient)?	
Why do you wish to have a social media account for us?	(What is the main aim/s of the account)?
Does anyone who will be using the account require further training?	
Please confirm that all staff with access to the account have read, and will abide by, the Trust social media policy and guidance document.	
Who is the head of directorate for this request?	
Has your head of directorate approved this request?	
Strategy	

Who is your target audience?	(Who are you trying to reach?)
What agreed business objective(s) does this initiative support?	
What benefit or perspective will this account offer the Trust that we don't have already? **Please give as much detail as possible on how you will use the social media account and what content you plan to post.** **Have you identified any risks in your use of this channel? Please detail the risks and mitigation.** **Please explain why think the proposed account would have longevity?**	
Resourcing – monitoring and responding	
What is the planned frequency of posts/tweets per week?	
How often do you plan to check the activity of this account?	

What is your strategy for responding to questions and comments?	
What tools do you intend to use to monitor the account/s?	
Timescales	
Proposed launch date	
How long will the account be required for?	

Before submitting this application form, please ensure you have read through our social media and digital policy and our Twitter account guidance documents.