providing the excellent care we would expect for our own families

The Royal Bournemouth and Christchurch Hospitals NHS Foundation Trust

Social Networking and Blogging Policy

Approval Committee	Version	Issue Date	Review Date	Document Author
Information Governance Committee	2.0	September 2015	September 2018	Information Governance Manager

Table of Contents

1. Executive Summary

The Trust recognises the benefits of social networking and blogging for both the Trust and the staff in terms of building networks and communities and sharing information.

The purpose of this policy is to provide staff with clear guidance on their responsibilities and the potential implications when putting information about the Trust, their colleagues or patients on the internet. This policy outlines the principles which staff should follow when accessing social media for professional and private use. This will prevent damage to the Trust's or the individual's reputation and the public perception of the Trust which may be caused by inappropriate use of these sites.

2. Scope of this Policy

This policy is based on the NHS best practice guidelines and guidance from the NHS England, the British Medical Association, the General Medical Council and the Nursing & Midwifery Council on the use of social media.
This policy applies to all staff, contractors and volunteers.

3. Training

The Trust will increase awareness through mandatory Information Governance training provided to new staff as well as existing staff to maximise compliance with patient confidentiality and information security requirements.

4. Definitions

4.1. Social Networking

Social networking is the use of interactive websites to communicate or interact with other users using text, images or video. Examples include Facebook, MySpace and LinkedIn. It is also includes the use of discussion and message boards and instant messaging.

4.2. Blogging

Blogging (also microblogging) is using a public website to share thoughts and opinions on various subjects. Examples include Twitter, Google+ and Tumblr.

4.3. User Generated Content

User Generated Content includes all material (including text, images, audio material, video material and audio-visual material) submitted to websites or any other digital media, for whatever purpose.

5. Use of Social Networks and Blogging While at Work

The Trust permits the use of the internet by staff in their own time (i.e., during authorised breaks) while at work, providing that it is done in accordance with the Trust's Email and Internet Use Policy and this Policy. Access to some social networking and blogging sites may be blocked by the Trust's IT network – this policy also applies to staff using their own personal mobile devices to access the internet during authorised breaks.

Staff should ensure that any use of social networking or blogging does not interfere with the performance of their duties during working hours or the ability of others to use the internet or PCs or laptops for work-related matters. This includes access to social networks and blogs using personal or Trust mobile phones or other mobile devices.

This Policy also applies to the use of social networking or blogging sites outside of work, particularly where staff have identified that they work for the Trust or the National Health Service. Staff are expected to behave appropriately, and in ways that are consistent with NHS values, the Trust's values and policies, their individual responsibility as a Trust employee and with the relevant professional codes of conduct for healthcare professionals.

Those members of staff that do divulge their employer should state clearly that they are acting in a personal capacity by including a disclaimer such as "My postings on this site reflect my personal views and do not necessarily 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.

6. 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 included in User Generated Content posted online. Any such incidents may constitute a breach of confidentiality and should be reported via the Trust's Adverse Incident Reporting (AIR) procedure.

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. In certain limited cases, social media may be used to make more generic information available to patients; see section 11, below.

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.

7. Information about the Trust and Colleagues

Work colleagues also have a right to privacy and must not be named on these sites 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 in any of their User Generated Content (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). Any User Generated Content referring to or including a colleague should be removed where a colleague asks.

Be wary of expressing personal opinions about colleagues and the Trust in User Generated Content 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 in any User Generated Content.

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 whistleblow without already having raised concerns through the proper channels within the Trust would not normally be considered appropriate.

8. 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 Bullying and Harassment in the Workplace Policy for further information. Staff who have concerns about this should contact their line manager or HR with a copy of the relevant User Generated Content.

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.

9. Guidance on Using Social Networking and Blogging Sites

- Do not discuss work-related issues online, including conversations about patients or complaints about colleagues. Even when anonymised, these are likely to be inappropriate.
- Use social media responsibly and professionally; if you wouldn't want your family or patients to read what you are posting, don't publish it.
- Be aware of how comments and images online can impact on your professional standing.
- Protect your own privacy through the use of appropriate privacy settings and withhold information which you would not want made public.
- Remember that all User Generated Content online is public, even with the strictest privacy settings. Once online, this information can be copied and redistributed, and it is easy to lose control of it.
- Always assume that any User Generated Content published online will remain online in perpetuity and will be visible to everyone.
- Normal laws, such as those regarding libel, copyright, equality and diversity etc., apply to User Generated Content – 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 such as websites like Wikipedia.
- Declare any conflicts of interest when making posting User Generated Content online.

10. 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 Internet Access 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.

11. Representing the Trust on Social Networks and Blogs

The Trust's official social media presence is managed by the Communications department. This department is authorised to publish User Generated Content on social networking and blogging sites on behalf of the Trust.

Staff should not set up or use social networking pages or sites to represent the Trust unless authorised to do so by the Communications Department.. All User Generated Content made on behalf of the Trust must be reviewed

and approved by the Communications Department before these are made available to others to read.

Where staff have been authorised to use social networking or blogging sites on behalf of the Trust, all account profiles on the social network or blog will belong to the Trust, including login credentials and information which allow the Trust to access and use the social networking or blogging sites. These are required to be handed over to the Trust on request and arrangements must be made to transfer ownership (including account passwords and related email accounts) to the Trust when the member of staff concerned is on annual or sickness leave and before that member of staff leaves the Trust permanently.

12. Use of social networking and blogging by patients and visitors

It is recognised that patients and their visitors will make use of social networking and blogging sites whilst in the hospital. It is important that patients and their visitors are respectful of their surroundings and the privacy and dignity of others when using mobile devices (such as mobile phones) and connecting to social media platforms whilst 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 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 posted the User Generated Content to delete this immediately, explaining this is 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 AIRs procedure.

13. Monitoring of this Policy

Any breaches of this Policy must be reported using the Adverse Incident Report (AIR) process. Any breaches of this Policy may result in disciplinary action.

14. Other Related Policies

Please refer to the following when reading this policy:

- Email and Internet Use Policy
- Bullying and Harassment in the Workplace Policy
- Disciplinary Policy
- Whistleblowing (Public Interest Disclosure) Policy

15. 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-by-topic/A/Advice/Social-networking-sites/
Information Commissioner's Office – social networking guidance:
https://ico.org.uk/media/for-organisations/documents/1600/social-networking-and-online-forums-dpa-guidance.pdf.