NHS
Leeds
Clinical Commissioning Group

Internet and Social Media Policy

Version:	1.2
Ratified by:	Audit Committee
Date ratified:	16 September 2020
Name & Title of originator/author:	Shak Rafiq, Communications Manager, Karen Rowe, Information Governance Manager
Name of responsible committee/individual:	Information Governance Committee
Date issued:	September 2020
Review date:	September 2022
Target audience:	All Staff

Table of Contents

1. Introduction

The CCG recognises that the use of the Internet is an essential tool that assists the organisation in conducting its business. Additionally, the CCG recognises that as well as general internet use, there is an increasing use of social media throughout all sectors of society.

CCG staff may access social media and the internet using NHS Leeds CCG equipment for personal use outside of their work hours; the CCG acknowledges the benefits of a more flexible approach to Internet and Social media access. Nevertheless where staff do access the Internet and social media, they need to be aware of any implications and impact on themselves, the CCG and wider NHS where they choose to discuss or post information about work related matters.

While there are many benefits to using the internet and social media, there can be risks associated with its use. For instance, breaching copyright, downloading inappropriate material and posting inappropriate material, referencing individuals, even outside of working hours, could have adverse implications for both the organisation and the individual involved. This policy sets out the guidelines and parameters for employees when using the internet and social media for both work and personal use which will enable them to make effective use of technology for the benefit of the CCG and its organisational aims and avoid any adverse impact.

Specific legislation will affect how employees use internet and social media. The current key laws and how it can affect usage is set out in Section 11: Related Law.

.

2. Purpose

The Internet is a general term that covers access to numerous servers and computer systems worldwide. Such systems include the World Wide Web (www) and NHS N3 web sites (prefixed nww) as well as any other services that are or may become accessible using internet technology connected to the CCG's network.

The CCG currently uses the N3 (Health and Social Care Network – HSCN) infrastructure to access these systems and as such is bound by the HSCN Statement of Compliance.

This policy covers all equipment used to access internet and social media including computers, laptops, tablets, mobile phones and Bring Your Own Devices (BYODs).

.

Failure to adhere to this policy will be fully investigated in accordance with CCG's procedures and, if appropriate, may result in disciplinary, civil and/or criminal proceedings (including potential dismissal or termination of association with the CCG) and where necessary referral to the appropriate regulatory bodies including the police and professional bodies.

Employees must speak with their line managers in the first instance if they have any questions regarding this policy. If you are a CCG volunteer, you should speak to the member of staff you normally liaise with.

Any changes or reviews to this or any other policy will be notified to staff via established communications routes such as email, Workplace, team brief, staff bulletin, internet and the extranet.

3. Scope

All employees, including those on temporary or honorary contracts, secondments, volunteers, Board members, students and partners working for the CCG who are provided with authorised access to CCG equipment, systems or information must be made aware of, and adhere to, this policy. This policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

4. Definitions

4.1 Social Media

This is the term commonly used for web-based and other mobile communications technologies that enable messages and opinions to be shared in dialogue with others who often share the same community interests. The world of social media is constantly changing and it's not possible to provide an exhaustive list of all channels and types of social media. Generally social media refers to communication tools that allow you to self-publish information online, as well as consumer review sites such as TripAdvisor or Glassdoor.

4.2 Internet

The Internet is a large system of connected computers around the world that allows people to share information, visit websites and communicate with each other:

4.3 Blog

Is a type of website, maintained by an individual with regular entries by way of a commentary, it can be seen as an online diary, a regularly updated autobiography or an opinion piece. It can also mean to maintain or add content to a blog. Visitors can add comments or messages to the blogs if this function is enabled.

4.4 Multimedia
The use of computers to present text, graphics, video, animation and sound in an integrated way.

4.5 Streaming
Streaming or media streaming is a technique for transferring data so that it can be processed as a steady and continuous stream. For example this can include Spotify, Vimeo, DailyMotion or YouTube.

4.6 Twitter
Twitter is an online news and social networking site where people communicate in short messages called tweets. Some people use this as a way of rapidly gathering support for campaigns and activities through resharing of information (retweets) and making a subject popular for a short space of time (trending).

4.7 YouTube
YouTube is a video sharing service where users can create their own profile, upload videos, watch, like and comment on other videos.

4.8 Facebook
Facebook is a social networking website where users can post comments, share photographs and post links to news or other interesting content on the web, chat live, and watch short-form video.

4.9 Workplace
An internal messaging app developed by Facebook (but not linked to any personal accounts) for use in workplaces allowing staff to communicate, collaborate and connect using familiar features such as groups, chat and video calls.

5. Duties
There are a number of key information governance roles and bodies that the CCG needs to have in place as part of its Information Governance Framework. These are:

- Quality and Performance Committee
- Audit Committee
- Accountable Officer
- Data Protection Officer
- Qualified Cyber Professional
- Senior Information Risk Owner
- Caldicott Guardian
- Information Asset Owner
- Heads of Service / Managers
- All employees

The accountability and responsibilities of staff are set out in more detail in the **Information Governance Policy and Framework** which must be read in conjunction with this policy.

All employees are personally responsible for compliance with the law in relation to their use of internet and social media that involves the use of work derived information. More specific usage requirements in terms of internet and social media usage are outline in Sections 7 and 8 of the policy.

All managers are responsible for ensuring that the employees they manage are aware of this policy and of their individual responsibilities in respect of this policy.

All employees are responsible for reporting information and security incidents and near misses including breaches of this policy, using the CCG Incident Management system (DATIX). This includes any employee responsible for managing any volunteers.

6. Obtaining Access to the CCG Provided Internet

New users will be provided with access to a copy of this policy, which should be read as part of their induction.

New users will be provided with a username and password for access to the CCG network and extranet. This will include access to the internet.

Employees must not share their password with anyone.

7. Internet Usage

The primary purpose for CCG provided internet access is for business related matters. However, this policy describes how the Internet may be used reasonably for other purposes to a limited degree.

The reasonable use of the internet is very subjective and inevitably leads to differing interpretations of what is considered acceptable and reasonable. The guidelines outlined in this policy therefore are to provide a yardstick for what is deemed to be reasonable and acceptable from a performance management perspective

7.1 Blocking Sites

Specific sites will have been blocked for purposes relating to security, network performance and confidentially of CCG's information and to prevent access to sites that contain illegal content.

The list, nature and range of blocked sites is determined by the CCG's Senior Management Team, having consulted with staff and with advice from the Senior Information Risk Owner and the CCG's Information Governance Committee and our web filtering/monitoring service provider.

Blocked sites may include those that provide file transfers or storage. Any transfer or storage of personal and sensitive personal data must comply with CCG's policy requirements and legislation and be reviewed through the Data Protection Impact Assessment Procedure.

7.2 Personal Use

It is accepted that employees may wish to use the internet for personal use while accessing the CCG network or using their personal mobile devices and/or smartphones.

Any such use of the Internet does not contribute to an employees contracted hours.

This usage will be permissible for reasonable periods in the following times:

- In their lunch break
- Outside core working hours

The internet may be used at other times on an exception basis, subject to the consent of the individual's Line Manager. Any such use will be within the constraints described in the Policy. It must be noted that the overriding principle is that CCG provided internet usage is for business purposes and that personal usage involving CCG equipment must not have an adverse effect on the operation of CCG business e.g. taking up undue "bandwidth", or attempting to involve other members of staff who are currently working.

Where a staff member may exceptionally take up a long period of time browsing the internet for personal purposes while at work, they should inform their Line Manager and ensure that they have their Manager's explicit support. Continuous personal use of more than one hour would fall into this category and does not contribute to working time. This would include "tabbing" in and out of internet sites (including social media sites) for personal use over such a period.

7.3 Acceptable Use

- Internet access related to undertaking work duties such as:
  - Accessing key NHS systems
  - Accessing and sharing work related information with CCG staff and partner organisations
  - Educational, developmental or research purposes
  - Obtaining health service information
  - Professional and Personal Development and accreditation as per an agreed Personal Development Review with the users Line Manger
  - Accessing news sites to be kept informed about the latest NHS (and related) information
  - Using communications tools to perform CCG communications and engagement activities
- Accessing the internet for personal use on CCG owned equipment in line with conditions set out in Section 7.2, and excluding sites and usage set out in Section 7.4

- Streaming information for work related purposes
- Downloading and updating software with authorisation from IT services.

7.4 Unacceptable Use

- Accessing, creating, downloading or transmitting (other than for properly authorised and lawful research) any obscene or indecent images, data or other material.
- Creating, downloading or transmitting (other than for properly authorised and lawful research) any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material.
- Accessing, creating, downloading or transmitting material that is designed to annoy, harass, bully, inconvenience or cause needless anxiety to other people.
- Creating, downloading or transmitting data or material that is created for the purpose of corrupting or destroying other user's data or hardware.
- Creating or transmitting junk-mail or spam. This means unsolicited commercial webmail, chain letters or advertisements.
- Using the internet to conduct private or freelance business for the purpose of commercial gain.
- Downloading streaming video or audio for entertainment purposes.
- Creating, downloading or transmitting data or material that infringes or breaches copyright
- Accessing sites that involve:
    - Gambling
    - Auctioning/Buying/Selling
    - Dating
    - Playing online games
    - Radicalisation
    - Grooming
- Arranging independent access to the internet through a Virtual Private Network (VPN)
- Downloading or installing any unauthorised software on CCG equipment without prior authorisation from IT services
- The downloading and use of any unlicensed software (including computer games) and any downloading of data/programs for purposes not consistent with service use. This also applies to any software brought in from home.
- Deliberate activities with any of the following characteristics:
    - Wasting staff effort
    - Unduly using up network resources
    - Violating the privacy of other users
    - Disrupting the work of other users
- Using unauthorised file sharing sites to transfer or hold CCG personal or confidential information (see Section 7.1)

7.5 Monitoring of Internet Use

Staff need to be aware that Internet traffic on CCG provided Internet facilities is logged automatically, this includes each site a user visits, with the time visited and pages viewed. These logs may be audited and, where any inappropriate usage/patterns are identified, disciplinary action could be taken and referral to the relevant regulatory body as well as the potential for criminal investigation/prosecution (see Section 11: Related Law).

If you unintentionally access, download or transmit any information of images that are in breach of this policy then please report this to your Line Manager, the IT Service Desk and report it on Datix (Incident Management System). This is to ensure that it does not result in disciplinary procedure where the breach of policy was accidental / unintended.

Data Protection Statement

Information recorded as part of this automated monitoring process includes user identification, domain names of websites visited, duration of visits and non-business files downloaded from the internet. Staff should be aware that this monitoring may reveal sensitive data about them, for example, visits to websites which details the activities of a particular political party or religious group might indicate the political opinion or religious belief of that staff member, or self-help or health advice sites might identify a physical or mental health condition.

8. Social Media

8.1 Social Media for Work Purposes

The term Social Media encompasses a variety of internet platforms (this includes, but is not limited to, Twitter, Facebook, YouTube, Blogs, consumer review sites, comments sections on media sites and forums) which allow individuals and organisations to publish, and share information and comments online. It enables individuals to become part of different networks of people with similar or opposing interests for example political views and debates. For some platforms this is done so without the influence of an organisation, “state” or editor – in other words you can self publish directly without the need for someone to approve or moderate content.

The CCG recognises that social media is a platform which will allow it to interact with stakeholders in order to enhance its profile, provide information about the role and aims of the organisation, make professional and developmental contracts and to gauge and understand the views of stakeholders such as patients.

There are risks, however, associated with the use social media. Where staff use social media sites for work purposes (or in personal use where that may have an impact on the CCG) they must do so in compliance with related law

e.g. ensure CCG held personal and confidential information is secure, that copyright is not infringed and defamation of character does not occur. This also applies to any individual working on behalf of the CCG such as volunteers.

Furthermore we have a duty to protect the most vulnerable people in our communities; this policy reflects specific advice around safeguarding of adults and children.

When participating in social media networks for work purposes:

- Staff must be clear that they are representing the CCG as should any volunteers when carrying out any duties on behalf of the organisation
- Staff can provide their name and role at the CCG, but should not provide personal details about themselves such as date of birth, home address etc.
- Staff should only cover areas in which they are expert or where they can signpost to trusted information sites such as the NHS website www.nhs.uk
- When intending to publish official CCG content staff need to ensure that there is authorisation to do so (the same as when information is posted on the CCG website)
- When commenting or posting any content, staff need to adhere to all policies relating to expected conduct and behaviour for an NHS employee or contractor

Where considering participating in or setting up a CCG social media presence:

- Staff must discuss the proposal with their Line Manager and the Communications and Engagement Team in the first instance, to ensure that it is appropriate and in line with the organisation's communication and engagement strategy
- Staff need to have an idea of what they are trying to achieve and how to link this activity to the overall business plan for a programme or business area. This may involve putting forward a Project Initiation Document
- Staff must ensure that they have the explicit approval of the CCG via Line Managers or the Communications and Engagement Team to represent the CCG on the matter. This should include a nominated person who will maintain the account and respond to queries as well as an understanding of what to do if an incident involving any social media content could affect the reputation of the CCG

and/or wider NHS, could affect patient safety or patient confidence in NHS-funded services.
You will be expected to complete a form, Appendix B, provided by the Communications and Engagement Team that provides this information as well as a single page summary reminding you of your responsibilities when running a team/project social media account(s).

8.2 Personal Use of Social Media

The CCG recognises that staff may wish to participate in social media sites out of work time for personal use. However, when someone clearly identifies their association with the CCG and discusses their work or work-related matters, they are expected to behave appropriately, and in ways that are consistent with the CCG's values and policies.

The same conditions for confidentiality and security of information (where it relates to CCG information) will apply for personal use as it does when using the information in a work setting. If an employee makes reference, in a personal capacity, to the CCG or the wider NHS then this must be clearly distinguishable from their professional capacity. This also includes any political debates or political affiliations you may have. Your biography should make it clear that any views you express are your own and not that of the organisation.

The NHS is always high on the political agenda, and whilst we acknowledge that references to political parties and their policies may often be inevitable, any political debate should be avoided.

Any electronic communication which is considered to breach professional conduct may result in the matter being referred under the CCG disciplinary procedure.

When accessing social media for personal use where comments or information relate to the CCG work, the following apply:

- Staff must remember that these sites are a public forum and form part of a network. At no time should staff assume that any entries will remain private.
- Staff are reminded that they are personally responsible for the content published and that these items may remain on these sites for a very long time. They may also be the subject of future media interest and could affect future employment prospects as they could be viewed by future employers. It is worth noting that content on some social media sites can be easily found through using an internet search engine (eg Google), please check the privacy settings of all sites and change them to best suit your needs.

- Staff should not post defamatory, derogatory or offensive comments on the internet about colleagues, patients, their work or the CCG.
- Staff must not reveal any confidential or personal information about patients, or staff.
- Where photos of other staff are taken informally at work or outside of the work environment such as social occasions and a staff member is then intending to share on social media, it should be done with consideration taking into account the perceptions of those other staff as to the level of circulation of those photos. Consent must be sought and given prior to capturing any images of employees – any potential sharing or wider use will need to be identified as part of this process. Any content pertaining to another member of staff should be removed if requested to do so.
- Likewise, photographs of staff taken with their consent and for work purposes should only be used for the specific purpose and situation (e.g. for a staff publication), should not be published outside of that agreed area. The artist/publisher should be clearly acknowledged. It is noted, however, that where a document (such as a staff publication) has been published in the public domain already it would be possible to link to the publication – this does not allow for the content to be reused for different purposes.
- Staff should not impersonate another colleague or any other individual or organisation on social networking sites/forums.

9. Safeguarding

9.1 Safeguarding Others

During the course of your work for the CCG you may have cause to engage in online conversations with, and the promotion of, engagement opportunities with children, young people and adults at risk. The use of social media/networking sites introduces a range of potential safeguarding risks to these groups.

Most children, young people and adults use the internet positively, but sometimes they and others may behave in ways that pose a risk. Potential risks can include, but are not limited to:

- Online bullying
- Grooming, exploitation or stalking
- Exposure to inappropriate material or hateful language
- The vulnerable person giving away personal details, which can be used to locate them, harass them or steal their identity

- Coercion into illegal activity, such as distributing illegal content or hate crime
- Indoctrination into ideations and encouraged into terrorist activities
- Encouraging violent behaviour, self-harm or risk taking
- People's wellbeing not being promoted, as their views, wishes, feelings and beliefs are not taken into account.

In order to mitigate these risks there are steps you can take to promote safety online:

- Don't target/or engage with children who are likely to be under the minimum requirement age for the social networking service that you are promoting. This is usually 13 years, but can vary by platform so check the terms and conditions of each platform.
- Don't accept 'friend' or connection requests from anyone you suspect to be underage and/or someone you are, or have been working with in a professional capacity. If you feel it is appropriate to do so, you can choose to block any individual or organisation from connecting with you.
- Avoid collecting, and don't ask users to divulge any personal details, including: home and email addresses, school information, home or mobile numbers.
- You should not use any information in an attempt to locate and or meet a child, young person or vulnerable adult that is not directly to do with work.
- The Sexual Offences Act (2003) combat increasing sexual approaches to access children and young people on-line. The Act 2003 created an offence of meeting a child following sexual grooming. This makes it a crime to befriend a child on the Internet or by other social media means and to arrange to meet or intend to meet the child or young person with the intention of abusing them.
- Be careful how you use images of children, young people or adults - photographs and videos can be used to identify them to people who wish to groom them for abuse.
    - consider using models, stock photography or illustrations
    - if a child, young person or adult at risk is named, do not use their image
    - if an image is used, do not name the child, young person or adult at risk
    - where necessary obtain parents'/carers/guardians or Lasting Power of Attorney’s written consent to film, or use photographs on web sites

- Ensure that any messages, photos, videos or information comply with existing policies and that you have completed a photo consent form. Please speak to the communications and engagement team for further advice and to access the consent form.
- Promote safe and responsible use of social media/networking to your audience online and consider providing links to safety and support organisations on your profile. Remind people to protect their privacy.
- Data Protection considerations - when you are collecting personal information about all users, you should always follow the requirements set out in the Data Protection Act 1998. You should not use social media to collect personal data and this should be done via alternative means, e.g. by signposting to a form on your website.

9.2 Safeguarding Yourself

If you are using corporate or personal social media/networking accounts for work related activity, you should also:

- Ensure that your privacy settings are set up so that personal information you many not want to share is not available to members of the public.
- Have a neutral picture of yourself as your profile image.
- Do not use your work contact details (email or telephone) as part of your personal profile or personal contact details as part of a profile you use for work.
- Keep yourself safe; if you are not sure then do not proceed without advice and support.
- Do not engage in intimate or sexual conversations.
- Ensure any personal pictures you upload are not intimate, compromising or sexually explicit.
- Should any employee encounter a situation whilst using social media that threatens to become antagonistic they should politely disengage and seek advice from the Communications and Engagement Team and/or their line manager.

With regard to personal safeguarding, you should report any harassment or abuse you receive online whilst using corporate or personal accounts for NHS Leeds CCG related business, to the Communications and Engagement Team in the first instance. They will advise you what further action should be taken. Keep yourself and others safe. Do not place yourself at risk and engage in risk taking behaviour on social media platforms. If you feel you have been the victim of malicious or criminal activity you should report this to the police as well as alerting the social media site(s) where this activity has taken place.

9.3 Reporting Safeguarding Concerns

Any content or online activity which raises a safeguarding concern must be discussed with the CCG safeguarding team on 0113 843 1713 and your line manager in the first instance.

Where a child, young person or adult is identified to be in immediate danger, dial 999 for police assistance.

Any online concerns should be reported as soon identified as law enforcement and child/adult safeguarding agencies may need to take urgent steps to support the person.

Contact numbers for Children's Social Work Services and Adult Social Care can be found on the Safeguarding page of the NHS Leeds CCG extranet https://extranet.leedsccg.nhs.uk/corporate-information/safeguarding/

As a minimum you should ensure you have completed your level 1 combined safeguarding children and adult training and you are aware of your role and responsibilities to safeguarding children, young people and adults as outlined in the NHS Leeds CCG Safeguarding Policy.

If you have concerns about a breach in the terms of service for a particular platform, e.g. participation of underage children, nudity in images, use of unsuitable language, grooming, stalking or ideation that could lead to terrorist activities etc. you should report this to the service provider. You should also report this activity to your line manager and the NHS Leeds CCG communications Team as consideration may need to be taken regarding continued use of that platform.

If you are concerned that any criminal activity is taking place or that there's any extremist content that could influence behaviour that could threaten the health and wellbeing of an individual or the wider community you should report this to the police.

10. Risk and Privacy risk Assessment

When considering a new project involving: web access, establishing a social media presence or participating in new social media networks the use of this media should be risk assessed. Employees must address any privacy concerns of implementing new processes with the assistance of the Information Governance team and a Data Protection Impact Assessment (DPIA) must be undertaken.

A DPIA will:

- Identify privacy risks to individuals
- Protect the CCG's reputation
- Ensure person-identifiable data is being processed safely
- Document risks and risk mitigations

11. Incident Reporting

All actual, potential or suspected incidents involving use of the internet or social media need to be reported in line with the CCG's Incident Reporting Policy.

12. Related Law

Some of the key legislation and common law is set out below and how it may affect use of information the internet and social media. Employees need to be aware of legal requirements for both work and personal use (where it may have an impact on the CCG)

General Data Protection Regulation and Data Protection Act 2018
Sets out the conditions for the processing of personal information by organisations and individuals. Employees need to be aware that any use of personal information stemming from work related business can only be used where conditions of the Regulation / Act can be met.

Common Law Duty of Confidentiality
This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further except in certain circumstances:

- Where the individual to whom the information relates has consented.
- Where disclosure is in the public interest.
- Where there is a legal duty to do so, for example, a court order.

Confidential information could relate to personal information of an individual or information contained in a business document e.g. contract.

Freedom of Information Act 2000
Allows the right of access to anyone to recorded information held by a public authority (such as a CCG) via a request for specific information or through accessing information via the public authority's publication scheme. Release of information is subjects to exemptions and conditions of the Act.

All staff, however, should consider all information which they come into contact with through the course of their work as confidential and its usage and any disclosure would be in line with agreed duties and for authorised work purposes. This would be the case regardless of whether the information may be made available through the Freedom of Information Act. For release of CCG held information, the CCG already has in place the processes for making information available through the request procedure or has made certain information publicly accessible through the CCG Publication Scheme.

It should be noted, however, that where a document has been published in the public domain already it would be possible to link to the publication.

The Public Interest Disclosure Act 1998
This Act allows employees to voice authentic concerns about misconduct and malpractice without receiving penalties such as dismissal, victimisation, or denial of promotion, facilities or training opportunities.

Human Rights Act 1998
Article 8 of the Act provides a right of privacy for individuals. In complying with the Act, public authorities (to which the Act applies) such as the CCG need to ensure that personal and confidential information is not disclosed into the public domain (unless a legal justification exists to do so).

Computer Misuse Act 1990
Under this Act it is an offence to have unauthorised access to computer material or to undertake unauthorised modification of programs or data on a computer.

Copyright, Designs and Patient's Act 1998 (as amended by the Copyright Computer Programs Regulations 1992)
No member of staff shall infringe copyright in copyright works stored on internet sites. Staff should not that downloading copyright text or images from an internet site without permission may constitute infringement of copyright even if it is not the intention to republish such works. Staff must always check copyright notices on websites.

13. Training
There are information governance implications involved in the use of internet and social media especially in terms of the confidentiality and security and legal use of information, therefore, it is important that staff understand their information governance responsibilities. All staff will receive information governance training via the CCG's Statutory and Mandatory Training Programme. Managers must actively ensure that all staff undertake and successfully complete the mandatory information governance training.

14. Implementation and Dissemination
Following ratification by the Audit Committee this policy will be disseminated to staff via the staff e-bulletin and communication through in-house staff briefings.

This policy will be reviewed every two years or in line with changes to relevant legislation or national guidance.

15. Monitoring Compliance and Effectiveness of this Policy
An assessment of compliance with requirements, within the Data Security and Protection Toolkit (DSPT), will be undertaken each year. The DSPT includes requirements relating to confidentiality, data protection, security of and access to information. Incidents are reported and all serious information governance

issues must be reported by the SIRO at Governing Body level and in annual reports.

Any suspicion of fraud or bribery should be reported at the earliest available opportunity through the Report NHS Fraud website or telephoning 08000 28 40 60

16. Advice

Advice and guidance on any matters stemming from the policy can be obtained by contacting your Line Manager or through the IG team.

17. Associated Documents

This policy should be read in conjunction with the core Information Governance Policies, in particular the Confidentiality and Data Protection Policy, and Information Security Policy which set out the rules for security and confidentiality of information:

- Information Governance Policy and Management Framework
- Confidentiality and Data Protection Policy
- Freedom of information Act and Environmental Information Regulations Policy
- Information Security Policy
- Network Security Policy
- Records Management and Information Lifecycle Policy

Other Related Documents:

- Incident Reporting Policy
- Risk Management Policy
- Email Policy
- Disciplinary Policy
- Anti-Fraud Policy
- Anti-Bribery Policy
- Whistle Blowing Policy
- Communications Strategy
- Starters, Movers and Leavers Guidance

18. Appendices

Appendix A Policy Consultation Process:

Title of document	Social Media Policy
Author	Shak Rafiq, Communications Manager, Karen Rowe, Information Governance Manager
New / Revised document	Revised
Lists of persons involved in developing the policy List of persons involved in the consultation process:	Shak Rafiq Karen Rowe Ian Corbishely IG/BI/IT Committee

Appendix B Social Media Account Set Up Form

Before completing this form please have an initial chat with the communications and engagement team

Please complete this form and return it to Leedsccg.comms@nhs.net so that your request for a social media account can be processed. It will help you consider how you ensure any social media account is regularly managed, updated and adheres to best practice guidance.

Section one: applicant's details **Please complete once you have read and agree to acceptable use guidance (page 2)**			
Name and job title:			
Department / service:			
Email address		Telephone number	
Signature		Date	
Section two: authorisation details (line manager / head of service)			
Name and job title			
Telephone number		Date	
Section three: reasons for application			
Proposed topic / subject area			
Please tell us why you want to use social media (please use a separate sheet if needed)			
Which social media sites do you wish to use and why (please specify eg Twitter, Facebook, Snapchat, Instagram etc)?			

Who will have access to the account(s)?			
To be completed by the communications and engagement team			
Decision of authorising officer	Approve / Reject	Reason	
Signed		Date	
Next steps (eg discuss set up of new account, reason for decision, any training etc)			

Acceptable use guidance

At NHS Leeds CCG, we want to develop a forward-thinking approach to social media and welcome people wanting to set up professional accounts that help explain our work to our peers or to the wider public.

We want to support you as you look to set up a social media account(s) and this does mean having to have some guidance in place to help you.

Before you set up any professional social media account(s) you need to read and agree to the below

- Keep out of it. You should not get involved in any debates online especially as there are many trolls looking for an opportunity to provoke a reaction. If you're concerned by anyone's comments or posts please speak to the communications and engagement team
- Keep schtum. Respect patient and staff confidentiality. Clearly, you mustn't reveal or share any confidential information about patients or staff.
- Keep it clean. No insults, obscenities or other behaviour that wouldn't be acceptable in the office. And don't share anything that might offend, so think before you say anything about religion, politics or other potentially controversial subjects.
- Keep it legal. Respect copyright, fair use, data protection, defamation, libel and financial disclosure laws.
- Keep it professional. Social media should not be used to provide specific individualised health advice, people should be encouraged to see a healthcare professional. Providing generic advice on health is fine eg how to stop smoking, using inhalers correctly or signposting to local service – where possible link to information provided on the NHS website www.nhs.uk
- Keep it professional part two. We won't say any more than you're setting up a professional account to talk about professional issues or provide engaging content for your audience. Private messaging is a no no unless there's a valid business reason for doing so. For anything of a more personal nature there's other apps out there…
- Keep sober. Yes it happens, people use professional accounts whilst under the influence. So if you're planning a night out, the safest thing you can do is sign out of your accounts.

- Keep up to date. If a major news story is breaking and you're about to post a message that could be taken the wrong way, it'll be better to leave it.
- Keep it real. Fake news is a major issue, just like avoiding trolls you need to ensure you only post verified content and do not respond to anything you're unsure of as it provides credibility to anyone posting fake news. If in doubt please speak to someone in the communications and engagement team.
- Keep it secure. Trust is great but you shouldn't share your login details/passwords with anyone except those authorised to access your account.
- Keep active. It's important that once you set up any account(s) that you keep active on social media. We may ask you to take down an account if it's not regularly managed and maintained.

Golden rule. If you're not prepared to say it in a room full of people, don't share it on social media

This is also a good time to remind you that you need to consider the above when posting content from your personal account too.

Agreeing to acceptable use guidance

Before we consider your application, we need to ensure that everyone agrees to the acceptable use guidance.

Line manager or head of service

I agree to authorise this application on behalf of those named on this form and understand that I could be asked to take any action if the social media accounts fail to meet the guidance above or activity takes place contrary to any other CCG policies.

Name		Job title	
Signature		Date	

All staff named on this form responsible for managing social media account(s)

I have read and understood the guidance on this form. I also understand that any use of social media is in line with any existing polices such as, but not limited to, information governance policy and management framework and social media and internet policy. I also understand that the communications and engagement team reserve the right to ask us to suspend or delete any account(s) for the reasons specified above as well as during any extraordinary events.

Name		Job title	
Signature		Date	

Name		Job title	
Signature		Date	

Name		Job title	
Signature		Date	

Name		Job title	
Signature		Date	

If any other colleagues are provided access to any account(s) in the future, they must read and sign this form.