Social Media Policy

January 2021

Authorship:	Senior Information Governance Specialist
Committee Approved:	NHS North Yorkshire CCG Audit Committee
Approved date:	February 2021
Review Date:	February 2024
Equality Impact Assessment:	Yes
Sustainability Impact Assessment:	Yes
Target Audience:	Governing Body and its Committees and Sub-Committees, CCG Staff, agency and temporary staff & third parties under contract
Policy Number:	NY-128
Version Number:	1.1

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
0.1	Senior Information Governance Specialist	First Draft	IGSG (Jan 2021)	
0.2	Senior Information Governance Specialist	Second Draft	Audit Committee February 2021	
1.0	Senior Information Governance Specialist	Final Approved Version		Feb 2021
1.1	Senior Information Governance Specialist	Requirement for new starters to complete Data Security training within first week of starting employment	IGSG (May 2021)	May 2021

Contents

1.0 Introduction

The world of communication is changing. Social media is changing the way we, and every organisation in the world conducts its business. Millions of people use social media responsibly every day and it is becoming an increasingly important communications tool.

For the purposes of this policy, NHS North Yorkshire Clinical Commissioning Group will be referred to as 'the CCG'.

The CCG aspires to the highest standards of corporate behaviour and clinical competence, to ensure that safe, fair and equitable procedures are applied to all organisational transactions, including relationships with patients, their carers, public, staff, stakeholders and the use of public resources. In order to provide clear and consistent guidance, the CCG will develop documents to fulfil all statutory, organisational and best practice requirements and support the principles of equal opportunity for all.

The CCG may wish to use social media to provide opportunities for genuine, open, honest and transparent engagement with stakeholders, giving them a chance to participate and influence decision making. These tools are used to build online communities and networks which facilitate peer to peer interactivity.

Staff should use their own discretion and common sense when engaging in online communication. They should know and follow the CCG Standards of Business Conduct & Declarations of Interest Policy. The same principles and guidelines that apply to staff activities in general also apply to online activities. This includes forms of online publishing and discussion, including blogs, wikis, file-sharing, user-generated video and audio, virtual worlds and social networks.

The following sections provide some general rules and best practices which you should abide by at all times.

2.0 Purpose

The purpose of this document is to provide guidance to CCG staff on social media/networking on the internet and the external use of other online tools such as blogs, discussion forums and interactive news sites. It seeks to give direction to staff in the use of these tools and help them to understand the ways they can use social media to help achieve business goals. This is a rapidly changing area and this policy is expected to be updated and amended as communication strategies evolve.

The purpose of this policy is to help protect the organisation, but also to protect staff interests and to advise staff of the potential consequences of their behaviour and any content that they might post online, whether acting independently or in their capacity as a representative of the CCG.

The aims of this document are to:

- To provide clarity to staff on the use of social media tools when acting independently or as a representative of the CCG and give them the confidence to engage effectively;
- To ensure that the organisation's reputation is not brought into disrepute and that it is not exposed to legal risk; and
- To ensure that internet users are able to distinguish official corporate CCG information from the personal opinion of staff.

3.0 Definitions / Explanation of Terms

3.1 Social Media Terms

'Social', 'social media' or 'social networking' are the terms commonly used to describe web sites and online tools which allow users to interact with each other in some way by sharing information, opinions, knowledge and interests.

The following terms are used in this document (note the below list is not exhaustive):

- Micro blogging – for example, Twitter
- Blogging – for example, WordPress, Tumblr, and Blogger
- Video sharing – for example, Flickr, Instagram, and YouTube
- Social bookmarking – for example, Reddit and StumbleUpon
- Social sharing – for example, Facebook
- Professional sharing – for example, LinkedIn

4.0 Scope of the Policy

This policy applies to those members of all staff, CCG Members, temporary staff, seconded staff, contractors and others undertaking work on behalf of the CCG. For those staff covered by a letter of authority/honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties on behalf of the CCG.

5.0 Duties, Accountabilities and Responsibilities

5.1 Accountable Officer

Overall accountability for procedural documents across the organisation lies with the Accountable Officer who has overall responsibility for establishing and maintaining an effective Information Governance Framework, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

5.2 SIRO

The CCG's SIRO is responsible for overseeing the implementation of appropriate processes and procedures to ensure that individual's information can be processed and held securely.

5.3 Caldicott Guardian

The CCG's Caldicott Guardian is responsible for overseeing and advising on issues of service user confidentiality for the CCG including breaches of confidentiality personal information.

5.4 Corporate Services Manager

Responsibility for the Social Media Policy lies with the Corporate Services Manager who has responsibility for the management, development and implementation of policy procedural documents.

5.5 Line Managers

Line managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to the use of the CCG's Social Media.

5.6 All Staff

All Staff are responsible for using social media responsibly.

Whenever employees engage with social media and post information about their work or employer it is highly likely that the information will be circulated to a wide audience.

Although members of staff are not acting on behalf of the organisation in a formal capacity when engaging with social media in their personal lives they must be mindful that, depending on the content, their online posts could potentially be damaging to the CCG, for example if they are inaccurate or flippant. Staff must also be aware of the potential legal implications of material which could be considered abusive or defamatory.

Staff must at all times comply with Data Protection Legislation and Privacy and Electronic Communications Regulations with regards to their use of social media.

All staff are mandated to undertake Information Governance training on an annual basis. This training should be provided within the first year of employment and then updated as appropriate in accordance with the Statutory and Mandatory Training Standard and Information Governance Training Needs Analysis.

5.7 Responsibilities for Approval

Audit Committee is responsible for the review and approval of this policy

6.0 Policy Procedural Requirements

6.1 Social Media in Your Personal Life

The CCG recognises that many employees make use of social media in a personal capacity. While they are not acting on behalf of the organisation, employees must be aware they can damage the organisation if they are recognised as being a CCG employee.

Although it is acceptable for staff to say they work for the NHS or CCG in posts and during online conversations, they should ensure they are clear that they are not acting on behalf of the organisation and post a disclaimer such as “the views posted are my own personal views and do not represent the views of the CCG” or “Tweets are my own views”.

All employees should be aware that the CCG reserves the right to use legitimate means to scan the web, including social network sites for content that it finds inappropriate.

Any communication that employees make in a personal capacity through social media must not:

- Bring the CCG into disrepute by criticising or arguing with customers, colleagues or rivals; making defamatory comments about individuals including judgments of their performance and character, or posting links to inappropriate content
- Breach confidentiality, for example by revealing information owned by the organisation; giving away confidential information about an individual (such as a colleague or customer contact)
- Breach the rights of data subjects under the Data Protection Act 2018 or General Data Protection Regulations.
- Include contact details or photographs of colleagues, customers or service users without their permission
- Discuss the CCG’s internal workings or its future business plans that have not been communicated to the public
- Breach copyright, for example by using someone else’s images or written content without permission or failing to give acknowledgment where permission has been given to reproduce something. If photos/videos are of the general public in public places then you can use them without obtaining permission
- Do anything that could be considered discriminatory, bullying or harassment of any individual, for example by making offensive or derogatory comments relating to protected characteristics under the Equality Act 2010
- Use social media to bully another individual or posting images that are discriminatory or offensive (or links to such content)
- Post information that breaches any of the conditions in CCG or NHS policies

Incidents of discrimination, bullying or harassment which take place via social media will be managed in line with CCG policy.

6.2 Line Manager Guidance

Under this policy managers should be clear on the social media participation for any project and that individual staff members should be identified for managing the agreed social media for the project once appropriate approvals have been received. Managers requiring guidance should contact the appropriate lead for social media in the CCG.

6.3 Guidance for staff given access to CCG Social Media

Where access has been given to use CCG social media sites, staff must not upload/post the following:

- Personal identifiable information of patients and/or their relatives
- Personal identifiable information of another CCG employee in relation to their employment including judgements of their performance and character
- Photographs or video of another CCG employee taken in the work situation without permission
- Defamatory statements about the CCG, its staff, services or contractors
- Confidential information on bulletin boards, forums or newsgroups
- '"Whistleblowing" posts, without already having raised concerns through the proper channels. All staff should be aware that the Public Interest Disclosure Act 1998 gives legal protection to employees who wish to whistleblow any concerns. HR35 Whistleblowing Policy incorporates the requirements of the Public Interest Disclosure Act 1998 (PIDA) and the Bribery Act 2010.

6.4 Photos and Videos

Video is an excellent medium for providing stimulating and engaging content, which can potentially be seen by many people as it is easily shared on social media sites and embedded on other people's websites.

Images of individuals in photos/videos are treated as personal information, in this instance, consent is required to use the images and you must take reasonable steps to tell the individual who you are, what you are taking their picture for and how they can access it. Individuals also have a legal right to remove that consent at any time. If photos/videos are of the general public in public places then you can use them without obtaining permission providing the footage is brief, incidental, and an individual is not engaged in a personal or private activity. It is considered best practice to advise people that a video is being taken either verbally or with a sign.

You must ensure that all video and media (including presentations) are appropriate to share/publish and do not contain any confidential, commercially sensitive or defamatory information.

If the material is official and corporate CCG content then it must be branded appropriately, and be labelled and tagged accordingly. It must not be credited to an individual or production company. Further guidance is available from the Information Labelling & Classification Procedure.

7.0 Public Sector Equality Duty

In developing this policy an Equality Impact Analysis (EIA) has been undertaken. As a result of the analysis, the policy, project or function does not appear to have any

adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

NHS North Yorkshire CCG aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

8.0 Consultation

Consultation with the CCG Communications and Engagement Team has been undertaken in the development of this policy and reviewed by Information Governance Steering Group prior to approval by the Audit Committee.

9.0 Training

Data Security Standard 3 within the Caldicott 3 review requires that all staff undertake appropriate annual data security training and pass a mandatory test, this must be completed by new employees within one week of commencement of employment. Further specific training may be required in line with job roles delegated to staff.

10.0 Monitoring Compliance with the Document

The CCG will monitor compliance with the policy throughout the year via:

- Monitoring and investigating incidents resulting in a breach of confidentiality. Guidance will be sort from the NECS IG Team as appropriate
- Lessons learnt from incidents will be reflected in policies and procedures as required and communicated to staff via the CCG newsletter.

Audit Committee is responsible for monitoring compliance against policy. This is done via updates provided from the IGSG.

11.0 Arrangements for Review

This policy will be reviewed every three years and in accordance with the following on an as and when required basis:

- legislative changes;
- good practice guidance;
- case law;
- significant incidents reported;
- new vulnerabilities; and
- changes to organisational infrastructure.

12.0 Dissemination

This policy will be published on the CCG's internet and will therefore be available to both staff and the public.

Staff will be made aware of the existence of this policy and all subsequent updates via the staff newsletter.

13.0 Associated Documentation

- Information Security Policy.
- Email and Internet Policy.
- Acceptable Use Policy.
- Data Protection and Confidentiality Policy
- Confidentiality: Code of Conduct

14.0 References

This policy was developed in line with the following practices and legislation:

- Data Protection Act 2018;
- Human Rights Act 1998;
- General Data Protection Regulation 2016
- Health and Social Care Act 2012 and HSC (Safety and Quality) Act 2015.
- The Computer Misuse Act 1990;
- The common law duty of confidentiality;
- National Data Guardian Standards;
- Caldicott principles;
- Information Commissioners Data Sharing Code of Practice