Social Media Policy

Version	Issue Date	Review Date	Document author	Reviewed by
1.0	October 2020	October 2022	Richard Moremon, Head of Communications	

Contents

==

1.0 Introduction

University Hospitals Dorset NHS Foundation Trust ('The Trust') recognises the value in social media for both the Trust and staff. The Trust encourages the use of social media as a way to celebrate our staff and their achievements, to share best practice and to engage with patients and the general public. The Communications Team represents the Trust online, acting as a facilitator, sharing updates and generating conversation. Staff are encouraged to participate on social media in a constructive, considered and positive manner.

2.0 Purpose and Principles

The trust recognises that social media can be a useful tool for networking with colleagues and provides a forum for the sharing of ideas and best practice. However, we must also ensure that confidentiality and the reputation of the trust are protected.

The purpose of this policy is to provide staff with clear guidance on their responsibilities and the potential implications when using social media. This policy outlines the principles which staff should follow when accessing social media for professional and private use highlighting to employees the actions that could be deemed to be inappropriate use of social media sites within and outside of the trust to avoid any breaches of trust policies or procedures. This will prevent damage to the trust's or the individual's reputation, which may be caused by inappropriate use of these sites.

The trust respects every employee's right to a private life and appreciates the benefits of social media sites. However, inappropriate use of these sites may bring the trust into disrepute and give rise to risks of legal claims against the organisation, which is vicariously liable for the actions of its staff. Employees need to be aware of their responsibilities as a member of the trust and this policy outlines these responsibilities.

3.0 Policy Scope

This policy is based on the NHS best practice guidelines and guidance from the NHS England, the British Medical Association (BMA), the General Medical Council (GMC) and the Nursing and Midwifery Council (NMC) on the use of social media and outlines the trust's expectations for online interactions, as well as the consequences of breaching the policy. This document does not form comprehensive guidance on how to use individual social media platforms and online tools. This policy applies to all staff, contractors, volunteers, and students working on behalf of the trust (hereafter referred to as 'staff').

This policy should be read in conjunction with the Email and Internet Use Policy, Information Governance: Code of Conduct for Employees in Respect of Confidentiality, IT Users Policy, Dignity at Work Procedure, Staff Discipline Procedure and the Mobile Computing Device policy. It should also be read in conjunction with the guidance on social networking provided by relevant professional registration bodies (see section 5.2).

Social media is rapidly evolving and expanding, and new platforms are regularly launched. Current blogging and social networking sites or applications include but are not limited to:

		Description	UK Users	Total Users	Useful information
	Facebook:	A social sharing networking site.	35,130,000	2,417,000,000	Highest traffic occurs between 1-3pm, however more engagement can be found between 7-8pm
	YouTube:	The top website used for video uploading and viewing.	23,000,000	1,900,000,000	1 billion hours of Youtube are watched daily
	WhatsApp:	Platform that allows users to send text messages as well as voice and video calls.		1,500,000,000	55 billion messages are sent each day on the platform
	Instagram:	A photo and video sharing social networking.	14,000,000	1,000,000,000	95 million posts are shared each day on Instagram
	Twitter:	A Micro-blogging platform.	13,000,000	883,000,000	Year-on-Year the total ad engagement rate was up to 91%
	Tik Tok:	App that allows users to create and share short 15 second videos.		800000000	The young demographic of Tik Tok sees users have spent spend almost an hour on the app every day.
	LinkedIn:	B2B platform for networking professionally.	20,000,000	590,000,000	More than 50% of all social traffic to B2B sites and blogs comes from LinkedIn
	Snapchat:	Send images and videos with a short life span over an app.	16,200,000	600,000,000	528,000 Snaps are shared every minute
	Tumblr:	A popular microblogging platform used to broadcast messages.	9,000,000	550,000,000	45% of Tumblr's audience is people under the age of 35
	Reddit:	An entertainment, social news and social networking website.	6,600,000	330,000,000	The average time a Reddit user spends on the site is 16 minutes
	Skype:	Telecommunications application that provides video and voice calls via the Internet.		300000000	The mobile app has been downloaded over 1 billion times
	Pinterest:	A popular photo sharing website.	10,300,000	266,000,000	50% of users have made a purchase after seeing a Promoted Pin on their feed
	Flickr:	An image hosting website used to showcase photography work.		112,000,000	On a high traffic day, Flickr users upload around 25 million photos
	Vimeo:	A video uploading and sharing website.	412,085	80,000,000	Vimeo gets 715 million monthy video views

Source: https://social-media.co.uk/list-popular-social-networking-websites. Statistics correct as of 2020.

Inappropriate use of social media by any member of staff which breaches the terms of this policy may result in disciplinary action up to and including dismissal from employment being taken.

4.0 Definitions

4.1 Social Media
'Social media' is used to refer to applications or websites that enable users to create, share and comment on content, and participate in social networking.

4.2 Social Networking
'Social networking' is used to describe the use of applications or websites to connect and interact with other users by sharing information, opinions, knowledge and interests. This applies to all forms of online publishing and discussion, including blogs, wikis, file-sharing, user-generated video and audio, virtual worlds and social networks. For clarity on any of the terminology used throughout this policy, please

contact the communications team (communications@uhd.nhs.uk)

5.0 Relevant Legislation

UK statute does not deal directly with the issue of social media. Some of the legislation, however, is relevant.
- The Human Rights Act 1998, which provides that employees have the right to private and family life, a right that can be extended to include privacy in the workplace. Article 10 of this Act states the right of everyone to 'freedom of expression'.
- The Regulation of Investigatory Powers Act 1998, which details the extent to which employers can monitor or intercept employees' communications.
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, which permit the monitoring of emails, telephone communications and usage of the Internet in certain circumstances.
- The Data Protection Act 1988, which deals with the processing of individual data and the monitoring of email communications. The Information Commissioner has produced an Employment Practices Code, which also provides guidance on monitoring communications and on breaches of the Data Protection Act 1998.
- The General Data Protection Regulations (GDPR) 2018 was passed on 25 May 2018 in the UK. It will help organisations understand the new legal framework in the EU as well as explaining the similarities with the UK Data Protection Act 1998, and describe some of the new and different requirements. For instance, it makes it clear that information such as an online identifier like an IP address can be personal data.
- Misuse may also involve breaches of the Equality Act 2010 while any dismissal for misuse will have to meet the test of fairness in the Employment Rights Act 1996 (ERA 1996).

Employees need to be aware that although they may believe they have restricted access of their online profiles to their 'friend' list and their postings do not mention the employer these are 'safe'. They are not, and are sufficiently public for employees to be under a duty to their employer to watch what they post. If an employee's actions result in their employer being brought into serious disrepute, this can lead to disciplinary action, including dismissal for gross misconduct, even where their profile states their views are their own. See Section 8 of this policy for more information.

Alongside this policy, guidance on the use of social media is provided by various professional members' organisations and registration bodies. It is the responsibility of staff to read and understand the relevant guidance for their professional and regulatory body, and to ensure that all their social media activities comply with the guidance in this policy.

6.0 Training
The communications team (communications@uhd.nhs.uk) will direct you to guidance and training wherever possible and will help empower staff to make their online interactions honest, consistent, transparent and relevant.
The trust will increase general awareness of the risks associated with social networking through the mandatory Information Governance training provided to all staff. This will help to maximise compliance with patient confidentiality and information security requirements.

7.0 Benefits of Social Media
Used properly, social media represents for individuals and the trust:
- an opportunity to increase direct contact with a range of stakeholders and more widely with audiences we have not traditionally reached via traditional communication channels
- a powerful way of interacting on a regular basis with key stakeholders
- a means of publishing information swiftly rather than relying on the traditional print and broadcast media schedules
- a way of highlighting relevant information available elsewhere from the Trust and/or the health and social care sector
- an opportunity to publicly support other health and social care providers by 'liking', sharing or re-tweeting information
- increase effectiveness of internal communication by using social media as an alternative internal channel
- a useful recruitment tool that can attract a new pool of potential employees to the trust
- improving the standing and coverage of the trust through users of alternative media channels who wouldn't necessarily visit our website
- video sharing platforms can showcase the trust in an exciting and engaging visual capacity
- social media is a platform that the public can use to provide feedback and praise the work of staff.

8.0 Corporate use of social media
Social media sites can present an opportunity for NHS organisations to engage, interact and communicate with key stakeholders. Used appropriately for professional purposes, they can improve our effectiveness and form a valuable tool in collaborative working, professional networking, recruitment, marketing and stakeholder engagement.

8.1 UHD corporate sites
University Hospitals Dorset NHS Foundation Trust maintains a corporate presence on the following social media channels (correct as at October 2020):
- Twitter: @UHD_NHS
- Facebook: @UHDTrust

- YouTube: https://www.youtube.com/user/BournemouthHospital
- Instagram: @UHD_NHS
- LinkedIn: University Hospitals Dorset NHS Foundation Trust

8.2 Establishing an official presence online

Anyone wishing to establish an additional official University Hospitals Dorset presence on social media e.g. team, department or clinical area, must, in the first instance, seek advice on the proposal from the communications team. The communications team will look at proposals in the context of the organisation's communications and social media strategies and will advise on the considerations surrounding an official presence, such as the time and resources required, adherence to the NHS identity, linking activity to an overall business plan, timeframes, evaluation tools, and ensuring accounts are based on stakeholder research.

Before any official presence can be established, a business case must be prepared that outlines how the activity will benefit the organisation and how that compares to the resource needed to maintain a presence. There must be clear evidence that there is a demand for engagement from a particular audience via the proposed channel and that the demand could not be met in another way or using existing official social media accounts. If intended to be accessed remotely, provision must also be made for a trust-managed device (e.g. iPhone) to be purchased as no official social networking accounts are to be accessed by staff using their own devices.

Subject to business case approval, new accounts must be approved by the communications team who will make a decision using the following criteria:
- objectives must be clearly defined and must link to the organisational objectives
- their introduction would not weaken the corporate trust social media accounts by diluting followers/supporters.
- measures and timeframes must be clearly defined. For example, how will the success of the account be determined and monitored, how regularly will the account be updated and new information shared.
- accounts must be based on clear evidence of audience needs and not on hearsay or presumption.
- other departments or other trusts having similar accounts will be not considered a good reason alone, there must also be evidence of a specific need for a new UHD account
- a content plan must be in place, as must a plan to communicate with stakeholders on an ongoing basis.
- niche, specialist audiences need to be reached/can be reached through this platform.
- there must be designated staffing and time to check on the account several times a day

- accounts must not be singularly used to promote internal, staff to staff communications
- account logins must be shared with the communications team

Please be aware that the communications team may close accounts for the following reasons:

- inactivity – if no original posts have been made for one month or more
- frequency – if there is more than one occasion where there have been less than three tweets/posts a week over a two-month period
- interest – if an account has not been active for two months or longer
- growth – If the account fails to reach 200 followers after being active for six months
- relevance – if the reason for the account is no longer relevant, e.g. if a service closes or a campaign ends.
- governance – if the account violates this or any other trust policies, or logins aren't shared

8.3 Principles
- uphold the trust values at all times when online.
- use common sense when determining whether something is appropriate when engaging online. If discussing work-related issues online, exclude conversations about patients or complaints about colleagues. Even when anonymised, these are likely to be inappropriate.
- you are personally responsible for any content you publish on social media, blogs, or any other form of online communication. All content, not limited to corporate use or purpose, is considered to be in the public domain, even if posted in private groups.
- be aware that what you put online will be accessible for a very long time and that deleting content does not always ensure it cannot be seen. Once online, information can be copied and redistributed, and it is easy to lose control of it.
- when online, use the same principles and standards that you would apply when communicating offline with people you don't know. If you wouldn't say something in an email or formal letter, don't say it online.
- be aware of how comments and images online can impact on your professional standing – in addition to this policy ensure that you are aware of and comply with any professional codes of conduct.
- protect your own privacy through the use of appropriate privacy settings.
- normal laws, such as those regarding libel, fair use, defamation, financial disclosure, copyright, equality and diversity etc, apply online. If you are unsure, check before you post or share anything online.
- making information such as your date of birth and other personal details publicly available could make it available to criminals for the purposes of identity theft.

- act in a transparent manner when altering online sources of information. If you make a mistake on social media, correct it immediately. If you change a post, indicate that you have done so and if you have caused offence, make sure you apologise.
- be aware that people who join your networks may be colleagues, patients, journalists or suppliers. It's also possible that people may not be who they say they are and you should bear this in mind when using social media and participating in online activities.
- if you are discussing Trust matters, ensure you are allowed to do so and you aren't sharing confidential information. If in doubt, check first, either with your line manager or with the communications team. Give your name and where relevant, job title, and always write in the first person. Be clear that you are not speaking on behalf of the organisation.
- you must not use our Trust logo on any accounts or websites without clearance from the communications team.
- never use social media to attack or abuse anyone, including colleagues. Do not use obscenities or engage in any conduct that would not be accepted in the workplace.
- show consideration for other's privacy and exercise caution and sensitivity when discussing controversial topics.
- blogging or participating in online activity for commercial or personal gain could constitute a conflict of interest. You should refrain from entering into any online social networking activity for gain without first reading the Trust's Managing Conflicts of Interest Policy.

9.0 Non-Corporate Use of Social Media

Staff already act as ambassadors for the trust online and are a great asset. Many staff are already using social media for both personal and professional reasons. This is not something the Trust wishes to discourage; instead social networking is embraced as part of a culture of openness.

9.1 Social Media Usage while at Work

Staff are encouraged to use social media during work time to contribute to their work as an employee of the trust – e.g., to share best practice, as a tool for discovering best practice and to check for important updates or news from the Trust.
The trust allows the use of the internet by staff in their own time (i.e., during authorised breaks) while at work. This policy also applies to staff using their own personal mobile devices to access the internet during authorised breaks.
Staff must make sure the use of social media does not interfere with the performance of their contracted duties or the ability of others to use PCs, laptops or devices for work-related matters, whether using during work time or their own time. They must also ensure all usage is in accordance with this policy and the 'Email and Internet Use Policy'.

9.2 Social Media Usage Outside of Work

Should your personal profile settings include reference to University Hospitals Dorset NHS Foundation Trust (including reference to Royal Bournemouth, Poole or Christchurch hospitals); this will identify a clear link to the organisation. Note that by referencing the trust in any personal social media updates could demonstrate that you have links to the trust and wider NHS. Particular caution is advised where staff have identified they work for the trust or the NHS. Staff are expected to interact online in ways that are consistent with NHS and trust values and policies. An employee's conduct outside of their employment with the trust may be subject to action under Disciplinary Policy and Procedure if considered by the trust to be relevant to their employment, or liable to bring the Trust into disrepute.

If anything is communicated online that could be perceived as having a connection to the trust, staff must make it clear they are sharing their own views and are advised to display a disclaimer such as: 'My postings on this site reflect my personal views and do not represent the positions, strategies or opinions of my employer.' The use of a disclaimer does not override the need to follow other principles in this policy.

9.3 Groups and Instant Messaging Services

The trust recognises the value in social networking instant messaging services (such as WhatsApp, Facebook, Snapchat, etc.) as a way for staff to communicate. However, the current services on offer do not meet NHS information governance standards for the transmission of confidential information and their use for this purpose has been explicitly banned by NHS Digital. Staff must not use instant messaging or private groups to share personal/confidential information about patients – any breaches of this will be met with disciplinary action. Even when set to 'private', these groups are not secure and discussions in such forums should be treated with the same caution and adherence to trust policies as discussions clearly in the public eye. Instant messaging services may be used by departments for purposes which do not relate to patients or breach confidentiality rules, such as for sharing best practice articles with colleagues, filling shifts at short notice, arranging social events, etc. If you are unsure whether a topic is appropriate for discussion via this medium, please check with communications or information governance first.

10.0 Roles and Responsibilities

The Trust aims to protect all staff from bullying and harassment including inappropriate behaviour from social networking sites. The Trust has a duty to protect the confidentiality of its patients and service users.

10.1 Members of Staff

A useful 'rule of thumb' is to say nothing in social media that you would not say in a face-to-face conversation with a fellow colleague/professional. Employees should take responsibility for what they post on social media and social networking sites and follow the guidelines set out within this policy. Employees should report any

inappropriate behaviour that they believe contravenes this policy to their Line Manager, Human Resources or the IT Department. Use of social media and social networking in a personal non-work-related capacity should not be undertaken during paid time.

<u>10.2 Line Manager</u>
Line managers should ensure that all new starters are aware of this policy and promote awareness of it within their individual departments. Line managers should investigate any allegations of misuse of social media and social networking sites in accordance with the trust's Staff Discipline Procedure, liaising with HR and Information Governance Departments as required.

11.0 Use of Social Media by Patients and Visitors
It is recognised that patients and their visitors will make use of social media while in our hospitals. It is important that patients and their visitors are respectful of their surroundings and the privacy and dignity of others when connecting to social media platforms while on trust premises.
To protect the privacy and dignity of others, no one is permitted to make pictures, videos or audio recordings in healthcare settings that show other service users, visitors or staff without the knowledge and consent of those individuals. Furthermore, no pictures, videos or audio recordings, or comments identifying individuals, should be posted on any social media without consent first being sought – this has the potential to cause significant upset.

If staff are aware that someone has taken pictures/videos/recordings (whether these have been posted online or not) without the consent of the individuals featured, or has uploaded content that could be offensive or harmful, they should ask the person who has made and/or shared the recording to delete this immediately, explaining this is necessary to respect the privacy and dignity of patients and visitors.
- Visitors: if they refuse to stop or delete, ask them to leave the premises. If they do not leave, escalate to team lead/manager who may involve the police depending on circumstances.
- Patients: if they refuse to co-operate, highlight to the nurse in charge or manager of the area, who should intervene.

All instances of pictures/videos/recordings being taken inappropriately in clinical areas must be reported via the Trust's Learning Event and Reporting Notification (LERN) procedure.

12.0 Patient Confidentiality
The rules regarding the confidentiality of patient information apply to social networking and blogging. Personal identifiable information about patients and/or their relatives/carers must not be posted online unless written consent has been obtained. Any such incidents may constitute a breach of confidentiality and should be reported using the Trust's LERN procedure.

Patients may wish to engage with the Trust on social media regarding their care or their condition. Social media must not be used to communicate individually with patients or other parties on behalf of the Trust about their individual health or treatment, and patients should be encouraged to contact their care team directly. In certain limited cases, social media may be used to make more generic information available to patients.

Staff should also be aware of their professional codes of conduct and guidance when being asked to accept patients or former patients as 'friends' on social networking sites.

If staff become aware that patients or their relatives have included inappropriate content on any social networking or blogging sites such as confidential information or defamatory remarks they should explain the issues involved and request that this is removed immediately to avoid potential legal action from the persons to whom it relates. Any concerns can also be raised with the Information Governance Manager.

13.0 Information about the Trust and Colleagues

Work colleagues also have a right to privacy and must not be named on social media or have photographs of them shared publicly unless they have given their permission. Staff must take care that they do not indirectly identify other staff or disclose information to or about any other member of staff on social media (for example, by revealing they have been successful in an application for a new role before other members of staff who have been unsuccessful have been informed). Anything referring to or including a colleague should be removed where a colleague asks.

Be wary of expressing personal opinions about colleagues and the Trust on social media as these may be defamatory. Under no circumstances should comments which may be perceived as offensive be made about patients, their relatives or carers, trust colleagues or the trust's business, even if anonymised.

Confidential information about the trust which staff have acquired through their employment by the trust must not be disclosed on social networking websites or blogs. This includes changes to services and financial information which has not yet been made public by the trust. The trust will request that such content is removed by the member of staff who has published the information, or if necessary request that the content is removed by the website provider.

This does not affect an employee's ability to raise concerns about the trust under the Trust's 'Public Interest Disclosure (Whistleblowing) Policy'. However, staff are expected to raise these concerns internally first. Using social media to whistle blow without already having raised concerns through the proper channels within the trust

would not normally be considered appropriate.

14.0 Bullying and Harassment
The use or social networking or blogging sites to bully, harass or intimidate other employees of the trust will lead to investigation and may result in disciplinary action being taken. See the trust's 'Dignity at Work Policy' for further information. Staff who have concerns about this should contact their line manager or Human Resource (HR) with a copy of any relevant content posted on social media.

Staff can also take action themselves to block contact or remove someone from a friends list. Staff can also report inappropriate use of a site using the processes made available on most reputable sites. In the most serious circumstances, for example if someone's use of a social networking site is unlawful, the incident should be reported to the police.

15.0 IT Security
Users of social networking and blogging sites should follow the rules and advice on the use of trust's network in the Trust's 'E-mail and Internet Use Policy' to access these sites and to protect the trust's network from viruses, unauthorised access and disruption. Be extra vigilant as downloads and emails from social networking sites can contain viruses or other malicious content.

16.0 Monitoring this Policy
The Human Resources Directorate will monitor statistics regarding the nature and number of incidents raised under this policy and the Staff Partnership Forum will monitor the implementation of this policy as part of its formal arrangements.
Any breaches of this policy must be reported using the Learning Event and Reporting Notification (LERN) process. Any breaches of this policy may result in disciplinary action.
An Equality Impact Assessments of this Policy has/will take place.
17.0 Review
This policy will be reviewed on a three-yearly basis as part of the HR procedure review programme.
18.0 Further Information
- BMA: http://www.bma.org.uk/press_centre/video_social_media/socialmediaguidance2011.jsp
- Nursing and Midwifery Council: http://www.nmc-uk.org/Nurses-and-midwives/Advice-bytopic/A/Advice/Social-networking-sites/
- Information Commissioner's Office – social networking guidance: https://ico.org.uk/media/for-organisations/documents/1600/social-networkingand-online-forums-dpa-guidance.pdf.

Appendix A: Top Tips for Social Media Usage

1. **Private doesn't always mean private!:** Even if your settings on Facebook or Instagram are set to private, any post you make could still be in the public domain. More people could be seeing your activity than you think.

2. **Respect confidentiality:** Patient identifiable information must not be shared via social media. If it hasn't been agreed that it can be in the public domain via a written consent form, then it shouldn't be there and should remain private.

3. **Views are mine:** It is advisable to make clear in your social media and social networking profile information that your views belong to you and do not represent those of the Trust.

4. **Use social media for the right reasons:** Social media is a great communication tool but is maybe not the best place to air disagreements or raise concerns about a department's or colleague's working practice. It is advised that these should be raised internally and in line with the Trust whistleblowing policy.

5. **The bottom line:** The main thing to remember is if you wouldn't share a comment, photo or video with your grandmother in real life, don't share it online. You are an ambassador for both the Trust and the NHS. Even if you delete a post, it may already have been picked up on.

Here are some helpful ideas to make the most of your social media presence:

The power of the hashtag #: Twitter is centred on the use of the hashtag. If you are tweeting about a particular subject, give it a hashtag and other users searching for that topic will be able to see your post. It's the best way to contribute to a trending conversation and also the best way to start or find one. Examples include #NHS or **#UniversityHospitalsDorset #AsOneUHD.** Multiple hashtags can be used but don't go overboard, only use a maximum of two.

Send us your snaps!: Positive news stories in and around the hospital are always warmly welcomed by the communications team for use in the weekly bulletin or on the intranet. If you want to supply an image though, please do ensure you have obtained written consent from the subject in the image. If you do have any news stories that you would like to share, email communications@uhd.nhs.uk or @UHD_NHS on Twitter.

Think mobile: 80 per cent of Twitter users access the site via mobile rather than at a desktop computer. Make your posts mobile friendly and they'll perform better!

Stick to a schedule: Spreading out your posts helps increase coverage and accessibility rather than publishing everything at once! Facebook pages and groups have a scheduling tool already built in and a website like Tweetdeck is really useful to spread tweets out.

Short and sweet: Don't ramble on! Social media is designed to be instant and studies have found that Facebook posts with less than 40 characters typically receive an 86 per cent boost in engagement while tweets with less than 100 characters attain a 17 per cent higher access rate on average.