NHS
North East &
North Cumbria

Corporate	ICBP038 Social Media & Instant Messaging Policy

Version Number	Date Issued	Review Date
2	October 2022	October 2024

Prepared By:	Senior Communications Manager, North of England Commissioning Support (NECS)
Consultation Process:	This policy has been developed in conjunction between the ICB and NECS
Formally Approved:	October 2024
Approved By:	Executive Committee

EQUALITY IMPACT ASSESSMENT

Date	Issues
June 2022	None identified.

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.

ACCESSIBLE INFORMATION STANDARDS

If you require this document in an alternative format, such as easy read, large text, braille or an alternative language please contact necsu.comms@nhs.net

Version Control

Version	Release Date	Author	Update comments
1	July 2022	Senior Communications Manager, NECS	New policy.
2	October 2022	Senior Communications Manager, NECS	Reviewed within first 6 months of ICB establishment

Approval

Role	Name	Date
Approver	Executive Committee	July 2022
Approver	Executive Committee	October 2022

Contents

1. Introduction

Social media is used by millions of people around the world and can have a significant impact on organisational, professional and individual reputations.

NENC ICB acknowledges the right of all staff to freedom of expression and recognises 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 ICB.

Staff who post comments or information online regarding the ICB, or the NHS and its partner organisations, are personally responsible for their actions and the online content they have created or actively shared.

Content posted, shared or created online or via a social media platform is hard to remove and should always be considered as if it were permanent. Even with strict privacy controls, it is difficult to prevent or control how it is used by third parties once posted. This means that the utmost discretion must be used when posting material.

Staff should follow the same behavioural 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.

1.2 Status

This policy is a Corporate Policy.

1.3 Purpose and scope

This policy aims to provide guidance for ICB staff, directors, volunteers, contractors and agency staff on the appropriate use of social media at all times. It also services to ensure that the privacy, confidentiality, and interests of the ICB, its employees, partners and patients, are upheld and protected.

It outlines the appropriate use of social media by ICB employees, directors, volunteers, contractors and agency staff both in a personal and professional capacity and sets out the responsibility of individuals when using social media in order to maximise benefits and minimise risks.

This document outlines the standards we require staff to observe when using social media, the circumstances in which we will monitor the use of social media and the action we will take in respect of breaches of this policy.

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 ICB 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 ICB information from the personal opinion of staff.

This policy applies to those members of staff that are directly employed by the ICB and for whom the ICB 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 ICB.

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):

- Social networking sites (Facebook, LinkedIn, Google+ Nextdoor)
- Blogs and micro-blogs, (Twitter, WordPress)
- Content sharing websites, (Flickr, YouTube, Instagram, TikTok, Prezi.com, Pinterest)
- 'Wikis' (Wikipedia, LinkedIn) - websites which allow users to add, modify or delete content
- Audio and video podcasts
- Message platforms/ applications (WhatsApp, Messenger, SnapChat, Signal, WeChat etc)
- Message or discussion boards/forums
- Dating websites

"**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, messenger.

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 ICB, 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 ICB 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 ICB employee.

Although it is acceptable for staff to say they work for the NHS or the ICB 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 ICB” or “Tweets are my own views”.

All employees should be aware that the ICB 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 ICB 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 UK General Data Protection Regulations.
- Include contact details or photographs of colleagues, customers or patients without their explicit permission.
- Discuss the ICB'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 ICB or NHS policies.

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

3.2.1 General rules for use of social media

Whenever you use social media you must adhere to the following general rules whether you are posting, commenting, reacting (i.e. liking) or sharing:

Always write in the first person, identify who you are and – if commenting on NHS/ healthcare matters - what your role is, and use the following disclaimer "The views expressed are my own and don't necessarily reflect the views of my employer". Always act in a transparent manner when altering online sources of information, such as websites like Wikipedia or LinkedIn.

Do not upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing derogatory or defamatory content.

Do not upload, post or forward any content belonging to a third party unless you have that third party's consent.

If you do post, upload or forward content from a third party it is your responsibility to make certain that they are an acceptable/ appropriate source of information.

Every member of staff carries individual responsibility as an NHS employee and to act in line with professional codes of conduct when using social media.

On joining an NHS or ICB related network or group on social networking sites or when making reference to the ICB as your employer you should identify yourself by displaying necsu.nenc-icb.contactus@nhs.net

Staff should not display work email addresses unless in a professionally related capacity.

It is acceptable to quote a small excerpt from an article, particularly for the purposes of commenting on it or criticising it. However, if you think an excerpt is too big, it probably is. Quote accurately, include references and when in doubt, link, don't copy.

Before you include a link to a third party website, check that any terms and conditions of that website permit you to link to it. All links must be done so that it is clear to the user that they have moved to the third party's website.

When making use of any social media platform, you must read and comply with its terms of use.

Do not post, upload, forward or post a link to chain mail, junk mail, cartoons, jokes or gossip.

Be honest and open but be mindful of the impact your contribution might make to people’s perceptions of us as an ICB. If you make a mistake in a contribution, be prompt in admitting and correcting it.

You are personally responsible for the content you publish into social media tools – be aware that what you publish will be public for many years.

Don't escalate heated discussions, try to be conciliatory, respectful and quote facts to lower the temperature and correct misrepresentations. Never contribute to a discussion if you are angry or upset, return to it later when you can contribute in a calm and rational manner.

If you feel even slightly uneasy about something you are about to publish, then you shouldn’t do it. If in doubt, ask.

Don’t discuss colleagues without their prior approval.

Always consider others’ privacy and avoid discussing topics that may be inflammatory.

Avoid publishing your contact details where they can be accessed and used widely by people you did not intend to see them, and never publish anyone else's contact details without their express consent.

Before your first contribution on any social media site, observe the activity on the site for a while before launching in yourself to get a feel for the style of contributions, the nature of the content and any 'unwritten' rules that other contributors might follow.

Activity on social media websites during office hours should complement and/or support your role and should be used in moderation.
If you notice any content posted on social media about us (whether complimentary or critical) please report it to the communications team. If it is out of hours please go to https://www.necsu.nhs.uk/contact/ for details of the Media On Call contact.

If a staff member is contacted by the media about posts they have made on a social networking site, whether or not those posts relate to the ICB or the NHS, they should inform the communications team immediately.

3.2.2 Personal use of social media during working hours

Personal use of social media is not permitted during working hours and the use of social media on ICB 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 ICB's networks.

If there is a specific business need to access such services, approval should be sought from the communications team. Authority will only be given where a clear business need is identified.

Staff using ICB IT equipment or their own personal smartphone devices to access social media during working hours should restrict this to designated break times only i.e. during a lunch or comfort break, or outside of normal working hours.

3.2.3 Commenting in online discussions / forums

Many members of ICB staff may already be actively involved with social media and comment in online discussion forums to share ideas about various areas of work. This positive professional involvement is encouraged by the ICB but employees should always be mindful of the points outlined in this policy.

3.2.4 Monitoring use of social media websites

Staff should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored and, where breaches of this policy are found, action may be taken.

Monitoring is only carried out to the extent permitted or as required by law and as necessary/ justifiable. Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you and us.

In particular uploading, posting forwarding or posting a link to any of the following types of material on a social media website, whether in a professional or personal capacity, will amount to gross misconduct (this list is not exhaustive):

Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

A false and defamatory statement about any person or organisation;
Material which is offensive, obscene, criminal discriminatory, derogatory or may cause embarrassment to us, our clients or our staff;

Confidential information about the ICB or any ICB staff, (which you do not have express authority to disseminate);

Any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or

Material in breach of copyright or other intellectual property rights, or which invades the privacy of any person.

3.2.5 Organisational use of social media

The ICB is already actively using sites like Facebook, Twitter and YouTube as part of a wider marketing and communications strategy. This is not only to update members of the public, patients, staff, stakeholders and the media about services but, most importantly, to engage with online audiences and get feedback on services and experiences which is feedback to teams and formally to the organisation.

This activity is coordinated and managed by the ICB's communication team.

Any departments wishing to use social media to promote their work should liaise with the communications team and should consider what they want to achieve - objectives, messages, audiences and goals and most importantly how activity can be measured.

Installation of social media applications on ICB devices will require approval by the Information Governance team. Access will only be provided to the application where use is for legitimate purposes and will align to this policy. Requests for such applications should be logged through the IT service desk.

3.2.6 Editing websites

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

If you edit the entry yourself from work, the source of the correction may be recorded as an NHS internet 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 ICB – including but not limited to derogatory and offensive comments - should never be removed but instead reported to the communications team who will agree on an appropriate response.

3.2.7 Professional and personal blogging

Any staff who have professional or personal blogs or websites in relation to health and social care should inform the communications team and must ensure that any activity is in line with this social media policy.

In these cases, if a blog makes it clear that the author works for the ICB and/or the NHS, it should include a clear disclaimer such as “these are my personal views and not those of NENC ICB”. The ICB logo should never be used on personal web pages.

Personal blogs and websites should not reveal confidential information about staff or the ICB. This might include aspects of ICB policy, plans, or details of internal discussions. If in doubt about what might be confidential, consult the communications team.

If a staff member thinks something on their blog or website gives rise to a conflict of interest or, in particular, concerns about impartiality or confidentiality, this must be discussed with the communications team.

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 with your line manager and the communications team.

3.2.8 Whistleblowing

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” normally involves raising the issue internally first. Using social media to whistleblow would not be considered appropriate and all staff should raise concerns through the proper internal channels as outlined in the ICB's Whistleblowing Policy.

Any member of staff who feels that they have been harassed or bullied, or are offended by material posted or uploaded by a colleague onto a social media website should inform their line manager

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 ICB.

3.4 Considerations for staff when using IM applications

Messaging tools such as WhatsApp or (Facebook) Messenger are considered to be social media platforms in their own right. As such, their use falls within the terms of this policy.

It is recognised, by the ICB and the wider NHS, that these services – most notably WhatsApp – are often useful by staff in performance of their duties. For instance, a team message group can be used to rapidly disseminate information. However, they also pose a significant risk if used improperly or without appropriate planning and governance. Any such use of messaging apps requires approval by Information Governance before they are available to download. Access will only be granted when the proposed use outlined would be compatible with this policy.

The following factors should be considered both before and while using a messaging platform or app in a work capacity. Please note, this is in addition to other guidance within this policy all of which also applies.

- 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 ICB employee in relation to their employment including judgements of their performance and character
- Photographs or video of another ICB employee taken in the work situation without explicit permission
- Defamatory statements about the ICB, its staff, services or contractors
- Confidential information on bulletin boards, forums or newsgroups

Staff should be aware that 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

Always remember: If you use your personal device for these purposes then losing it may have professional as well as personal ramifications. As a result, it is strongly recommended that only work devices be used.

3.5 Guidance for staff given access to social media on behalf of the ICB

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 ICB employee in relation to their employment including judgements of their performance and character
- Photographs or video of another ICB employee taken in the work situation without explicit permission
- Defamatory statements about the ICB, 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 ICB content 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 ICB).

4. Implementation

4.1 This policy will be available to all staff for use in relation to the specific function of the policy.

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

5. Training Implications

5.1 The Executive Director will ensure that the necessary training or education needs and methods required to implement the policy are identified and resourced or built into the delivery planning process. This may include identification of external training providers or development of an internal training process.

5.2 It has been determined that there are no specific training requirements associated with this policy/procedure however all staff are expected to undertake annual Data Security Awareness training.

6. Documentation

6.1 Other related policy documents:

- Confidentiality and data protection policy
- Information governance and information 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
- Information Labelling & Classification Procedure

6.2 Legislation and statutory requirements:

- Obscene Publications Act 1959 & 1964
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Employments Rights Act 1998
- Crime & Disorder Act 1998
- Employment Rights Act 1998
- Public Interest Disclosure Act 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Privacy and Electronic Communications Regulations 2003
- Bribery Act 2010
- Equality Act 2010
- Data Protection Act 2018

6.3 Best practice recommendations

- 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*** Records Management Code of Practice - NHSX Accessed 14 December 2021
- NHS Digital ***Social Media Guidance*** https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/nhs-digital-style-guidelines/how-we-talk/social-media#social-media-guidance Accessed 13/01/2020
- NHSX ***Use of Mobile Messaging Guidance in Health and Care settings*** https://www.nhsx.nhs.uk/information-governance/guidance/use-mobile-messaging-software-health-and-care-settings/ Accessed 19/05/2021

7. Monitoring, Review and Archiving

7.1 Monitoring

The Board will agree with the Executive Director a method for monitoring the dissemination and implementation of this policy. Monitoring information will be recorded in the policy database.

7.2 Review

7.2.1 The ICB Board 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.**

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

7.2.3 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 sponsoring director and a revised document may be issued. Review to the main body of the policy must always follow the original approval process.

7.3 Archiving

The ICB Board will ensure that archived copies of superseded policy documents are retained in accordance with the NHS Records Management Code of Practice 2021.

SCHEDULE OF DUTIES AND REPONSIBILITIES

Through day to day work, employees are in the best position to recognise any specific fraud risks within their own areas of responsibility. They also have a duty to ensure that those risks, however large or small, are identified and eliminated. Where it is believed fraud, bribery or corruption could occur, or has occurred, this should be reported to the CFS or the chief finance officer immediately.

ICB Board	The ICB Board has responsibility 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.
Chief Executive	The Chief Execuitve has overall responsibility for the strategic direction and operational management, including ensuring that ICB process documents comply with all legal, statutory and good practice guidance requirements
Executive Director of Corporate Governance, Communications and Engagement	The ICB Executive Director of Corporate Governance, Communications and Engagement will ensure that use of social media will: comply with corporate branding be used in a manner to enhance the ICB's ability to engage with stakeholders comply with statutory and regulatory rules as well as national guidance and best practice They are also responsible for: • ensuring the generation and formulation of this policy • identifying the appropriate process for regular evaluation of the implementation and effectiveness of this policy identifying the competencies required to implement this policy, and either identifying a training resource or approaching Workforce Learning and Development
All line managers	All line managers are responsible for ensuring that appropriate processes are complied with when using any form of social media or instant messenger application.

All Staff	All staff, including temporary and agency staff, are responsible for: • Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken. • Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities. • 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. • Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager. • Undertaking training / attending awareness sessions when provided.
Information Asset Owners	Information Asset Owners (IAOs) are responsible for: • Liaising with records management/IG leads to ensure that records management practices are in line with the guidance and protocols on confidentiality. • Ensuring appropriate record audits are undertaken. • 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. • Ensuring appropriate consideration is given to records management within business continuity plans. • Ensuring they obtain appropriate certifications of destruction. Investigate and take relevant action on any potential breaches of this policy supported by other applicable staff in line with existing procedures.
Commissioning Support Staff.	Whilst working on behalf of the ICB NECS staff will be expected to comply with all policies, procedures and expected standards of behaviour within the ICB, however they will continue to be governed by all policies and procedures of their employing organisation.

APPENDIX A

EQUALITY IMPACT ASSESSMENT
Initial Screening Assessment (STEP 1)

As a public body organisation we need to ensure that all our current and proposed strategies, policies, services and functions, have given proper consideration to equality, diversity and inclusion, 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).

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
Job Title: Senior Governance Officer
Organisation: North of England Commissioning Support Unit

Title of the service/project or policy: Social Media and Instant Messaging Policy

Is this a;
Strategy / Policy ☒ **Service Review** ☐ **Project** ☐
Other Click here to enter text.

What are the aim(s) and objectives of the service, project or policy:
This is Policy is designed to provide guidance to 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 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 ICB

Who will the project/service /policy / decision impact?
(Consider the actual and potential impact)

- **Staff** ☒
- **Service User / Patients** ☐
- **Other Public Sector Organisations** ☐
- **Voluntary / Community groups / Trade Unions** ☐
- **Others, please specify** Click here to enter text.

Questions	Yes	No
Could there be an existing or potential negative impact on any of the protected characteristic groups?	☐	☒
Has there been or likely to be any staff/patient/public concerns?	☐	☒
Could this piece of work affect how our services, commissioning or procurement activities are organised, provided, located and by whom?	☐	☒
Could this piece of work affect the workforce or employment practices?	☐	☒
Does the piece of work involve or have a negative impact on: • Eliminating unlawful discrimination, victimisation and harassment • Advancing quality of opportunity • Fostering good relations between protected and non-protected groups in either the workforce or community	☐	☒

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:

This policy is for use by all employees. It is a standard which applies to all staff and doesn't impact on equality.

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

Accessible Information Standard	Yes	No
Please acknowledge you have considered the requirements of the Accessible Information Standard when communicating with staff and patients. https://www.england.nhs.uk/wp-content/uploads/2017/10/accessible-info-standard-overview-2017-18.pdf	☒	☐

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**
Claire Riley	Executive Director of Corporate Governance, Communications and Involvement	June 2022

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.