Avon and Wiltshire NHS
Mental Health Partnership NHS Trust

Staff Use of Social Media and Social Networking Policy

Board library reference	Document author	Assured by	Review cycle
P127	Head of Communications	Finance and Planning Committee	3 years

This document is version controlled. The master copy is on Ourspace.

Once printed, this document could become out of date.

Check Ourspace for the latest version.

Contents

1. Introduction

The world of communication is changing and the Trust aims to be a dynamic organisation embracing new technologies and ways of working. The rise of social media is changing the way we, and every organisation in the world conducts its business. Millions of people use social media everyday responsibly and it is becoming an increasingly important communications tool.

Social media can be used to raise awareness of Trust activities, have a discussion or consult with service users, pick up news items swiftly and be aware of any Trust issues circulating so they can be addressed quickly.

The Trust currently uses social media as a tool to engage with service users, staff, media and other stakeholders to deliver positive, key messages for good healthcare and services. Staff are encouraged to follow, support and promote it.

2. Purpose or aim

The purpose of this policy is to make its employees and workers fully aware of the relevant Trust expectations in the context of their personal and professional use of social media.

This policy covers the use of social media through personal devices. The use of Trust owned devices is addressed in the Acceptable Use Policy.

This policy will reduce the risks to the Trust associated with the use of social media by:

- Aiming to ensure the confidentiality of personal information relating to service users, carers, employees and workers and others associated with the Trust.
- Aiming to ensure compliance with relevant data protection, copyright and defamation legislation.
- Prohibiting the publication of material on social media sites that would damage the reputation of the Trust or give inaccurate or misleading information about the Trust's business.

3. Scope

This policy applies to all Trust employees and workers.

4. Definitions

4.1 Social media

Social media is the term commonly used for web-based and other mobile communications technologies that enable message and opinions to be shared in dialogue with others who often share the same community interests. Such technologies can include instant messaging and other similar services.

4.2 Personal social media sites

Personal social media sites are those sites which individuals use to share information about their personal lives outside the working environment.

4.3 Professional social media sites

Professional social media sites are sites used for professional networking

4.4 Social networking

Social networking is the use of interactive web based sites or social media sites, allowing individuals on-line interactions that mimic some of the interactions between people with similar interests that occur in life. Popular examples include Facebook, Flickr and Instagram.

4.5 Blogging or Tweeting (micro-blogging)

Blogging or Tweeting (micro-blogging) is using a public website to write an on-line diary (known as a blog) or sharing thoughts and opinions on various subjects. Blogs and Tweets are usually maintained by an individual with regular entries of commentary, descriptions of events, and may include other material such as graphics or video. Many blogs and tweets are interactive allowing visitors to respond leaving comments or to potentially send messages to others. It is increasingly common for blogs to feature advertisements to financially benefit the blogger or to promote a blogger's favourite cause.

4.6 Personal/Portable/Electronic Devices

Personal devices (e.g. mobile phones/ smartphones/ personal laptops etc.) provide a means of communication and access to the internet. These may also include photograph or video cameras and satellite navigation or tracking facilities.

4.7 Copyright

All staff must at all times comply with the law in regard to copyright/plagiarism. Posting of someone else's work without permission is not allowed (other than short quotes that comply with the "fair use" exceptions). This includes the "lifting" (reusing content without permission) of images and videos from other sites, including that of the Trust and its partner organisations.

4.8 Defamation

Defamation is the act of making an unjustified statement about a person or organisation that is considered to harm their reputation. Defamation law can apply to any comments posted on the web, irrespective of whether they are made in a personal or professional capacity.

5. Policy statement

The Trust recognises that many staff enjoy the benefits of using social media in a personal and professional capacity. Additionally many organisations, including AWP, use social media to share information and views and raise awareness.

The Communications team will provide guidance and training to empower staff to interact online in a way that is credible, consistent, transparent and relevant.

When an employee or worker is using social media, whether or not they have identified themselves as having an association with the Trust, they are expected to behave appropriately at all times and in a manner that is consistent with the Trust's values and policies, in addition to any professional codes of conduct applicable to the individual (see also 5.1 below).

Employees who are found to breach this policy may be managed in line with the Trust's Disciplinary Policy. Relevant misconduct may constitute gross misconduct and may result in dismissal.

Employees are responsible for reading, knowing, and complying with the Terms of Service of the sites they use.

6. Employee use of social media and social networking

Posts made through personal accounts that are public can be seen, and may breach organisational policy if they bring the organisation into disrepute. This includes situations when you could be identifiable as a Trust employee whilst using social networking tools or occasions when you may be commenting on AWP related matters in a public forum.

Staff should use their own discretion and common sense when engaging in online communication. The following guidance gives some general rules and best practices which you should abide by at all times. Employees and workers, when using social media or any on-line communication, must not:

- reveal any confidential information about service users, staff, or the Trust;
- engage in any activities on the internet or share information which might bring the Trust into disrepute;
- use social media in any way to attack or abuse colleagues;
- alter online sources of information on websites such as Wikipedia from a Trust perspective;
- use the internet in any way to attack or abuse colleagues, stakeholders, service users and carers;
- post defamatory, derogatory or offensive comments on the internet about colleagues, service users, their work or the Trust;
- post information relating to work related grievances or any Trust management processes such as disciplinary, sickness absence or performance issues; and
- share photos or images of service users or carers, even if requested to do so, unless this forms part of an ongoing Communications-approved campaign for which you have authority to work on. In which case, you must provide a valid and completed consent form

Staff should follow the Standards of Business Conduct. The same principles and guidelines that apply to staff activities in general also apply to online activities.

Individuals holding themselves out as connected to AWP must not use the medium in such a way that confidential information is disclosed, is illegal, immoral or brings the organisation into disrepute or results in any adverse publicity.

Staff should refer to the Overarching Information Governance Policy regarding information sharing.

Staff should be aware of their association with AWP when using online social networks. They must ensure that their profile and related content is consistent with how they would wish to present themselves with colleagues, patients and service users. Staff should be aware that even if they have secure privacy settings on their personal account that if they are members of a group, all the other members will have the ability to see and use contact details.

Staff are personally responsible for the content they publish on blogs, wikis or any other form of user-generated media, and should use the same principles and standards online that you would apply to communicating in other media with people they do not know.

Staff who hold a professional registration must comply with the relevant requirements of their professional body in relation to the use of social media. AWP will report relevant misconduct in line with its Disciplinary Policy.

Use of Trust computers and internet enabled devices to access to social networking sites for personal use must be in accordance with the Trust's Acceptable Use Policy.

Guidance and advice relating to access to social media as part of your role is available on Ourspace.

6.1 Access to social networking sites for personal use

Access to social networking sites for personal use may only be accessed via personal portable devices during non-working time e.g. before commencing work, during breaks or after work.

6.2 Personal blogs

Any employee writing a personal blog should adhere to the guidance given above if the blog touches on any work related matters. Staff must also include a disclaimer which says:

“Any views expressed in this blog are entirely my own and not those of my employer.”

6.3 References and endorsements

For social networking sites such as LinkedIn where personal and professional references are the focus, if an employee is representing themselves as an AWP employee, they may not provide professional references about any current or former employee, contactor, vendor or contingent worker. An employee may provide a personal reference or recommendation for current or former employees, contractors, vendors and contingent workers provided:

- the statements made and information provided in the reference are factually accurate; and
- they include the disclaimer below:

“This reference is being made by me in a personal capacity. It is not intended and should not be construed as a reference from AWP Trust.”

6.4 Whistleblowing

The Trust’s Whistleblowing Policy states the routes of communication to raise a concern and no member of staff will use social media or networking to undertake whistleblowing.

See Ourspace for further information on whistleblowing.

6.5 Responding to the media

The Trust does not encourage staff to engage in “unofficial”, spontaneous exchanges in response to published media comment on behalf of the Trust. Any employee requiring advice on responding through approved channels should contact the Communications team for advice.

7. Trust use of social media and social networking

The Communications Team must be consulted before any social media is used on behalf of the Trust.

8. Roles and responsibilities

8.1 Executive Directors and Locality / Specialist Delivery Unit Directors

Executive Directors and Locality / Specialist Delivery Unit Directors are responsible for implementing the standards of compliance specified in this policy within their areas of responsibility.

8.2 Managers

Managers are responsible for:

- ensuring that employees and workers fully understand the information governance standards and expectations for their role.

- taking appropriate action when they are aware of breaches of this policy in a timely, fair and appropriate way in accordance with the Trust's Disciplinary Policy and/or the Policy for Managing Poor Staff Performance.
- ensuring that those associated with the Trust who are not directly employed by the organisation are aware that they should not share information about staff or service users or any other details that may bring AWP into disrepute.
- providing support to staff who find themselves the subject of cyber bullying, inappropriate postings or information sharing on online sites.

8.3 All employees

All Trust employees and workers are responsible for:

- ensuring that they follow this policy in relation to their personal use of social media, both in a professional and personal capacity.
- reporting any incidents of cyber bullying that they are aware of in relation to colleagues or service users to their line manager

9. Monitoring

The Communications Team will monitor activity on any Trust social media account during normal office hours, and outside of this in the event of increased activity. This will include evaluating the utility as well as the content of the accounts. I.e., not only how many 'follows' or 'likes' an account has, but how often information on that account is being viewed or clicked on.

If necessary, any staff member's failure to observe the guidance issued in line with the social media strategy will be dealt with in accordance with the Trust's disciplinary policy and procedure.

10. Training

Advice on compliance with this policy will be provided by the Communications Team.

Use of social media can present risks regarding inappropriate sharing of information. Information Governance training is available on the MLE which raises awareness of information risk and should be undertaken by all staff annually in line with IG toolkit requirements.

11. References and associated documents

- Acceptable Use Policy
- Data Protection Policy
- Freedom of Information Policy
- Health and Safety Policy
- Disciplinary Policy and Procedure
- Capability Policy and Procedure
- Whistleblowing Policy
- Nursing and Midwifery Council – Advice on Social Networking Sites
- BMA Social Media Guidance

12. Appendix 1: Quick tips for staff using social media and social networking

- When online, use the same principles and standards that you would apply to communicating in other media with people you do not know. If you wouldn't say something in an email or formal letter, don't say it online.
- Identify yourself by giving your name and, when relevant, role at AWP if you are discussing AWP or AWP related matters. Write in the first person. You must make it clear that you are speaking for yourself and not on behalf of AWP (you must not use the organisation's logo on personal web pages or social media accounts).
- It is possible that people may not be who they say they are and you should bear this in mind when participating in online activities.
- If you publish content to any website outside of NHS England that could be perceived to have a connection to the work you do or subjects associated with NHS England, you must display a disclaimer such as this:

  "My postings on this site reflect my personal views and don't necessarily represent the positions, strategies or opinions of AWP."
- Respect your audience. Don't use personal insults, obscenities, or engage in any conduct that would not be acceptable in the workplace. You should also show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory, such as politics and religion.
- If someone from the media contacts you about posts you have made, you must talk to the External Communications Team (awp.communicationsteam@nhs.net).

Version History

Version	Date	Revision description	Editor	Status
1.0	19 June 2012	First draft for discussion at GNG	KE	Draft
1.1	21 September 2012	Policy agreed at GNG 31 July 2012, MWMG 8 August 2012 and ESEC on 21 Sep 2012	TW	Approved
1.2	11 November 2013	Policy agreed at ESEC on 11 November 2013	ADP	Approved
1.3	7 July 2014	Administrative Amendments	SM	Approved
1.4	15 December 2015	Extension to review date approved by Quality and Standards Committee	HD	Approved
1.5	19 January 2016	Review date extended to 30 June 2016, as approved by Quality and Standards Committee	HD	Approved
2.0	31 January 2017	Administrative review and approved by Director of Finance and Senior Information Risk Owner	Head of Communications	Approved