County Durham and Darlington NHS
NHS Foundation Trust

CDDFT Policy	
Reference Number	POL/HI/IG/041
Title	**Social Media Policy**
Version number	1.0
Document Type	Policy
Original Policy Date	October 2018
Date approved	November 2018
Effective date	November 2018
Approving body	Integrated Quality Assurance Committee
Originating Directorate	Health Informatics Department
Scope	Trust Wide
Last review date	October 2018
Next review date	September 2021
Reviewing body	Data Security and Protection Committee and Informatics Strategy Sub Committee
Document Owner	
Equality impact assessed	Yes – Oct 2018
Date superseded	New Policy
Status	Approved
Confidentiality	Staff in Confidence
Keywords	Social Media Policy

Approval

Signature of Chairman of Approving Body	
Name / job title of Chairman of approving Body:	
Signed paper copy held at (location):	Corporate Records Office DMH

Table of Contents

Document Management Information

Version Control

Date	Version No	State	Author
Oct 18	1.0	Draft	HODSP

Authorised Revisions			
Date	**Section**	**Details**	**Authorised By:**
October 2018	all	New Policy	DSPC / ISSC / IQAC

1. Introduction

Social media is now part of everyday life for millions of people and has a significant impact on organisational, professional and individual reputations. This policy outlines the appropriate use of social media by employees of the Trust including staff employed in Trust subsidiary companies (all Trust staff); agency staff, Trust governors, volunteers, students undertaking education and training and staff from other organisations working on Trust premises.

It sets out the responsibility of individuals when using social media, both in a personal and professional capacity, in order to maximise benefits and minimise risks and is in line with national guidance from the NHS and a number of professional bodies.

2. Purpose

The social media policy outlines expected behaviours and personal responsibilities for all Trust staff (and others listed above) when using social media. Staff should follow the same behaviour standards online as they would in their everyday roles and abide by their legal and ethical duties to protect patient/service user and colleague confidentiality.

The policy applies to Trust staff when accessing social media either on computers, laptops, tablets or smart phones owned or controlled by the Trust or connected to the Trusts network, or on their own personal laptops, tablets or smart phones.

The Trust acknowledges the right of all staff to freedom of expression and recognise that all staff are entitled to use social media in a personal capacity. This policy is not to stop the use of social media but provides up-to-date guidance to avoid potential problems arising for both individual staff members and the Trust.

3. Duties

3.1. Board of Directors

The Board of Directors is responsible for ensuring there is a robust system of corporate governance within the Trust. This includes ensuring that the Trusts' policies comply with all legal, statutory and good practice requirements in relation to social media.

3.2. Chief Executive

The Chief Executive is accountable for ensuring the proper application of this policy through effective management arrangements.

3.3. Head of Communications & Charity

The Head of Communications and Charity for the Trust has delegated responsibility on all issues relating to media and social media, including the development, upkeep and sharing of this policy via internal communications across the Trust.

3.4 Caldicott Guardian

The Trust Caldicott Guardian has a strategic role which involves representing and championing patient confidentiality, ethical processing and issues at senior management level. As such, the Caldicott Guardian will be called upon for advice in relation to social media usage and any circumstances where staff may have contravened this policy in relation to patient confidentiality.

3.5 Data Protection Officer

The Data Protection Officer has a responsibility for all Trust information and advises on options for lawful processing of information. As such, the Data Protection Officer will be called upon for advice in relation to social media usage and any circumstances where staff may have contravened this policy in relation to Trust information.

3.6 Line Managers/Supervisors/Matrons/Ward Managers

All managerial staff across the Trust are responsible for ensuring adequate implementation of this policy amongst all Trust staff and those within the scope of this policy.

3.7 Corporate affairs / Trust Secretary

The Trust Secretary is responsible for ensuring adequate implementation of this policy amongst Trust governors. An addendum to the Governors code of conduct in respect to social media and the conduct of Governors will be developed with the Governors signing this to confirm their agreement and compliance from February 2019.

3.8 All Trust staff (including locum, agency staff, honorary contract holders and volunteers)

All staff are responsible for complying with this policy. Everyone who chooses to use social media, either for personal or professional use, must adhere to this policy or report any potential misuse of social media to line managers.

4. Social Media Requirements

4.1. Standards for Trust employees

This policy applies to staff use of social media both in a personal and professional capacity and has been produced in accordance with social media guidance from a range of professional bodies (see references in section nine). All staff are reminded of their ethical duties as qualified health and social care professionals and as representatives of the NHS and should never compromise their own professional codes of conducts when using social media.

4.2. Legal responsibilities

The use of social media to share information and comment must always take account of principles outlined in the Data Protection Act 2018 (and the General Data Protection Regulation) for personal or individually identifiable information relating to patient/service users, carers, staff or other individuals. Content posted will remain online indefinitely and, as published information, is subject to the same laws and legislation as traditional media, e.g. libel / defamation.

4.3. Organisational use of social media

Trusts are increasingly using social media in an organisational capacity to share information and gain valuable feedback about services and experiences. This activity is coordinated and managed by the Trusts communication team at a corporate level. Teams must not set up social media accounts which purport to represent the views of the Trust. Any departments wishing to use social media to promote their work must liaise with the communications team.

4.4. Requirements for staff

As social media blurs the lines between personal voice and organisational voice, the following requirements for staff clarify how best to enhance and protect personal and professional reputations when using social media:

4.4.1. Responsibility as an employee

When posting on social media sites, whether or not staff have identified themselves as an employee of the Trust, staff must behave appropriately and in line with the Trust's wider values and policies, taking account of all relevant legislation covering personal confidentiality, e.g. The Data Protection Act 2018 (and the General Data Protection Regulation). Every member of staff carries individual responsibility as an NHS employee, or when representing the NHS, and in line with professional codes of conduct when using social media, staff must:

- **never** reveal confidential information about patient/service users, staff or organisational business
- **never** engage in activities or comment which might bring the Trust directly into disrepute
- **never** post defamatory, derogatory or offensive comments about colleagues, patient/service users or the Trust

Staff must not display work email addresses unless in a professionally related capacity. Staff who do not directly identify themselves as Trust employees when using social media, must be aware that the content they post could still be considered as relevant to their employment with the Trust (for example by posting any racist, sexist or other derogatory remarks).

Any member of staff who brings the Trust into disrepute when using social media, for example by engaging in comments or activity which could potentially damage or undermine the reputations of other staff, the Trust and / or public confidence in the NHS, could potentially face disciplinary action in line with the Trust's Disciplinary Procedure.

All staff should be aware that the Public Interests Disclosure Act 1998 gives legal protection to employees who wish to 'whistleblow' any concerns. The Act makes it clear that the process of 'whistleblowing' or 'speaking up' involves raising the issue internally first. Using social media to whistleblow is not considered appropriate and all staff should raise concerns through established internal channels. The Trust has a Raising Concerns Policy available on the Trust Intranet.

The Trust has clear channels in place for staff to raise concerns through Freedom to Speak Up Guardians and Ambassadors. Further details can be found on the Trust intranet.

4.4.2. Think twice before posting content

Privacy does not exist in the world of social media and photographs, videos and comments can be shared easily, even when privacy settings are set appropriately. Staff must consider what could happen if something they post becomes widely known and how that may then reflect on them personally, professionally, and on the Trust. Comments can be easily forwarded, copied or photographed and staff should not post comments online that they would not say in public or in the workplace.

When attending events, awards, conferences and even in day-to-day business, the role of social media is integral, however staff must always be considerate to other colleagues by seeking verbal consent for any content to be shared and must not post information if they have been asked not to. Staff must also remove information about a colleague if that colleague asks them to do so or could potentially face disciplinary action in line with the Trust's Disciplinary Procedure.

4.4.3. Be respectful

Content on social media sites can easily encourage follow on comments or discussion of opposing ideas and staff should consider carefully how any resulting debate would reflect on them personally, professionally and on the Trust. Under no circumstance should derogatory, abusive or personal comments be made about patient/service users, Trust colleagues**,** Trust business, or Trust partners. This may amount to cyber-bullying and could be subject to disciplinary action.

4.4.4. Social networking sites

Social networking sites like Facebook and Twitter provide a great way for people to keep in touch but also provide opportunities for third parties to collate vast amounts of information and share ideas. Staff should be mindful of the personal information they disclose on social networking sites. Where staff associate themselves with the Trust (through providing work details or joining a Trust or NHS network/fan page), they should also act in a manner which does not bring the Trust or their profession into disrepute. This applies to both open and private sections of a site if staff identify themselves as employees of the Trust.

If anyone within the scope of this policy is contacted by the media about posts they have made on a social networking site in relation to their role, or the NHS, they must inform the communications team before responding. Equally, if an individual is contacted by a journalist who has found their contact details online and wishes to discuss their role, or the NHS, they must inform the communications team before responding.

4.4.5. Use of social media in a personal capacity during working hours

We recognise that some staff may use social media as part of their professional roles, however, personal use of social media is not permitted during working hours where it is not part of their professional role e.g. Communications team. The use of social media on Trust IT equipment is restricted as these sites can contain vulnerabilities that negate the effectiveness of security software and take up a lot of bandwidth on the Trust's networks.

If there is a specific business need to access such social media sites via Trust equipment, approval should be sought from the communications team and via the ICT service desk. Authority will only be given where a clear business need is identified.

Staff using their own personal smart phone devices to access social media during working hours for personal reasons must restrict this to designated break times only i.e. during a lunch or comfort break, or outside of normal working hours (before or after a shift).

4.4.6. Commenting in online discussions

Many staff may already be actively involved with social media and comment in online discussions to give their point of view or share ideas about various areas of work. This positive professional involvement is encouraged by the Trust but employees must always act in accordance with this policy.

4.4.7. Editing websites

If staff find any errors about the Trust on websites such as Wikipedia or LinkedIn please alert the communications team to agree an appropriate response before making any changes. Please note:

- If staff edit any entries themselves from Trust equipment, the source of the correction may be recorded as a NHS IP address and staff should therefore be aware of the tone and language used and not post any derogatory or offensive comments. If correcting an error, staff must also be transparent about who they are and the capacity in which they are responding.
- Criticism of the Trust must never be removed but instead reported to the communications team who will agree an appropriate response.
- Any derogatory or offensive comments relating to the Trust must not be removed but instead reported to the communications team who will agree an appropriate response.

4.4.8. Professional and personal blogging

Any staff who have professional or personal blogs in relation to health and social care must inform the communications team and ensure any content is in line with this policy and the responsibilities outlined in section 5.4.1. In these cases, if a blog makes it clear that the author works for the Trust and/or the NHS, it should include a clear disclaimer such as “these are my personal views and not those of my employer”. The Trust logo must never be used on personal web pages.

Personal blogs and websites must not reveal confidential information about patient/service users, other staff, or organisational business of the Trust, for example, any aspects of the Trusts plans, or details of internal discussions. This would be treated as a breach of confidentiality and staff could potentially face disciplinary action in line with the Trust Disciplinary Procedure. If in doubt about what might be confidential, staff must consult the communications team. If a staff member thinks something on a blog or website gives rise to a conflict of interest or has particular concerns about impartiality or confidentiality, this must be raised via the communications team and corporate affairs. If a staff member is offered payment to produce a blog for a third party this could constitute a conflict of interest and must be discussed the communications team and corporate affairs.

4.4.9. Guidance around instant messaging apps

NHS Digital have recently published their Information Governance consideration for staff on the use of instant messaging software in acute clinical settings v1.0 (09/11/18)[1].

A proportionate approach is needed: staff need to balance the benefits and risks of instant messaging depending on the purpose for which they wish to use it (e.g. using it in an emergency versus as a general communication tool). Whilst complying with data protection legislation.

The choice of app is very important:

- **Encryption** – does the app meet the NHS end-to-end encryption standard of "AES 256"?
- **End-user verification** – can the app verify that the people using the app are indeed who they say they are?
- **Passcode protection** – can a secondary PIN be used to protect the app, and can it be time-out enabled?
- **Remote-wipe** – can the messages be removed if the device is lost, stolen or redeployed to another staff member?
- **Message retention**[2] – does the app allow automatic deletion of messages after a set period of time?

Be sure to follow your organisation's policies in relation to mobile devices and instant messaging. Remember too that losing your device will now have professional as well as personal ramifications.
The National Cyber Security Centre (NCSC) publishes helpful advice on how best to secure your device, including advice that is specific to different operating systems.4 In particular:

- Don't allow anyone else to use your device
- Set your device to require a passcode immediately, and for it to lock out after a short period of not being used
- Disable message notifications on your device's lock-screen
- Enable the remote-wipe feature in case your device is lost or stolen

App Usage

• **Ensure you are communicating with the correct person or group, especially if you have many similar names stored in your personal device's address book**

- If you are an instant messaging group administrator, take great care when selecting the membership of the group, and review the membership regularly
- Switch on additional security settings such as two-step verification
- Review any links to other apps that may be included with the instant messaging software and consider whether they are best switched off
- Separate your social groups on instant messaging from any groups that share clinical or operational information
- Unlink the app from your photo library

[1] https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/information-governance-resources/information-governance-and-technology-resources use of instant messaging software in acute clinical settings v1.0 (09/11/18) NHS England Publications Gateway Reference: 08496 Prepared by: Kiran Mistry, Data Sharing and Privacy Unit, NHS England

[2] 1 It is important to handle all medical records in line with all relevant legislation, codes of practice and guidance, such as the General Medical Council (GMC) Code of Confidentiality.

The Trust acknowledges that many staff use some instant messaging tools in a personal capacity and that instant messaging can have great value, however this does not replace other formal routes of communication with colleagues.

All staff are reminded that it is against the law to reveal any detail that could identify a patient via these channels and could result in the Trust receiving a large fine and the member of staff facing disciplinary action.
Until this guidance is available and made clear to the NHS, under **no circumstances** should CDDFT personal identifiable information, including special category data be shared in this way.

5. Definition

Social media supports social interaction and, by definition, is highly accessible via data enabled devices. It involves online communities or networks of people sharing information, ideas and engaging in dialogue. Examples of 'social media' which are included in this policy are (but not limited to):

- social networking sites (Facebook, LinkedIn, Google+)
- blogs and micro-blogs, (Twitter, WordPress)
- content sharing websites, (Flickr*,* YouTube, Instagram, Prezi.com, Pinterest)
- 'wikis' (Wikipedia, LinkedIn) - websites which allow users to add, modify or delete content
- audio and video podcasts
- message or discussion applications (WhatsApp / Snapchat)
- dating websites

Further definitions of social media terms are provided in **Appendix A**.

Caldicott principles – The Caldicott Principles were developed in 1997 following a review of how patient information was handled across the NHS. In 2013, Dame Fiona Caldicott completed her second Information Governance Review and introduced a seventh principle:

- justify the purpose
- don't use personal confidential data unless it is absolutely necessary
- use the minimum necessary personal confidential data
- access to personal confidential data should be on a strict need-to-know basis
- everyone with access to personal confidential data should be aware of their responsibilities
- comply with the law
- the duty to share information can be as important as the duty to protect patient confidentiality.

6. Key Performance indicators

To ensure compliance with legislation
To ensure all staff are aware of their responsibilities when using social media and linked to the Trust.

To monitor social media where any CDDFT information has been added or responded to by CDDFT staff.

7. References

- General Medical Council (2013) Doctors' use of social media
- Royal College of Nursing (2015) Getting started on Twitter
- Nursing and Midwifery Council (2016) Guidance on using social media responsibly
- Royal College of GPs (2013) Social media highway code
- Health and Care Professions Council (2012)
- Public Health England (2015) Social Media Use
- Department of Health Digital guidance and best practice for the health and care system
- NHS Employers (2013) HR and Social Media in the NHS
- NHS Employers (2016) Social media guidelines and tools
- NHS Confidentiality Code of Practice (2003)
- NHS Caldicott Principles (2013)
- Public Interests Disclosure Act 1998
- Data Protection Act 2018
- General Data Protection Regulation 2018

8. Trust Associated Documents

IT Security policy
IT Security Incident Management policy
Trust Incident Management policy
Data Protection policy
Internet and acceptable use policy
Email code of practice and policy
Disciplinary policy
Raising concerns at work (Whistleblowing) policy
Mobile Devices policy
Mobile Communication policy
Transferring personal information policy

9. Appendix

Appendix 1 – Equality Impact Assessment
Appendix 2 – Dissemination plan

Appendix 1: Equality Analysis / Impact Assessment

Division/Department:	Nursing / Health Informatics
Title of policy, procedure, decision, project, function or service:	Social Media Policy
Lead person responsible:	
People involved with completing this:	Data Security and Protection Committee

Type of policy, procedure, decision, project, function or service:

Existing ✓

New/proposed □

Changed □

Date Completed: 17/10/18

Step 1 – Scoping your analysis

What is the aim of your policy, procedure, project, decision, function or service and how does it relate to equality?

To ensure Trust is compliant with legislation and staff abide by the Policy.

Who is the policy, procedure, project, decision, function or service going to benefit and how?

Full Trust staff;

What barriers are there to achieving these outcomes?

None

How will you put your policy, procedure, project, decision, function or service into practice?

Full distribution Trust wide; held on staffnet policy central register

Does this policy link, align or conflict with any other policy, procedure, project, decision, function or service?

No

Step 2 – Collecting your information

What existing information / data do you have?

Follows the current policy in the trust

Who have you consulted with?

Data Security and Protection Committee

What are the gaps and how do you plan to collect what is missing?

None

Step 3 – What is the impact?

Using the information from Step 2 explain if there is an impact or potential for impact on staff or people in the community with characteristics protected under the Equality Act 2010?

Ethnicity or Race

None

Sex/Gender

None

Age

None

Disability

None

Religion or Belief

None

Sexual Orientation

None

Marriage and Civil Partnership (applies to workforce issues only)

None

Pregnancy and Maternity

None

Gender Reassignment

None

Other socially excluded groups or communities e.g. rural community, socially excluded, carers, areas of deprivation, low literacy skills etc.

None

Step 4 – What are the differences?

Are any groups affected in a different way to others as a result of the policy, procedure, project, decision, function or service?

No

Does your policy, procedure, project, decision, function or service discriminate against anyone with characteristics protected under the Equality Act 2010?

Yes □ **No** ✓

If yes, explain the justification for this. If it cannot be justified, how are you going to change it to remove or mitigate the affect?

Step 5 – Make a decision based on steps 2 - 4

If you are in a position to introduce the policy, procedure, project, decision, function or service? Clearly show how this has been decided.

Review – Data Security and Protection Committee; Approval ISSC & IQAC and loaded to staffnet with a Trust bulletin stating new reviewed policies available.

If you are in a position to introduce the policy, procedure, project, decision, function or service, but still have information to collect, changes to make or actions to complete to ensure all people affected have been covered please list:

How are you going to monitor this policy, procedure, project or service, how often and who will be responsible?

Data Security and Protection have continual assessments quarterly in place for all their policies and procedures.

Step 6 – Completion and central collation

Once completed this Equality Analysis form must be forwarded to the Trust Equality and Diversity Lead and must be attached to any documentation to which it relates.

Appendix 2: Dissemination Plan

(To be completed and attached to Policy and Guidance documents when submitted to the Committee approving this document)

Policy or Guidance (P&G) Title: **Social Media Policy**			
Date finalized **November 2018**		**Dissemination Lead** (contact details)	
Previous P&G already being used?	Yes	**If yes, what in what format and where?**	
Proposed action to retrieve expired copies of P&G: **Delete old policy from sharepoint – retain old copy and publish new copy**			

To be disseminated to	**How will be disseminated, who will do and when?**	**Paper or electronic**	**Comments**
Full Trust	Policy and procedure central library	Electronic	

Dissemination Record – to be used once Policy or Guideline Approved
Date uploaded onto the Trust's Intranet …April 2016

Disseminated To (either directly or via meetings, etc)	**Format (i.e. paper or electronic)**	**Date disseminated**	**No of copies sent**	**Contact Details / Comments**
General comments:				