

Social Media Policy

V2.0

Document reference:	POL 014
Document Type:	Policy
Version:	2.0
Purpose:	The purpose of this policy and its associated documents is to ensure that staff are aware of the correct approach towards the use of social media in both a professional capacity and a personal capacity. This policy should be read in conjunction with the Social Media Procedure .
Responsible Directorate:	Corporate Affairs
Executive Sponsor:	Fiona Alexander, Director of Communications
Document Author:	Communications Officer
Approved by:	Board of Directors
Date Approved:	23/01/2017
Review Date:	23/01/2020
Related Controlled documents	Social Media Procedure Handling the Media Policy Freedom of Information Policy Information Governance Policy Information Risk Management Policy Disciplinary Policy Dignity at Work Policy Photographic, Video and Mobile Device Consent Policy Celebrity and VIP Visitor Policy Raising Concerns (Incorporating Whistleblowing) Policy Acceptable use of ICT policy Data Protection, Confidentiality and Disclosures Policy Mobile Computing policy v1.0 Disciplinary policy v1.0
Relevant External Standards/ Legislation	Include details of any legislation / national standards etc tha the policy relates to
Target Audience:	All groups of staff, including bank staff.
Further information:	Communications Officer

Paper Copies of this Document

If you are reading a printed copy of this document you should check the Trust's Policy website (<http://sharepoint/policies>) to ensure that you are using the most current version.

Version History:

Version No.	Date of Release	Document Author	Ratified by	Date Ratified
V2.0	23/01/2017	Communications Officer	Board	23/01/2017

Summary of changes from last version:

Development of a separate procedure
Change in language
Reflect technological changes since the last policy was written

Table of Contents

1	Introduction / Purpose	3
2	Policy Statement	3
3	Definitions	4
3.1	Social media	4
3.2	Blogs	4
3.3	Twitter	5
3.4	Facebook	5
3.5	Snapchat	5
3.6	YouTube	5
3.7	LinkedIn	5
3.8	WhatsApp	5
3.9	Trolls	6
3.10	Viral effect	6
4	Policy Requirements	6
5	Role and Responsibilities	6
5.1	Directors	6
5.2	Local Managers	7
5.3	Other Individuals	7
5.4	All Staff	7
5.5	Specific groups / committees	8
6	Training	8
7	Monitoring Matrix	8
8	References	8
	Appendix A - Monitoring Matrix	9

1 Introduction / Purpose

The policy and supporting procedure aim to ensure that any and all social media activity by Trust staff does not bring the Trust, any of its services or Trust staff, into disrepute or otherwise contravene its existing policies and procedures by making available content which is offensive, libellous, or which makes publicly available personal information of patients, visitors or staff members, or which is otherwise evidential of misconduct.

Through implementation of this policy and its associated documents, the Trust will:

- provide clear guidance for staff on the appropriate use of social media in a personal capacity and reinforce the lines drawn by professional codes of conduct
- set out the process and rules for setting up, using, monitoring, and managing social media accounts on behalf of the Trust and its services
- educate staff on the use of social media to ensure any risk associated with its use is minimised
- inform staff of what constitutes unacceptable or inappropriate use and the consequences of such use which may result in dismissal
- help Trust staff to understand how social media can help Heart of England NHS Foundation Trust (HEFT) achieve its business objectives in a professional and responsible fashion
- empower Trust staff to contribute effectively to collaborative online activity when it supports the work of the organisation, and its vision and values
- This policy is provided so that staff are aware of the organisational stance and their personal responsibilities for the appropriate use of social media and online access.

This policy applies to all areas and activities of the Trust and to all Trust staff. For the purposes of this policy and its associated documents, Trust staff shall be defined as all permanent and fixed-term members of staff, bank staff, as well as contractors, volunteers, students, locum and agency staff, and staff employed on honorary contracts.

The Trust has a responsibility to ensure the operational effectiveness of its business, including its public image and for the protection of its information assets of all kinds. This involves ensuring patient/staff confidentiality and maintaining security in accordance with NHS Information Governance Policy and good practice.

Employees who are found to breach the Trust's policy will be managed in line with the Trust's Disciplinary Policy.

2 Policy Statement

This document ensures that staff are aware of the correct approach towards the use of social media in both a professional capacity – i.e. on behalf of the Trust or any of its services – and a personal capacity.

Staff should:

- Feel empowered to contribute effectively to collaborative online activity when it supports the work of the organisation, and its vision and values

- Be aware of the organisational stance and their own personal responsibilities for the appropriate use of social media and online access
- Be aware of what constitutes unacceptable or inappropriate use and of the consequences of such use

Staff should not:

- Breach the confidentiality of staff, patients or the Trust
- Bring the Trust into disrepute by posting content that is inappropriate or unacceptable

3 Definitions

For the purposes of this policy, “social media” shall be defined as any online communication channel which facilitates networking via the World Wide Web, which is not developed by the Trust, including but not limited to:

- social networking and “micro-blogging” websites and services, such as Twitter, Facebook, Google+ and LinkedIn
- video and image sharing sites, such as Pinterest, Instagram, YouTube, Vimeo and Vine
- personal websites
- personal blogs

A “social media account” shall be defined as any page, group or other specific channel of communication set up using social media.

More detailed definitions are included below.

3.1 Social media

Social media refers to websites and related products or services – such as mobile phone apps – which allow quick and dynamic (usually public) interaction between users. Social media includes, but is not limited to: blogs, provided by platforms such as Blogger, WordPress and Tumblr; online video hosting services like YouTube and Vimeo; photography and videography platforms such as Instagram and Vine; micro-blogging sites, the most popular of which is Twitter; professional networks, including LinkedIn; and social networking sites like Bebo, MySpace, Facebook and Google+. For the purposes of this policy and associated procedure, social media shall also include online forums, personal websites and blogs

3.2 Blogs

A blog (short for “web log”) is a website which allows somebody to create short articles (“posts”), usually available chronologically and sortable by date or category. Each post usually has a comments section which allows readers to post feedback. Blogs can belong to and be updated by an individual or multiple authors

3.3 Twitter

Twitter is a “micro-blogging” site. Unlike a more traditional blog, posts – known as tweets – are limited to 140 characters. Anyone can join twitter and start to follow other users. Tweets from users they follow will show in a user’s timeline (on their home page on the website or in a feed as part of an app). Users can post text or links to other websites, or media such as video content or photos. It’s also possible to send private messages to other users – also limited to 140 characters. [About Twitter](#). The Trust has a [Twitter account](#) which is managed by the communications team.

Tweets can be set to private and will only be seen by your followers.

3.4 Facebook

Facebook is a social networking site built largely on the connections between “friends”. Users can become Facebook friends with other users by sending them friend requests and having these accepted. Organisations can also set up Facebook “pages”, which other users can “like” in order to receive updates on products, services and other news. Users can post links to other websites, and can post photos and videos via Facebook itself. It’s possible to configure privacy settings to control how much other users can see. Facebook also has a private messaging feature. Privacy settings can be adjusted, so personal information, posts and photos can only be seen by people you know. Other social networking sites include Bebo, MySpace and Google+.

3.5 Snapchat

Snapchat is an app that’s primarily used for creating multimedia messages referred to as “snaps”; snaps can consist of a photo or a short video, and can be edited to include filters and effects, text captions, and drawings.

3.6 YouTube

YouTube is a website built on the ability for anyone to post, share and comment on videos. Videos can be linked to from other social media tools and can also be embedded into other websites. Settings for each video can be configured to control who can see, comment, rate and respond to it. [About YouTube](#)

3.7 LinkedIn

LinkedIn is a professional network, allowing users to connect with colleagues present and past, and to promote themselves to prospective employees and other professional contacts.

3.8 WhatsApp

WhatsApp Messenger is a cross-platform mobile messaging app which allows you to exchange messages without having to pay for SMS. WhatsApp Messenger uses the same internet data plan that you use for email and web browsing. In addition to basic messaging WhatsApp users can create groups, send each other unlimited images, video and audio media messages.

3.9 Trolls

A troll is a user who posts content with the chief intention of offending or abusing other users of the internet.

3.10 Viral effect

The viral effect explains the process via which messages are spread across social media. One user posts content, which is then reposted by multiple other users, and in turn by yet more users, enabling content to spread like a “virus”

4 Policy Requirements

The Director of Communications shall approve all procedural documents associated with this policy, and any amendments to such documents, and is responsible for ensuring that such documents are compliant with this policy.

There are many benefits to the Trust in using social media, but to maximise these, and to reduce the risks, it's essential that staff conduct themselves in the correct manner:

- When using social media in a personal capacity, it's essential that staff do not post any content which jeopardises their employment and/or brings the Trust into disrepute.
- Personal usage of social media should only take place outside work hours or during breaks.
- Requests for the creation of Trust social media accounts – i.e. those set up by and on behalf of the Trust – must be sent to the communications team, who will then begin the approval process for the account. The final say on whether a Trust account may be created belongs to the Executive Team.
- The team which owns and manages the account must work with the communications team on the creation and maintenance of the account, and must share the login details.
- When using Trust social media accounts, staff must follow the best practice, rules of conduct and other guidance set out in the Social Media Procedure. Failure to do so may result in disciplinary action and could lead to dismissal.
 - It should be outside of working hours or during breaks.
 - It should not interfere with work performance.
 - It must not be used for personal profit (e.g. running a business) nor for the benefit of any non NHS organisation
 - It must comply with the provisions of this policy

5 Role and Responsibilities

5.1 Directors

The Executive Team will review all requests for the creation of social media accounts to be used on behalf of the Trust, and is responsible for approving or rejecting these requests. It shall also consider any special conditions or circumstances which may affect the approval or rejection of such a request.

5.2 Local Managers

Managers (Band 8C or above) must ensure that any of their staff wishing to use social media on behalf of the Trust adhere to this policy and its associated documents. Responsible managers must approve any requests for accounts to be used on behalf of the Trust before the request for the account is sent to the Communications team, and must assign and approve the relevant resources to manage the social media account. They must also raise any concerns over the conduct of their staff relating to the use of social media, in either a personal or professional capacity, to the Communications team, Director of Communications, the Governance team and/or an appropriate senior manager, as necessary

5.3 Other Individuals

5.3.1 Director of Communications

The Director of communications is responsible for the implementation of this policy and accompanying procedure. The Director of Communications will also review any requests for new social media accounts to be used on behalf of the Trust and will present these to the Executive Team for approval

5.4 All Staff

All staff using social media should make themselves familiar with this policy and accompanying procedure, and must ensure that their use of social media does not breach the requirements of the policy and procedure. Any “approved staff” - i.e. those staff granted access to use social media in a professional capacity – must ensure adherence to this policy and the accompanying procedure, including attendance at any relevant training.

They must also comply with the requirements of any guidance or policies issued by any applicable professional bodies including, but not limited to, the Nursing and Midwifery Council and the General Medical Council. Approved staff will agree to the login details for their professional social media accounts being shared with the Communications team.

If they leave the Trust or the team on behalf of which the account is used, approved staff will ensure that management of the social media account for which they are responsible is passed to another member of their team, approved by the responsible manager. Passwords must be changed and admin access revoked for departing member of staff where possible. If no staff member is available to hand over to, ownership of the account must be handed over to the Communications team, who will arrange to have the account managed elsewhere or close the account.

Trust staff must ensure that any content published is consistent with their role in the organisation and doesn't compromise their own reputation or that of the Trust, and doesn't breach patient, staff or the Trust's confidentiality. Staff must follow the guidance in the Social Media Procedure to ensure their usage does not bring the Trust into disrepute or

otherwise breach Trust policy or break any law when they are setting up personal social media accounts.

5.5 Specific groups / committees

5.5.1 Communications team

The Communications team is responsible for reviewing the policy and associated documents, for monitoring compliance and for handling any queries relating to the policy. They have devised a proforma which staff must use to submit their requests for the creation of social media accounts to be used on behalf of the Trust. The team shall also conduct the initial review of new social media accounts and present these to the Director of Communications, work with staff members to set up any approved accounts intended for use on behalf of the Trust and deliver any necessary training. They will review usage of all Trust social media accounts no less frequently than once a week and will conduct a quarterly review of each account. They will also maintain a register of all active social media accounts set up on behalf of the Trust and review this register on a quarterly basis.

5.5.2 IT Services department

IT Services will grant access to social media websites via Trust network accounts for staff managing social media accounts which have been approved by the Executive Team. The department will also liaise with the Communications team to ensure that access is revoked in the case of misuse, if deemed appropriate.

6 Training

The Communications team are available to offer guidance on the appropriate use of social media for staff who will be using it as part of their duties. Bespoke sessions can be set up as and when they are required.

7 Monitoring Matrix

See **Appendix A**

8 References

Nottingham University Hospitals NHS Trust. Corporate Use of Online Social Networks Policy. (Cited 2 June 2014.)

Norfolk and Norwich University Hospitals NHS Foundation Trust. Policy on the Personal Use by Staff of Social Media. (Cited 28 July 2014.)

Appendix A - Monitoring Matrix

MONITORING OF IMPLEMENTATION	MONITORING LEAD	REPORTED TO PERSON/GROUP	MONITORING PROCESS	MONITORING FREQUENCY
Keeping records of submission requests for new social media accounts	Communications Officer	Director of Communications	Short summary will form part of the social media activity report	Monthly
Daily monitoring of social media posts mentioning HEFT	Communications Officer	Director of Communications	<p>Concerns and compliments will be sent to the relevant department and Patient Services team.</p> <p>Number tallies will be kept within the Communications team, included as part of social media activity report</p>	Daily
Weekly monitoring of dedicated HEFT social media accounts	Communications Officer	Director of Communications	Checked weekly to ensure the account is being regularly updated and that content is appropriate. If not, it will be escalated to line manager in the first instance	Weekly