Bank Member Guidelines

Social Networking

Contents:

1 Scope

2 Purpose

3. Key Definitions

4 Responsibilities
4.1. Bank Member Human Resources
4.2. Bank Member

5 Process/ Interactions
5.1 Social Media at work / while Working a Shift via NHSP
5.2 Personal Use of Social Media
5.3 Social Media and Work Colleagues
5.4 Social Media and NHSP/Client Trusts

6 Breach of Guidelines

1. Scope

These guidelines apply to all Bank member (BMs) who carry out assignments via NHS Professionals (NHSP) at all NHSP offices and Client Trusts. These guidelines are intended to supplement the terms of the Bank member Registration document and Code of Behaviour.

2. Purpose

The purpose of this document is to ensure that BMs are aware of their rights and responsibilities regarding the use of social networking. It attempts to explain clearly what is not permitted and what constitutes acceptable use. NHSP accepts that some of our Client Trusts may provide BMs access to the Internet via the NHS global network (NHSNet). The use of the Internet is a privilege, not a right. Access to Internet web sites is monitored at all times and all users of the internet services must abide by the Client Trusts Terms & Conditions as outlined in each local Trust policy. The Internet services should be used for purposes that directly, or indirectly, relate to the activities of our Client Trusts. While on an assignment, Bank members must ensure that they are familiar with the Trust's email and internet policy at the site they are working.

3. Key Definitions

Social Media/ Social Networking Site/ Platform	For the purposes of these guidelines, social media is any online platform or app that allows parties to communicate instantly with each other or to share data in a public forum. This includes but is not limited to social forums such as Twitter, Instagram, Facebook and LinkedIn. Social media also covers blogs ,video and image-sharing websites such as YouTube. Bank Members should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area. Bank members should follow these guidelines in relation to any social media that they use
Social Networking Application	Social Networking application is any computer-based software which allows a user to post material unto a public domain.
Social Media Monitoring	Social media monitoring is a process of monitoring and responding to mentions related to a business that occur in social media.
Social Media Icons	These are links that can be displayed in different ways on a site. These icons are button like links to services such as Twitter and Facebook and allow visitors quick access to an individual's social profile.

4 Responsibilities

4.1 Bank Member HR- must:
• Ensure BMs are aware of these guidelines and parameters outlined.
• Take appropriate action when notified of instances in which social media behaviours have
  been found unacceptable.

4.2 Bank Member- The BM must:
• Protect NHSP and Client Trust(s) reputation and that of their profession.
• Behave online in a similar way to that which would be expected of them in any other situation
  at work.

5. Process/ Interactions
BMs that have identified their association with NHSP and our Client Trusts on any social media
site are expected to act in a manner which acknowledges the duty of care they owe to their
colleagues and the Trust.
Once information is published on the internet it is no longer considered to be private, therefore
BMs will be held accountable for any information that is challenged on the basis that it
compromises them, colleagues and or NHSP/the Client Trust. BMs must not use their mobile
phones in the workplace to upload photographs on to social media sites.

5.1 -Social Media at Work/ while working a Shift via NHSP
Generally, BMs are not permitted to access social media sites from NHSP/ Client Trust
computers or devices at any time (this includes computers or devices distributed by the
organisation(s) for work purposes.) However, in the event that BMs are permitted to access
such sites as part of their role, they are reminded to comply with all aspects of these guidelines
as well as the policy of the Trust where they are carrying out assignments. Links must only go
to suitable websites. A web page is classified unsuitable if it contains, or directly links to material
which:

• is offensive
• is unlawful
• presents virtual/real risk to users

Accessing social network sites from personal mobile phones during working hours is a misuse
of resources and will be dealt with in line with the NHS Professionals Disciplinary Procedure.
NHSP understands that BMs may wish to use their own personal devices such as mobile
phones, iPads etc to access social media websites while at work. BMs must limit
their use of social media on their own equipment to [their official rest breaks such as their lunch
break/times.

Personal mobile phones should not be used in clinical areas except for where they are provided
by the Trust or are deemed essential for work related use (for example as a point of contact for
on call medical staff). Where these devices are not essential for work, use personal mobile
phones must be switched off, and locked away in a secure environment before entering clinical
areas, ensuring a safe and comfortable environment for patients.

Taking of clinical photographs or videos is not routinely permitted on any mobile phone/
electronic device on any Trust premises or community setting.

5.2 Personal Use of Social Media

NHS professionals recognises that Bank members make use of social media in a personal capacity. While not working for the organisation, Bank members must be aware that they can bring the organisation into disrepute if they are recognised as being one of its members. Bank members online profile (for example, the name of a blog or a Twitter name) must not contain the organisation's name.

If Bank members do discuss their work on social media (for example, giving opinions on their specialism or the sector in which the organisation operates), they must include on their profile a statement along the following lines: "The views I express here are mine alone and do not necessarily reflect the views of the Organisation I work for."

While using social networking sites in a personal capacity, and not acting on behalf of NHSP/ Client Trust(s), BMs must not:

• Behave in a manner that would not be acceptable in any other situation
• Bring NHSP/Client Trusts into disrepute
• Breach confidentiality for example by revealing information owned by the organisation, giving away confidential information abouts colleagues, customer
• Use offensive/intimidating language discussing the organisation's internal workings
• Pursue personal relationships with patients/service users
• Post inappropriate comments about work colleagues/patients/NHSP/Client Trusts
• Post links to inappropriate content
• Comment on work related issues
• Post pictures/comments/personal details/clinical details which identify any individual without their prior consent. This includes pictures taken on wards or in other work areas where patients or patient details could be captured or pictures in uniform.
• Post any information, photos or other items online that could embarrass you, your family, your colleagues, NHS Professionals, our Client Trusts and any Patients. This includes information that may be posted by others on your page.
• Do anything that could be considered discriminatory against, or bullying or harassment of any individual such as making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age, or using social media to bully another individual (such as a colleague, employee NHSP or Client Trust)

Before participating in any online community, understand that anything posted online is immediately made public and made available to everyone, everywhere. Any text or photo placed online becomes the property of the site(s) and is completely out of your control the moment it is placed online - even if you limit access to your site.

Professionally qualified BMs may place their registration at risk if they fail to adhere to the above guidelines. The Nursing and Midwifery Council (NMC) take Social Networking seriously. They have stated that Nurses and Midwives could risk their registration if they share sensitive information, make inappropriate comments, or befriend patients online. Pursing personal relationships with patients/service users is not acceptable under any circumstances. These actions could bring about disciplinary proceedings which could result in the termination of a BM's registration with NHSP. For more information, please visit the links below:

NMC https://www.nmc.org.uk/standards/guidance/social-media-guidance/
GMC:https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/doctors-use-of-social-media/doctors-use-of-social-media

BMs should be mindful of the personal information they disclose on social networking sites, i.e. home address, phone number(s), birth date or other personal information. Making such information publicly available can expose BMs to identity theft/ other forms of fraud.

5.3 Social Media and Work Colleagues
When interacting with colleagues online, BMs should be mindful of their responsibility to be professional, courteous and not to use social media to attack or abuse colleagues. When uploading material such as pictures from a social event that includes other colleagues (BMs and Client Trust staff) on social media sites, BMs must ensure they obtain permission from colleagues first and not to post anything if not granted permission to do so.

5.4 Social Media and NHSP/Client Trusts
BMs should not post comments/questions or observations in connection with their registration with NHSP or any work they carry out / experience they have at Client Trusts; whether positive or negative. Any concerns should be raised via the appropriate channels rather than being expressed on social media.

6. Breach of Guidelines
BMs who fall in breach of these guidelines will be subject to the NHSP disciplinary guidelines. The matter will be investigated to ascertain the nature and extent of the breach. If BMs are concerned about another BMs behaviour online, they should report this to NHS Professionals. Concerns can be raised by visiting the contact us tab on the NHSP website, www.nhsprofessionlas.nhs.uk . The report must be made along with any supporting evidence of their complaint in order for appropriate action to be taken in accordance with NHSP's guidelines. For further clarification, please contact the Bank Member HR team at bmhumanresources@nhsprofessionlas.nhs.uk.