Joint Policy for Cumbria Partnership Foundation Trust & North Cumbria University Hospital NHS Trust

Policy Title: Social Media Policy

Reference	POL/COR/008
Version	1.0
Date Ratified	14/05/2019
Next Review Date	March 2022
Date Published	06/06/2019
Accountable Director	Executive Director of Workforce, OD & Engagement
Policy Author	Head of Communications (NCUH)

Please note that the Intranet / internet Policy web page version of this document is the only version that is maintained.

Any printed copies or copies held on any other web page should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.

Policy On A Page

SUMMARY & AIM

This policy aims to ensure that all Trust employees are aware of their responsibilities in relation to the use of social media and to provide a framework of good practice. This applies to all websites and channels, including those not operated by the trusts and also apply irrespective of whether the activity occurs on trust premises or outwith.

The objective of these guidelines is to ensure that staff make best use of social media channels while maintaining the Trust's professional image, avoiding misuse and protecting individual staff. It is also essential that staff adhere to Data Protection and confidentiality requirements.

The risk of misuse by staff of any social media can be quantified as both financial and reputational. In the event of a breach of information, the Information Commissioner (ICO) has the ability to fine trusts and this is also made public upon investigation. In addition, if anyone is found to be harassing an individual through social media, this can be a criminal charge in line with the Protection from Harassment Act 1997.

KEY REQUIREMENTS

- Staff are responsible for how they portray the trusts and their profession when they are using social networking site. They must comply with the requirements of the Data Protection Act 2018 and General Data Protection Regulation (GDPR), the code of confidentiality and any relevant professional codes of conduct even when they are off-duty

- Staff must consider the potential impact on both the reputation of themselves and the trusts when they use such sites

TARGET AUDIENCE:

This policy applies to all employees of CPFT and NCUH who use web-based social networking sites whether or not they have identified themselves as members of a profession or as an employee of our organisations.

TRAINING:

Information governance training is provided to all members of staff at their induction, followed by the mandatory training which also covers information governance issues.
In addition, a 'social media toolkit' is available on the staff website

TABLE OF CONTENTS

1. INTRODUCTION

The Trusts recognise that the use of electronic communications and the internet are widespread, and that the majority of our staff have access to computers, tablets and mobile phones both in and out of the workplace. It is important that all of these are used sensibly with regards to social media such as Facebook, Twitter and YouTube.
Please note that the absence of or lack of explicit reference to a specific site or channel does not limit the extent of the application of this policy. The application of this policy may include personal websites as well as those to which employees may subscribe.

Staff are responsible for how they portray the Trust when they are using social networking sites and must also comply with the requirements of the Data Protection Act 2018, the code of confidentiality and any relevant professional codes of conduct, even when they are off-duty.

Staff should also be aware of the positive opportunities social media offers in promoting our services and staff.

2. PURPOSE

The purpose of this policy is to ensure that:

- The trusts are not exposed to legal and governance risks from the use of social media
- The reputation of the Trusts' staff and services are not adversely affected

This policy applies to all employees of the trusts, whether permanent, part-time or temporary. It applies equally to agency, locum, fixed-term contract, seconded, student and volunteer staff.

3. SOCIAL MEDIA AND SOCIAL NETWORKING

3.1 Overview

The Trusts recognise that social networking sites (e.g. Facebook, Instagram, Snapchat,Tumblr, LinkedIn, Twitter, YouTube, What's App and blogs) can be a useful and fun way for individuals to keep in touch with friends and colleagues.

However, it must be noted that risks can arise from the use of such sites by its staff. These risks include:

- A staff member may disclose too much personal information about themselves and risk identity theft
- A staff member may disclose person-identifiable information about patients or other members of staff without authorisation and risk breach of confidence
- A staff member may make inappropriate or harmful statements about their work, colleagues or the trusts and risk breach of the relationship of trust and confidence
- Staff may be pictured in activities or make comments that could be open to misinterpretation

- Staff members may make comments in their professional capacity which go against their professional code of conduct

Staff are reminded that information posted on these websites becomes public and may be viewed by colleagues, patients, members of the public and the press.

These guidelines do not mean that a member of staff can never post comments on these websites about their work for the Trusts. However, before posting comments, the staff member should always consider whether they would be happy for their patients, colleagues or managers to read the comments, and consider what their reaction might be.

The Trusts have several official accounts on social networking sites. The Communications Team has lead responsibility for these pages and encourages all staff to submit ideas and comments for them to share with our followers. Any official accounts must have prior permission to communicate on behalf of the organisations. Contact Communications.helpdesk@cumbria.nhs.uk for more information and please also read the Trusts' Guidance on social media toolkit.
https://staff.cumbria.nhs.uk/download_file/667/753

3.2 Social networking using trust-owned equipment

Please see the 'Information & Cyber Security Acceptable Use Policy (Joint)' on the Trust website.

3.3 Social networking using privately-owned equipment

The trusts recognise that staff may access or contribute to social networking websites in their personal time outside of work, using their own equipment.

Using social media has blurred boundaries between public and private life, and online information can be easily accessed by others. Although individuals may believe they have restricted access of their personal profiles to their own audience (friend/followers list), all postings to social media websites are regarded as being in the public domain and as such potentially accessible to all.

It is important to be aware of the limitations of privacy online and privacy settings should be regularly reviewed for social media accounts for the following reasons:

- Patients, the Trust, members of the public or any other organisation that you have a relationship with, may be able to access your personal information.
- Once information is published online it can be difficult to remove as other users may distribute (share/retweet) it further or comment on it.
- Social media sites cannot guarantee confidentiality whatever privacy settings are in place and information about your location may be embedded within photographs/updates may be available for others to see.

Employees are responsible for any information they may post on social networking sites or blogs that identifies their workplace, work colleagues or users of the trusts' services. Therefore they are urged to use discretion and must not:

- Post information that is speculative or derogatory, or that could bring the trusts into

disrepute, including private messenger and using special category data under GDPR (i.e. race, sexual orientation etc.) which potentially crosses the line into harassment
- Cause embarrassment to the trusts, its members, staff, patients or the general public
- Post sensitive or confidential information about the trusts or our employees
- Post information which could potentially identify a patient (e.g. patient's name, address, postcode, ID numbers, rare condition, celebrity status etc.)
- Post comments about patients or colleagues which could cause offence, even if names are not mentioned directly
- Posting comments or images which are discriminatory or could amount to bullying or harassment
- Posting recognisable signs or pictures relating to the trusts, or any pictures of staff or patients without their explicit, fully-informed consent
- Posting information about grievances/ disciplinary processes, or any other formal and sensitive procedures
- Post material that breaches the NHS Code of Confidentiality
- Post material that breaches set professional guidelines

Staff will be held responsible and personally liable for any comments, images and information they may post relating to the trusts in any way, which may result in disciplinary action if comments or material are adjudged to have been posted with intent. Staff are also liable for actions which may be taken by patients or colleagues.

In addition, staff must not send or post communications which encourage behaviour that could be linked to safeguarding issues, for example:

- Bullying
- Luring and exploitation/ grooming
- Building or pursuing relationships with patients or service users
- Theft of personal information
- Encouraging self-harm or violence
- Inciting hatred or discrimination including homophobic or race related comments - anything that covers the special category data under DPA 2018
- Glorifying activities such as excessive drinking or drug taking

Staff are reminded that they will be held responsible and personally liable for any material intentionally or unintentionally posted relating to the Trust in any way. A breach of this may result in action taken in line with the trusts' disciplinary policy on the Trust website.

3.4 Guidance on the use of social networking websites

Staff are offered the following advice if they decide to use social networking websites:

- Tweet discreet: on social media be aware what you say. Do not reveal any Trust information without approval. Do not reveal personal details such as your date of birth or contact details. Disclosing such information may raise the risk of identity fraud.

- Follow the rules – All information must be processed fairly, lawfully and transparently – please refer to the Joint Data Protection Policy

- It has been known for NHS staff occasionally to have to take out restraining

orders on obsessive patients – employees with concerns relating to this may not wish to use public networking websites.

- Before posting images or joining any campaigns/causes, be aware that patients, colleagues and managers may see this information.
- If, after careful consideration, you decide to post comments relating to your work in any way, you should make it clear that the comments expressed are your own and not those of your employer**.**
- Social media activities must not interfere with work commitments
- Trust logos should not be used without consent
- If you wish to set up an 'official' social media account to represent your service, please refer to the social media guidance toolkit and contact the Communications team in advance of setting an account up

3.5 Usage concerns

Where staff are harassed, bullied or victimised by a message or post from another member of staff or from a patient or visitor, whether inside or outside of work, and, the individual does not respond to an initial request for the activity to stop, contact your line manager, HR Advisor, Freedom to Speak Up Guardian or staff representative in the first instance.

Staff considering themselves to be at risk of receiving inappropriate or obsessive attention from patients via social networking sites should seek advice from line management or HR.

3.6 Professional codes of practice

Staff who are members of a professional body must be aware that posting inappropriate comments about colleagues or patients may put their professional registration at risk if they do so. The Nursing and Midwifery Council, General Medical Council and other professional bodies provide guidance with regards to standards of conduct and performance and ethics.

The Nursing and Midwifery Council has also published specific guidance on its website about social networking: http://www.nmc-uk.org/Nurses-and-midwives/Advice-by-topic/A/Advice/Social-networking-sites/

3.7 Social networking and recruitment

The policy of the trusts is not to use information gained from social networking sites as part of its recruitment process but staff must be aware that potential employers may see their social network profile and you may wish to consider how you may be perceived as a result of what you post on a social network site.

3.8 Organisational use of social media

We have several social media accounts with thousands of followers and high levels of engagement which are managed by the Communications team. Contact the team if you have information you would like to share through these.
Facebook:

- Cumbria Partnership NHS Foundation Trust: Facebook
- North Cumbria University Hospitals NHS Trust: Facebook

Twitter:

- Cumbria Partnership NHS Foundation Trust: Twitter
- North Cumbria University Hospitals NHS Trust: Twitter

You Tube:

- Cumbria Partnership NHS Foundation Trust: YouTube
- North Cumbria University Hospital Trust: YouTube

3.9 Recording of patient consultations

Generally patients do not need their doctor or clinician's permission to record a medical (or other) consultation or treatment. Patient recordings which are made either covertly and overtly in order to keep a personal record of what the doctor/staff member said are deemed to constitute personal 'note taking' and are therefore permissible.

NHS Protect has produced formal guidance – *"Patient recording NHS staff in health and social care settings May 2016"* which sets out some useful practical guidance for NHS bodies.

If a formal request to record a consultation were to be made by a patient or their family then potentially that itself may not be a problem, and could in fact improve engagement and help to foster a more constructive relationship with that individual. However, problems may arise if such recordings were then to be distributed on a social media platform or by other means. This would open up concerns about recordings being edited or taken out of context and only showing part of the true picture of what had been said. If shared publicly, identification of the patient (possibly deemed a vulnerable person) becomes a real concern.

Although staff cannot place restrictions on a patient wishing to record notes of a consultation or conversations with a health professional, where it is felt absolutely necessary by the patient to do so, staff should ensure that:

- any recording is done openly and honestly
- the recording process itself does not interfere with the consultation process or the treatment or care being administered
- the patient understands that a note will be made in their health record stating that they have recorded the consultation or care being provided
- the patient is reminded of the private and confidential nature of the recording and that it is their responsibility to keep it safe and secure
- any recording is only made for personal use and not for wider circulation such as social media

- patients are aware that the misuse of a recording may result in criminal or civil proceedings
- patients are discouraged from undertaking recordings in the first place, unless it is deemed absolutely necessary highlighting the above responsibilities.

4. TRAINING AND SUPPORT

Information Governance training is provided to all members of staff at their induction, followed by mandatory training which also covers information governance issues. The Communications team is another point of contact for any training requests regarding social media use.

5. PROCESS FOR MONITORING COMPLIANCE

The process for monitoring compliance with the effectiveness of this policy is as follows:

Aspect being monitored	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
Breaches of confidentiality	Reporting through the trusts' incident reporting processes	Head of Information Governance / Data Protection Officer	Information Governance Group	Quarterly
Serious incidents/breaches	Reporting through the trusts' incident reporting processes	Medical Director/Chief Nurse	Quality & Safety Committee	Monthly

Wherever the above monitoring has identified deficiencies, the following must be in place:

- Action plan
- Progress of action plan monitored by the Information Governance Committee minutes
- Risks will be considered for inclusion in the appropriate risk registers

6. REFERENCES:

General Medical Council: Confidentiality – Guidance for Doctors
http://www.gmc-uk.org/static/documents/content/Confidentiality_core_2009.pdf

General Medical Council; Good Medical Practice – Respect for Colleagues
http://www.gmc-uk.org/guidance/good_medical_practice/working_with_colleagues_respect_for_colleagues.asp

Nursing and Midwifery Council: Guidance on the use of Social Networking sites:

http://www.nmc-uk.org/Nurses-and-midwives/Advice-by-topic/A/Advice/Social-networking-sites/

Nursing and Midwifery Council: Standards of conduct, performance and ethics for nurses and midwives
http://www.nmc-uk.org/Documents/Standards/The-code-A4-20100406.pdf

7. ASSOCIATED DOCUMENTATION:

Information & Cyber Security Acceptable Use Policy
Confidentiality Policy
Data Protection Act Policy
Dignity at Work Policy & Procedure
Disciplinary Policy
Media Management Policy
Guidance for social media toolkit

8. DUTIES (ROLES & RESPONSIBILITIES):

8.1 Chief Executive / Trust Board Responsibilities:

The Chief executive has ultimate responsibility for ensuring that the appropriate Information Governance policies and procedures are in place and enacted accordingly.

8.2 Executive Director Responsibilities: Executive Director of Workforce, OD & Engagement

All policies have a designated Executive Director and it is their responsibility to be involved in the development and sign off of the policies, this should ensure that Trust policies meet statutory legislation and guidance where appropriate. They must ensure the policies are kept up to date by the relevant author and approved at the appropriate committee.

8.3 Caldicott Guardian Responsibilities:

The Caldicott Guardian is appointed by the Trust Board to oversee the safe and secure use and sharing of patient information. The role holder takes a lead role in respect of Clinical Information Assurance Requirements.

8.4 Managers Responsibilities:

Line managers are responsible for ensuring their staff are aware of this policy and report any serious breaches appropriately.

8.5 Joint Head of Information Governance / Data Protection Officer:

The Trust Head of Information Governance / Data Protection Officer will provide the Information Governance Group with reports on any information security related incidents.

8.6 Staff Responsibilities:

Staff are responsible for ensuring that they comply with this and related policies.

8.7 Joint Information Governance Board Responsibilities:

The group will receive reports from the Head of Information Governance / Data Protection Officer with regard to breaches of confidentiality. The group will oversee any action that is required as an outcome of the reports.

8.8 Communications team

The Communications team is responsible for managing and updating the content on the trusts' official social media accounts as well as providing guidance and support to other staff members as appropriate. The team will also report any incidents that arise on the trusts' official accounts.

9. ABBREVIATIONS / DEFINITION OF TERMS USED

ABBREVIATION	DEFINITION
GDPR	General Data Protection Regulation
ICO	Information Commissioner

TERM USED	DEFINITION
Social Media	Social media includes the various online technology tools that enable people to communicate via the internet, to share information and resources. Social media can include text, audio, video, images, podcasts and other multimedia communications
Social Networking	Web-based social networking occurs through a variety of websites allowing users to share content, interact and develop communities around similar interests. Examples include Facebook and Twitter.

DOCUMENT CONTROL

Equality Impact Assessment Date	
Sub-Committee & Approval Date	*Joint Information Governance Board 17/05/2019*

History of previous published versions of this document:

Trust	Version	Ratified Date	Review Date	Date Published
NCUH IG25	3.0	01/02/2016	31/01/2019	09/02/2016

Statement of changes made from previous version

Version	Date	Section & Description of change
V0.1	28/03/2019	Joint policy based on NCUH policy. No equivalent policy at CPFT
V0.2	15/05/2019	General amendments

List of Stakeholders who have reviewed the document

Name	Job Title	Date
Kath Hughes	Head of engagement & communications, CPFT	15/04/2019
Angela Jeffries	HR business partner, CPFT	15/04/2019
Laura Irving	Communications officer, CPFT	08/04/2019
Julie Clayton	Head of communications & engagement, NHS North Cumbria CCG	05/04/2019
Wendy Forster	Communications officer, CPFT	05/04/2019
Andrew Butler	Communications advisor, NCUH	04/04/2019
Derrick Bates	Information & Cyber security officer, NCUH	04/04/2019
Yvonne Salkeld	Joint head of information governance	09/04/2019