

1. Introduction

1.1 The University Hospitals of Leicester (UHL) recognises that social networking media is a valuable resource that can develop skills and knowledge, however, the growing popularity of social networking sites has increased the risks of potentially serious legal and professional implications if inappropriately used, even if inadvertently. These guidelines therefore seek to make it clear to staff what is acceptable in terms of social networking in relation to their employment.

1.2 All staff are also required to read the following. The Trust's

- Information Governance Policy (Trust Reference B4/2004).
- Email and Internet Access Usage Policy (Trust reference A9/2003),
- Information Security Policy (Trust reference B40/2024, formerly A10/2003) and
- Personal Information Policy (Trust reference B39/2007).

In addition further specific information may be obtained from the Trust's Consent to Examination or Treatment Policy (Trust reference B35/2024 – formerly A16/2002), in relation to medical images and the Resolution Policy (Trust reference B39/2020).

1.3 These guidelines apply to any social networking activity undertaken during working hours, but also to any undertaken in personal time if the individual or the information can be linked to the Trust, patients or colleagues in any way.

1.4 For the purpose of these guidelines, social networking is the process of building online communities, often accomplished both through 'groups' and 'friends lists' that allow greater interaction on websites.

1.5 Examples of social networking include internet sites such as Facebook, Instagram (photograph sharing facility), LinkedIn, Twitter and Yammer (internal UHL social networking facility). There are also many thousands of personal blogs. Other web media, for example, email discussion posts/lists, newsgroups, consumer feedback websites or professional bodies' websites may also be considered a form of social networking. This list is not exhaustive.

1.6 Anything posted on social networking websites (including the internal UHL networking site Yammer) which is deemed to be offensive, harmful, inappropriate, inflammatory, a breach of any Trust policy, UHL Trust Values or is damaging to the Trust's reputation will be liable to action under the Trust's Disciplinary Procedure. This can include references to colleagues, staff, managers, patients or visitors either named or unnamed. Action under the Trust's Disciplinary Procedure can be at any level up to and including dismissal. It is worth noting that as a general rule social media should not be used to post any comments or thoughts that would not be made using other forms of communication i.e. notice boards.

1.7 It is also not felt to be appropriate to use just social media to swap shifts with colleagues and any request to swap shifts should always be done through normally established channels to ensure an appropriate skill mix is maintained.

2. Scope

2.1 These guidelines are for all UHL staff, staff on honorary contracts, student placements, bank and agency staff, Trust volunteers and sub-contracted staff.

3. Recommendations, Standards and Procedural Statements

3.1 Accessing Social Networking Sites at Work

3.1.1 It is acknowledged that there is direct benefit for staff to use Social networking professionally to share good practice and access current research. The Trust also uses social networking to engage the local community and share examples of service developments.

3.1.2 All staff must read and comply with the Trust's Email and Internet Access and Monitoring Policy; staff are urged to specifically look at the sections relating to the use of the internet for personal use during working hours. This includes the use of the internet to check social networking sites via personal mobile telephones as outlined in Appendix B of the Email and Internet Use Policy.

3.1.3 The Trust will undertake routine monitoring of employee usage of all social networking sites in line with its stated information security policy standards. This will include a review of any inappropriate access to social networking sites or submissions of content by staff that are not in line with the stated Trust values. Staff should be aware that the Trust reserves the right to review and respond to any content submitted by its employees that relates directly to Trust services.

3.2 Posting Information on Social Networking Sites

3.2.1 All social networking sites have the potential to be accessible to others and therefore be part of the public domain even if users have the highest possible privacy settings and staff need to be aware that it is the responsibility of the individual who is posting images, comments, words and blogs to ensure the content submitted is appropriate. These guidelines also apply to closed networking groups such as those on Facebook and WhatsApp.

3.2.2 It is strongly recommended that staff should avoid identification of UHL as their employer and what job they do if they are operating a personal profile on a social networking site. Staff should be aware that even if UHL is not identified, but they post comments that are deemed to be inappropriate and could bring the Trust into disrepute they may still be in breach of professional codes of conduct and UHL policies.

Postings that refer to good news stories i.e. awards or examples of a good experience etc some staff may wish to share. A general principle to be considered is, 'Would this be appropriate to display on a public notice board'. If this is the case, then it would be reasonable to consider this information a suitable posting. Information of this type would normally have the consent of any individuals involved to be shared publically.

3.2.3 Staff must not use personal social media for the following:

- To build or pursue relationships with patients and service users even if they are no longer receiving care and should ignore friendship requests from current or former patients.
- To discuss work related issues, or discuss patients or colleagues (even if anonymised) unless for previously agreed educational purposes.
- To post pictures of patients or service users, or colleagues in uniform without consent. Any pictures taken within UHL premises or the use of UHL logos must not be posted without the expressed permission of the Director of Communications and Engagement. Staff should refer to the Trust's Consent to Examination or Treatment Policy for specific information. There may be occasions when images of patients and or clinical procedures are required for professional usage only and staff should refer to the Trust's Policy on Consent to Examination or Treatment for specific guidance.

- To post any other inappropriate, discriminatory or illegal comments which also includes reference to activities undertaken whilst off sick that could be deemed to be detrimental to recovery.
- To raise or escalate formal concerns. This should be done through the procedures that UHL already has in place to do this.
- To speak on behalf of the Trust unless officially designated to do so.

3.2.4 Any breach or suspected breach of the conditions outlined above will be investigated in accordance with the Trust's Disciplinary Policy and disciplinary action may be taken, up to and including dismissal. Inappropriate posts on social media may be used as part of Disciplinary, Sickness or Fitness to Practice investigations. Staff should also be aware that they have a responsibility to comply with relevant Professional Codes of Conduct/ Practice related to the use of social networking. Examples of this could be where comments have been made by a member of staff about inappropriate postings made by someone else not employed by the Trust or making inappropriate or hurtful comments about colleagues.

3.2.5 Staff will be aware that patients and their families are increasingly prepared to comment about the care that the Trust delivers on social media websites. This can provide useful feedback to help improve services. Where criticisms are made about an identifiable individual then careful consideration has to be given as to whether this merits action by the Trust to protect the individual concerned. Where such a situation is felt to exist please contact the Director of Corporate and Legal Affairs, the Director of Communications and Engagement and if necessary the CMG People Partner for assistance.

3.2.6 If a member of staff has concerns about the Trust, a particular practice or anyone within the Trust then the appropriate way to raise a concern is via the Trust's Resolution Policy, through the Trust's Freedom to Speak up – Raising Concerns Policy (Trust reference A15/2001), the Junior Doctor's Gripe tool or via the concern line on extension 3636.

3.3 Professional Use of Social Networking/ Media

3.3.1 It is clear that there are many benefits in the use of social media professionally and the Trust is currently developing a Social Media Toolkit to support this. Staff who use Trust verified social networking sites professionally should ensure that comments posted are not personal comments and ideally should ensure that they keep two separate accounts, one for professional use and one for social use. Staff who wish to set up an Trust verified account (an account that is not a personal account but one that a staff member uses for their professional work for the Trust) should contact the Communications team for guidance.

3.3.2 Staff with professional social networking accounts should always ensure that they comply with the Trust's policies on confidentiality and respect privacy and copyright legislation and take advice if they are in any doubt over the information they are about to post. Further information can also be obtained from relevant regulatory bodies and professional organisations.

Links to some of these are below but this is not an exhaustive list.

NMC - <http://www.nmc-uk.org/nurses-and-midwives/advice-by-topic/a/advice/social-networking-sites/>

GMC - http://www.gmc-uk.org/guidance/ethical_guidance/21186.asp

BMA – <https://www.bma.org.uk/advice/employment/ethics/social-media-guidance-for-doctors>

3.3.3 If staff wish to set up social networking sites on behalf of their service they should contact the Communications team in the first instance.

3.4 Requests for information via social media

3.4.1 Any member of staff setting up a social media account (either in their own name, in the name of a team, or service) should be aware that they could receive an FOI request via that social media channel. The Information Commissioner confirms that FOI requests made via messages to accounts operated by public bodies on sites such as Twitter or Facebook can trigger those organisations' duties to disclose information under the FOI Act. Any such request should be forwarded to Corporate and Committee Services to deal with formally. Please refer to the UHL Freedom of Information Act 2000 and Environmental Information Regulations 2004 Policy (B33/2024 – formerly A9/2004) for further information.

4. Education and Training

4.1 New staff will be made aware of the Social Networking Guidelines as part of corporate and local induction processes.

4.2 The revised Social Networking Guidelines will be circulated to all managers by the HR team and asked that they be disseminated to all staff once they have been updated and approved.

4.3 If an employee needs clarification with regard to these guidelines they should speak to their line manager or seek advice from a member of the HR team.

5. Monitoring and Audit Criteria

Key Performance Indicator	Method of Assessment	Frequency	Lead
Number of investigations/ complaints about staff using social networking sites, inappropriately	Audit	Yearly	Human Resources
Number of cases identified above that lead to informal / no action.	Audit	Yearly	Human Resources
Number of cases identified above that lead to disciplinary action being taken.	Audit	Yearly	Human Resources

7. Supporting Documents and Key References

Employees should be aware that some actions relating to social networking media may be illegal and could therefore have consequences beyond their employment. There is a range of legislation regarding the publication of information as detailed below. This list is not exhaustive:

- UHL Resolutions Policy
- UHL Disciplinary policy and procedure
- Obscene Publications Act (1959/1964)
- Telecommunications - Lawful Business Practice (Interception of communications) Regulations 2000
- The Criminal Justice Act (1988)
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)
- Copyright (Designs and Patents Act, 1988) as amended by the Copyright (Computer Programs) Regulations 1992
- Data Protection Act (1998)
- Regulation of Investigatory Powers Act 2000
- UHL Information Governance Policy
- UHL E mail and Internet Access Usage Policy
- UHL Information Security Policy

- UHL Use of Personal Information Policy
- UHL Consent to Medical Examination or Treatment Policy
- Relevant Professional Bodies' Codes of Conduct

8. Key Words

Social Media, Networking, Profile, Facebook, X (formerly known as Twitter) Twitter, Instagram, TikTok, Posting, Snapchat, Hashtags, Online, You Tube, Telegram, LinkedIn, Pinterest, Reddit

This line signifies the end of the document

This table is used to track the development and approval and dissemination of the document and any changes made on revised / reviewed versions

DEVELOPMENT AND APPROVAL RECORD FOR THIS DOCUMENT			
Author / Lead Officer:	Rachel Wardle		Job Title: ER Team Leader
Reviewed by:			
Approved by:	Policy and Guideline Committee		Date Approved: 15.3.24 (latest version)
REVIEW RECORD			
Date	Issue Number	Reviewed By	Description Of Changes (If Any)
DISTRIBUTION RECORD:			
Date	Name	Dept	Received