

|                  |   |
|------------------|---|
| <b>Corporate</b> | <b>CCG CO23 Social Media and Instant Messaging Policy</b> |
|------------------|---|

| <b>Version Number</b> | <b>Date Issued</b> | <b>Review Date</b> |
|-----------------------|--------------------|--------------------|
| V1.1                  | September 2020     | September 2022     |

|                              |   |
|------------------------------|---|
| <b>Prepared By:</b>          | Senior Governance Officer (IG),<br>North of England Commissioning Support |
| <b>Consultation Process:</b> | Head of Corporate Services, CCG   |
| <b>Formally Approved:</b>    | 8 <sup>th</sup> September 2020  |
| <b>Approved By:</b>          | Executive Committee   |
| <b>Policy Adopted From:</b>  | CO23: Social Media and Instant Messaging Policy (1)                       |

## Equality Impact Assessment

| <b>Date</b> | <b>Issues</b> |
|-------------|---------------|
| August 2022 | See Section 9 |

## POLICY VALIDITY STATEMENT

Policy users should ensure that they are consulting the currently valid version of the documentation. The policy will remain valid, including during its period of review. However, the policy must be reviewed at least once in every 3 year period.

## Version Control

| Version | Release Date | Author  | Update comments  |
|---------|--------------|---|--|
| V1      | April 2020   | Senior Governance Officer (IG),<br>North of England Commissioning Support | New policy template.   |
| V1.1    | August 2020  | Senior Governance Manager, NECS   | Policy Extension. No legislation updates or external environment impacts identified. |

## Approval

| Role           | Name                      | Date           |
|----------------|---------------------------|----------------|
| Approval (1)   | Combined Management Group | 10 March 2020  |
| Approval (1.1) | Executive Committee       | September 2020 |

# Contents

|   |    |
|---|----|
| 1. Introduction .....   | 4  |
| 2. Definitions .....  | 5  |
| 3. Policy for social media and the use of instant messaging applications..... | 6  |
| 4. Implementation .....   | 10 |
| 5. Training implications .....  | 10 |
| 6. Documentation.....   | 10 |
| 7. Monitoring, review and archiving .....                                     | 11 |
| 8. Equality Analysis.....   | 12 |
| Appendix A: Duties and Responsibilities .....                                 | 15 |

# 1. Introduction

Social media and instant messaging software is changing the way we, and every organisation in the world conducts its business. Millions of people use social media and instant messaging applications every day and it has become an important communications tool.

For the purposes of this policy, NHS County Durham 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 relevant and appropriate documentation, processes and systems 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, social networks and using instant messenger applications.

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

## 1.1 Status

This policy is a corporate policy.

## 1.2 Purpose and aims

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 document will also highlight the considerations required in respect of information governance (IG) issues when using instant messaging and will seek to remind staff that the law places obligations on organisations to protect patient confidentiality safeguarding data.. 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 or share via instant messaging applications, whether acting independently or in their capacity as a representative of the CCG.

The aims of this document are:

- 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.

## 1.2 Scope

This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. 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.

## 2. Definitions

**'Social', 'social media' or 'social networking'** are the terms commonly used to describe websites 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

“Instant Messaging” or IMs, are any form of real-time text based communications sent from one person in a network (public or private) to any one or more people who share that network’, or applications for example but not limited to Whatsapp, Viber, Instagram

### **3. Policy for social media and the use of instant messaging applications**

#### **3.1 Responsibilities**

It is the responsibility of everyone within the organisation to use social media and instant messaging applications 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, confidential or flippant. Staff must also be aware of the potential legal implications of material which could be considered abusive, libellous or defamatory.

Staff should only consider the use of an instant messaging application if the organisation does not provide a suitable alternative. If staff choose to use instant messaging applications they 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).

Staff must at all times comply with Data Protection Legislation and Privacy and Electronic Communications Regulations with regards to their use of social media and instant messaging applications. The main points to consider are:

- The transfer of sensitive data across unregulated servers outside the European Economic Area (EEA)
- Compliance with data protection requirements regarding ‘fair processing’, individuals’ rights, and records management
- Data protection security risks, including bringing your own device (BYOD) to work.

#### **3.2 Social media and instant messaging in your personal life**

The CCG recognises that many employees make use of social media and IM applications 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 or IM applications 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 or personal 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 patients without their explicit 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 or IM applications to bully another individual or post images that are discriminatory or offensive (or links to such content)
- Post or share information that breaches any of the conditions in CCG or NHS policies.

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

### **3.3 Line manager guidance for social media access**

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.

### 3.4 Considerations for staff when using IM applications

The use of an instant messaging application should only be considered if the organisation does not provide a suitable alternative.

Staff and managers should consider the security features of instant messaging applications to ensure that the message stays private. If the message contains a patient's identity or information that could potentially be used to identify a patient or colleague then particular attention to, **Encryption, End-user verification, Passcode protection, Remote-wipe and Message retention** needs to be addressed

Staff should remember that instant messaging conversations may be subject to freedom of information requests or subject access requests and as such should not upload unless justifiable 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 explicit permission
- Defamatory statements about the CCG, its staff, services or contractors
- Confidential information on bulletin boards, forums or newsgroups

#### **Devices used to access IM applications:**

- should not be accessible to others
- should to require a passcode immediately, and for it to lock out after a short period of not being used
- should have message notifications disabled on the device's lock-screen
- should have the remote-wipe feature enabled in case the device is lost or stolen

#### **Staff communicating on IM applications:**

- Should ensure that communications are being shared with the correct person or group
- 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
- Unlink the app from your photo library

### **3.5 Guidance for staff given access to social media on behalf of the CCG**

Where access has been given to use 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 explicit permission
- Defamatory statements about the CCG, its staff, services or contractors
- Confidential information on bulletin boards, forums or newsgroups
- Raising Concerns at Work, 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 raise any concerns. The Raising Concerns at Work Policy incorporates the requirements of the Public Interest Disclosure Act 1998 (PIDA) and the Bribery Act 2010.

### **3.6 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, IM applications and embedded on other people's websites.

Images of individuals in photos/videos are treated as personal information where the person's identity is clear and can reasonably be worked out. In this instance, informed and explicit 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 (available on request from the CCG).

## **4. Implementation**

This policy will be available to all staff for use in relation to the use of social media and IM applications.

All managers are responsible for ensuring that relevant staff within the CCG have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

## **5. Training implications**

It has been determined that there are no specific training requirements associated with this policy/procedure.

## **6. Documentation**

### **6.1 Other related policy documents**

- Confidentiality and data protection policy
- Information governance and risk policy
- Information security policy
- Safeguarding children policy
- Safeguarding vulnerable adults policy
- Standards of business conduct and declarations of interest policy
- Equality and diversity policy
- Harassment and bullying policy
- Raising Concerns at Work policy

### **6.2 Legislation and statutory requirements**

- Equality Act 2010
- Data Protection Act 2018
- Freedom of Information Act 1998
- General Data Protection Regulations 2016
- Human Rights Act 1998
- Employment Rights Act 1996
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Bribery Act 2010
- Privacy and Electronic Communications Regulations 2003

## 6.3 Best practice recommendations

- Royles, D, NHS Employers, *Driving a permissive use of social media - #NHSEngage*, <http://www.nhsemployers.org/Aboutus/news-dean/commentry/Pages/DrivingAPermissiveUseOfSocialMediaNHSEngage.aspx>, Accessed 29/07/2013
- Talbott, A, NHS Employers, *HR and Social Media in the NHS*, <http://www.nhsemployers.org/Aboutus/Publications/Documents/HR-social-media-NHS.pdf>, Accessed 29/07/2013
- White, C, NHS Networks, *Using social media to engage, listen and learn*, <http://www.networks.nhs.uk/nhs-networks/smart-guides/documents/Using%20social%20media%20to%20engage-%20listen%20and%20learn.pdf>, Accessed 29/07/2013
- Information Governance Alliance, ***The Records Management Code of Practice for Health and Social Care 2016***  
<https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care>, Accessed 9 May 2017
- <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> Accessed 24/02/2020

## 7. Monitoring, review and archiving

### 7.1 Monitoring

The Chief Officer will oversee, on behalf of the Governing Body, a method for monitoring the dissemination and implementation of this policy.

Monitoring information will be recorded in the policy database.

### 7.2 Review

The Governing Body will ensure that this policy document is reviewed in accordance with the timescale specified at the time of approval. No policy or procedure will remain operational for a period exceeding three years without a review taking place.

Staff who become aware of any change which may affect a policy should advise their line manager as soon as possible. The governing body will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

For ease of reference for reviewers or approval bodies, changes should be noted in the 'document history' table on the front page of this document.

**NB:** If the review consists of a change to an appendix or procedure document, approval may be given by the sponsor director and a revised document may be issued. Review to the main body of the policy must always follow the original approval process.

## 7.4 Archiving

The Governing Body will ensure that archived copies of superseded policy documents are retained in accordance with The Records Management Code of Practice for Health and Social Care 2016.

## 8. Equality Analysis

### Step 1

As a public body organisation we need to ensure that all our strategies, policies, services and functions, both current and proposed have given proper consideration to equality and diversity, do not aid barriers to access or generate discrimination against any protected groups under the Equality Act 2010 (Age, Disability, Gender Reassignment, Pregnancy and Maternity, Race, Religion/Belief, Sex, Sexual Orientation, Marriage and Civil Partnership, Carers and Health Inequalities).

A screening process can help judge relevance and provides a record of both the process and decisions made.

This screening determines relevance for all new and revised strategies, policies, projects, service reviews and functions.

Completed at the earliest opportunity it will help to determine:

- The relevance of proposals and decisions to equality, diversity, cohesion and integration.
- Whether or not equality and diversity is being/has already been considered for due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED).
- Whether or not it is necessary to carry out a full Equality Impact Assessment.

#### Name(s) and role(s) of person completing this assessment:

Name: Beverley Smith  
Role: Senior Governance Officer

#### Title of the service/project or policy:

Social Media and Instant Messaging Policy

Is this a:

Strategy / Policy

Service Review

Project

If other, please specify:

## What are the aim(s) and objectives of the service, project or policy:

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 document provides the awareness required by staff should they chose to use instant messenger applications when a secure method of messaging isn't made available by the organisation and the associated risks. This is a rapidly changing area and this policy is expected to be updated and amended as communication strategies evolve. This policy aims 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.

## Who will the project/service /policy / decision impact?

Consider the actual and potential impacts:

- Staff
- service users/patients
- other public sector organisations
- voluntary / community groups / trade unions
- others, please specify:

| Questions   | Yes | No |
|---|-----|----|
| Could there be an existing or potential impact on any of the protected characteristic groups?   |     | X  |
| Has there been or likely to be any staff/patient/public concerns?   |     | X  |
| Could this piece of work affect how our services, commissioning or procurement activities are organised, provided, located and by whom?   |     | X  |
| Could this piece of work affect the workforce or employment practices?  |     | X  |
| Does the piece of work involve or have an impact on: <ul style="list-style-type: none"> <li>Eliminating unlawful discrimination, victimisation and harassment</li> <li>Advancing equality of opportunity</li> <li>Fostering good relations</li> </ul> |     | X  |

If you have answered no to the above and conclude that there will not be a detrimental impact on any equality group caused by the proposed policy/project/service change, please state how you have reached that conclusion below:

The policy is based on the former NHS County Durham CCG Social Media & Instant Messaging Policy and published Information governance considerations for staff on the use of **instant messaging software** in acute clinical settings from the NHS. There is new information included in the document however the conclusion of 'no impact' is appropriate.

If you have answered yes to any of the above, please now complete the 'STEP 2 Equality Impact Assessment' document.

## Governance, ownership and approval

| Please state here who has approved the actions and outcomes of the screening |                           |             |
|--|---------------------------|-------------|
| Name   | Job title                 | Date        |
| Beverley Smith   | Senior Governance Officer | August 2020 |

### Publishing

This screening document will act as evidence that due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED) has been given.

**If you are not completing 'STEP 2 - Equality Impact Assessment' this screening document will need to be approved and published alongside your documentation.**

A copy of all screening documentation should be sent to: **NECSU.Equality@nhs.net** for audit purposes.

## Duties and Responsibilities

|                                 |   |
|---------------------------------|---|
| <b>Council of Members (COM)</b> | The council of members has delegated responsibility to the Governing Body (GB) for setting the strategic context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents.   |
| <b>Chief Officer</b>            | The Chief Officer has overall responsibility for the strategic direction and operational management, including ensuring that CCG process documents comply with all legal, statutory and good practice guidance requirements.  |
| <b>Chief Finance Officer</b>    | <p>The Chief Finance Officer as CCG Governance Lead will ensure that use of social media will:</p> <p>comply with corporate branding be used in a manner to enhance the CCG’s ability to engage with stakeholders</p> <p>comply with statutory and regulatory rules as well as national guidance and best practice</p> <p>They are also responsible for:</p> <ul style="list-style-type: none"> <li>• generating and formulating this policy</li> <li>• identifying the appropriate process for regular evaluation of the implementation and effectiveness of this policy</li> <li>• identifying the competencies required to implement this policy, and either identifying a training resource or approaching Workforce Learning and Development (Governance Directorate, Commissioning Support Unit) for assistance</li> </ul>  |
| <b>All line managers</b>        | All line managers are responsible for ensuring that appropriate processes are complied with when using social media.  |
| <b>All Staff</b>                | <p>All staff, including temporary and agency staff, are responsible for:</p> <ul style="list-style-type: none"> <li>• Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken.</li> <li>• Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities.</li> <li>• Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly.</li> <li>• Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager.</li> <li>• Attending training / awareness sessions when provided.</li> </ul> |

|   |  |
|---|--|
| <b>Commissioning Support Unit (CSU) Staff</b> | Whilst working on behalf of the CCG, CSU staff will be expected to comply with all policies, procedures and expected standards of behaviour within the CCG, however they will continue to be governed by all policies and procedures of their employing organisation.  |
| <b>Information Asset Owners</b>               | <p>Information Asset Owners (IAOs) are responsible for:</p> <ul style="list-style-type: none"> <li>• Liaising with records management/IG leads to ensure that records management practices are in line with the guidance and protocols on confidentiality.</li> <li>• Ensuring appropriate record audits are undertaken.</li> <li>• Ensuring appropriate information governance /confidentiality clauses are in third party contracts relating to records management such as secondary storage, scanning companies before using the company.</li> <li>• Ensuring appropriate consideration is given to records management within business continuity plans.</li> <li>• Ensuring they obtain appropriate certifications of destruction.</li> </ul> <p>Investigate and take relevant action on any potential breaches of this policy supported by other applicable staff in line with existing procedures.</p> |