West Midlands Ambulance Service
University NHS Foundation Trust

SOCIAL AND DIGITAL MEDIA POLICY

DATE APPROVED:	25 May 2021
APPROVED BY:	Executive Management Board
IMPLEMENTATION DATE:	May 2021
REVIEW DATE:	April 2024
LEAD DIRECTOR:	Communications Director
IMPACT ASSESSMENT STATEMENT:	No adverse impact on Equality or Diversity

Document Reference Number:	Policy – 024 (Version 2.2)

Trust us to care.

Change Control:

Document Number	Policy - 024
Document	Social and Digital Media Policy
Version	2.2
Owner	Communications Director
Distribution list	All Staff
Issue Date	May 2021
Next Review Date	April 2024
Author	Communications Director

Change History:

Date	Change	Comment/Approved by
June 2013	Draft created	Senior Press Officer
24 September 2014	Sent for comment – work needed	TU Policy Group
21 January 2014	Agreed subject to a few changes - agreed	TU Policy Group
22 January 2014	Sent for approval - agreed	Regional Partnership Forum
10 April 2014	Sent for approval and implementation – agreed	Workforce & Organisational Development Committee
April	Reviewed no changes	Communications Director
04 May 2016	Presented and agreed no changes	Policy Group
October 2016	Agreed no longer sits with HR	Director of Workforce & OD
25 October 2016	Sent for approval – agreed	Executive Management Board
09 November 2016	Sent for information only – approved	Regional Partnership Forum
Renumbered from HR-Policy-030		
June 2017	Twitter Account Guidelines updated	Press Officer
Renumbered from PC – Policy – 001 due to change in referencing		
April 2020	12-month extension	Executive Management Board
March 2021	Draft of Version 2.2	Communications Director
8 April 2021	Agreed following changes	Policy Group
20 April 2021	Agreed	Executive Management Board
25 May 2021	Agreed	Regional Partnership Forum

CONTENTS

1 Introduction

1.1 Social media is a term commonly used for web-based tools available on the internet that allow people to interact with each other by sharing information, knowledge, opinions and interests.

Examples of social media sites include but are not limited to:

- Social networking sites (eg Facebook, Twitter, Instagram, TikTok, Snapchat)
- Blogs and personal websites
- Messaging boards
- Photo and video content sharing sites (eg YouTube, Pinterest, Flickr, Tumblr)
- Business sites (e.g., LinkedIn, WhatsApp)
- Microsoft Teams
- Zoom

1.2 This list is not exhaustive as social media is a constantly evolving area and the types of social media available changes over time.

1.3 West Midlands Ambulance Service University NHS Foundation Trust (WMAS / The Trust) uses social media as part of its communication strategy. The communications department has authority to speak on behalf of the Trust and is responsible for managing the Service's official sites, including Facebook, Twitter, Instagram, LinkedIn, Wordpress, and YouTube.

1.4 Social media, like other communication tools, is used to improve the public's understanding of the Trust and its work, promote health, and engage with the general public and groups that are often known as 'hard to reach'. When using social media sites, the communication department will, on behalf of the Trust, ensure it:

- is respectful towards patients, members of the public and Trust employees
- does not reveal confidential or sensitive information about patients, staff or the Trust
- is transparent
- updates the channels on a regular basis and responds to users posts
- consideration should be given to the impact that a live social media posts could have on patients and relatives.

1.5 The communication team adheres to all Trust policies and procedures when using social media and ensures that the organisations official social media sites are kept updated at all times.

1.6 The Trust does allow access to social networking sites from work computers. It is also recognised that many staff use these sites on personal devices such as smart phones.

1.7 Members of staff may choose to identify themselves as working for the Trust through words, pictures or videos and/or discusses their work on a social networking site. Even if staff choose not to, they must remember that they may be identified online as Trust employees through a general understanding within their online network of family, friends and associates and 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. Whether they identify as a member of staff or not, they must act in a way that respects confidentiality and protects patients, members of the public. This is in line with current HR policies, HCPC registration (if applicable) and also reduces the chances of bringing the Trust and themselves into disrepute.

2 Purpose

Purpose of the document:

- To help staff understand their responsibilities when using social media and the legal implications involved.
- To illustrate where problems can arise for individual staff members and the Service.
- To differentiate between using a personal social media account and an official WMAS account.
- To maintain UK GDPR and Caldicott Principles.

3 Scope

3.1 This policy applies to all 'staff' who are directly employed by the Trust; by this we mean staff in substantial positions, bank staff, students (internal and external) and volunteers such as CFR's. This is in line with the Volunteers Agreement that is signed by all volunteers.

3.2 The policy sets out the responsibilities of staff when using social media and the legal implications involved. It is not intended to stop individuals from using social media sites in their own time, but to outline some areas of best practice and illustrate where problems can arise.

4 Objectives

The objectives of this policy are to enable staff:

- to understand their responsibilities when using social media and what should, and should not, be written or posted
- to highlight the potential risks involved when posting on social media
- to document the Trusts intentions for the use of social media
- to understand the implications of malicious intent of using social media inappropriately
- to know where they can go for further advice.

5 Responsibilities

All employees and volunteers have a responsibility to follow the principles set out in this policy. Anyone who is found to have breached them may face action in line with the Trusts Investigation Policy. In particular, staff should ensure that they know Trust policy on patient confidentiality, the Caldicott Guardianship scheme and follow these at all times.

6 Principles

6.1 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 use could damage their own reputation and that of the Trust.

6.2 When a member of staff identifies their association with the Trust – for example, by stating they work for the West Midlands Ambulance Service or posting pictures of themselves in uniform or at work - and/or discusses their work, they are expected to behave professionally, and in a way that is consistent with the organisation's policies and procedures.

6.3 Even if a staff member does not directly associate themselves with the Trust, their link with the organisation can become known through images on friends' sites or on the Trust website, or by someone searching for names via internet search engines.

6.4 When using any social media channel staff should follow the principles outlined below;

6.4.1 Use Social Media

Staff should only use personal social media when it does not interfere with fulfilling their job requirements or their commitments to the Trust, patient's and colleagues.

6.4.2 Make it Clear Opinions are your Own

If a member of staff discloses that they work for the Trust or can be identified as an employee through association with other people, they should ensure their profile and related content is consistent with how the Trust would expect them to present themselves to colleagues and business contacts.

6.4.3 Staff should also make it clear that their views are their own, not those of their employer. However, the use of a disclaimer does not override the need to follow other principles in this policy and does not eliminate the possibility of action under the disciplinary policy.

6.4.4 Communicate as Yourself

If a member of staff associates themselves with West Midlands Ambulance Service on their social media site, they are expected to post under their real name. This demonstrates openness, honesty, and accountability.

If an employee posts under a pseudonym and at a later stage these posts are associated with their real name, all previous posts will be admissible in a disciplinary investigation or hearing. This is in line with the Malicious Communications Act 1988 which carries a maximum fine of £5,000 or a 2-year custodial sentence.

6.4.5 Respect Others

Individuals must not post anything contrary to the Trusts policies on equality, diversity and inclusion. Anything containing racist, sexist, homophobic, sexually explicit, threatening, abusive, disrespectful or other unlawful comments must not be published.

Take care not to speak or act in a way that could reasonably 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 as well as comments about individual Trust employees.

Staff should seek permission from colleagues before posting personal details or images that may link them with the Trust and should not post anything about someone if they have been asked not to in line with UK GDPR. Staff must always remove information about a colleague if they have been asked to do so.

6.4.6 Be Aware of how Online Posts are, or Can Become Public

Staff should be aware of privacy limitations when posting material using social media, and the extent to which information can be in the public domain. Whatever is posted on a social media site could be in the public domain immediately or, if initially shared with a limited group of followers or friends, could still be copied and shared or published elsewhere.

Staff should carefully consider what they want to say before they publish anything, and work on the basis that anything they write, or post could be shared more widely without their knowledge or permission.

Individuals should be aware that their statements could be picked up and be portrayed in a manner that suggests they represent the Trust. Such posts could impact on colleagues or bring the Trust into disrepute.

Staff should configure their privacy settings and review them regularly as:

- social media sites cannot guarantee confidentiality, and do change settings
- the public, employers or any organisation staff they have a relationship with, may be able to access their personal information
- once information is online, it is almost impossible to remove it completely.
- Social media sites provide information on how to check your security settings.

6.4.7 Staff should be careful when sharing or retweeting posts, as they could be seen to be endorsing someone else's point of view.

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 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

6.4.8 **Get your Facts Right**
When posting information, staff must ensure it is factually correct. If they discover they have posted something incorrectly, they should amend it and make it clear they have done so.

6.4.9 **Ensure Comments are Legal**
All comments must be legal and must not incite people to commit a crime. Staff must be aware that comments on social networking sites are still covered by British Law, even if posted using a pseudonym. Comments can still result in legal action from an individual or Police prosecution. This is in line with the Malicious Communications Act 1988.

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.

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 social media activity which has caused concern by any employee, it reserves the right to investigate the matter fully.

6.4.10 Understand the implications of Defamation of Character

Staff could face legal proceedings for posted comments aimed at named individuals or an organisation that are considered to harm reputation.

6.4.11 Respect Copyrights

Staff need to be aware that all photographs are protected by copyright. Individuals should check with the owner before using them. If staff wish to use any Trust photographs, please contact the Communications team.

6.4.12 Be careful when talking about work-related issues

Staff should only share information about the Trust that is in the public domain and should not add derogatory comments on these issues. Staff must also respect patient confidentiality and should not disclose information that could identify a patient. See section 6.4.14 & 6.4.15 – Protect patient confidentiality.

6.4.13 Don’t bring yourself or the Trust into disrepute

Staff should not air grievances or publish anything that risks bringing the Trust into disrepute. Naming and making derogatory comments about others, including but not limited to; members of staff; management; volunteers; and patients could result in action under the disciplinary policy.

You must not use a Trust account to promote suppliers or commercial companies. This includes any marketing activity or anything that would be perceived as an endorsement unless this is approved by the Trust Communications Team.

6.4.14 Be careful about the use of photos

If staff post any photos of themselves or colleagues in uniform, or in an identifiable work setting, they must ensure that these represent a professional image of the Trust. Any comments made must also reflect professionalism.

Staff must not post images containing patients or any information that could identify a patient on personal social media accounts unless they have written permission from the patient to do so. They should also not post images of any incidents on any personal social media sites. This does not prevent staff sharing, retweeting or linking to images that have been published on official Trust sites.

6.4.15 Confidentiality must be respected by anyone who posts anything about their work on the internet, and under no circumstances should anything be posted that identifies a patient. Staff should ensure they know the Trust policy on patient confidentiality and follow it at all times.

This NHS Code of Practice states that all NHS staff have a duty to keep confidential all information about patients, and to not disclose this information to anyone not involved directly in their care.

It is generally accepted that information provided by patients to the health service is provided in confidence and must be treated as such.

Obligations of confidentiality apply to all patients including the deceased.

It is Trust policy to gain written consent from patients for all disclosures of identifiable information to the media and for publicity purposes. As well as names and other personal details, this includes the use of images of the patient undergoing treatment in a real-life situation and where the patient is posing for a picture; and the release of taped 999 calls.

Individual consent from staff must also be sought for the release of recording of 999 calls.

The following is patient-identifiable information and should not be disclosed:

- Patient’s name, address, full postcode or date of birth
- Pictures, photographs, videos, audiotapes or other images of patients
- NHS number and local patient identifiable codes
- Anything else that may be used to identify a patient directly or indirectly. For example, photograph of house in street, rare diseases, cars, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

The Department of Health & Social Care definition of anonymised information is “information which does not identify a patient directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full postcode and any other detail or combinations of details that might support identification.”

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.

6.4.16 Indirect Breaches of Confidentiality

Nothing written by staff should comment on, or provide additional information about, cases already in the public eye – for example, any incident that has already been reported in the media.

While individual pieces of information may not alone breach patient confidentiality, the sum of published information online could be sufficient to identify a patient through a 'jigsaw' process. In cases where an incident becomes public knowledge after information has been posted, the member of staff should consider whether the published details could now be considered to be breaching the patient's confidentiality and, if so, remove them.

6.4.17 Respect Safeguarding Issues

The Trust's Dignity at Work Policy and Procedure around Bullying and Harassment 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.

All employees are expected to treat their colleagues with respect and dignity and must ensure their behaviour does not constitute bullying and/or harassment Posts made by staff must not encourage behaviour that could be linked to safeguarding issues, for example:

- Bullying
- Luring and exploitation
- Theft of personal information
- Encouraging self-harm or violence
- Glorifying activities such as excessive drinking or drug taking

These kinds of posts may be investigated and result in disciplinary action and potentially legal action.

6.4.18 Adhere to other Services Policies and Procedures

Staff using social networking sites should always adhere to codes of conduct and policies which are part of their professional and employment requirements. These include:

- Professional code of conduct (e.g., Health Care Professions Council)
- Other codes of conduct (e.g., confidentiality clause in your contract)
- Relevant trust policies, including: Code of Conduct, IM&T Use of Trust Computers, Caldicott Guidelines.

7 Staff with Authorised Access to Social Media Sites for Work Purposes

Some staff are authorised to access social media sites either for monitoring purposes, or to post information on behalf of the Trust. Staff who are given access to social media sites such as YouTube, Twitter and Facebook for work purposes must:

- only use these sites in an ethical and lawful manner – subject to the same principles as above, such as patient confidentiality, not bringing the Service into disrepute and not posting sensitive information.
- not access their personal accounts – such as Facebook, Twitter and blogs, unless it is for the benefit of the Service
- make total separation between their personal accounts and any accounts monitored or updated on behalf of the Service.

7.1 Some staff are using twitter as part of their daily work under a scheme being run by the Communications Department. This involves the Trust communications team setting up an official account for that staff member and them using it to communicate with the public about their role in the ambulance service.

7.1.1 No staff member will be able to tweet using an official account until they have met with a communications' team member and had an introduction to twitter, how and when to use an official account, and also gone through the dos and don'ts of using an official account.

7.1.2 At no time will using twitter be allowed to take priority for the staff member; their treatment of patients and the 'day' job will always come first.

7.1.3 All usernames and passwords will be held by the communications team and the staff members tweets can be accessed, edited and even deleted at the communications team's discretion.

7.1.4 Please see Annex A which is the Association of Ambulance Chief Executives NHS Ambulance Social Media Guidance Document which sets out best practice for those with corporate social media accounts.

8 Being Harassed, Bullied or Victimised via a Social Networking Site?

If a staff member believes they are being harassed, bullied or victimised as a result of another member of staff's post to an internet or social media site, they should take action by accessing the Trusts Dignity at Work policy which outlines the informal and formal action that can be taken.

The Trust will not tolerate any member of staff being harassed, bullied, victimised intimidated by any member of staffs posts on social media. Staff are encouraged to report such issues as per the dignity at work policy.

Alternatively, reporting the incident to the police or to the social media site is also an option open to the individual.

If a third party feels that a staff member is being bullied or harassed on social media sites, the this can be reported using the Raising Concerns Policy (Freedom To Speak Up Policy).

Staff should be aware that all comments made on social media can be investigated by the Police under the Malicious Communications Act 1988.

9 Misconduct

Any member of staff found to be using social media sites inappropriately, as outlined in the principles above, may be subject to disciplinary action and will be managed in line with the Trusts Investigations Policy.

10 Further Information & Advice

Any staff who are in any doubt about what they should or should not post on social media sites – particularly about their work – or who discover online content that may harm the reputation of the Service, should contact the Communications Department by email to: pressoffice@wmas.nhs.uk or by calling 01384 246 496. Their call will be taken in the strictest of confidence.

If a member of staff is contacted by the media about anything Trust-related they have written or to request other information or an interview, they should contact the communications department using the above methods.