NHS
Bradford District and Craven
Clinical Commissioning Group

Internet and social media policy

This policy outlines a framework for all NHS Bradford district and Craven Clinical Commissioning Group (CCG) employees in understanding their obligations and responsibilities when using the internet and social media.

Key information

Responsible director:	Strategic director of organisation effectiveness
Author:	Kamal Wrathall, senior communications manager
Approval body:	Audit and governance committee
Date approved:	25 May 2022
Version:	2.0
Review date:	May 2024

Version control

Version no.	Date	Author	Description	Circulation
V1.0	Nov 2020	Kamal Wrathall	Version approved by audit and governance committee.	CCG wide
V2.0		Kamal Wrathall	Version approved by audit and governance committee.	CCG wide

Contents

1 Introduction

NHS Bradford district and Craven Clinical Commissioning Group (CCG) shares information about the work that we do on social media, and other online platforms such as websites, blog sites, discussion forums and interactive news sites. The CCG recognises that the use of the internet and social media is a valuable medium to assist in the conduct of its day to day business.

Social media and online activity is used by the CCG as a method of communication to help achieve strategic goals, namely:

- to help patients and the public understand their health, care and the services available to them
- to encourage participation and engagement with stakeholders
- as an enabler to allow the CCG to understand emerging developments or trends more quickly
- to allow important messages to be communicated to other organisations, employees, patients and the public in real-time (for example in response to a crisis such as increased weekend demand for A&E services)
- to enable the CCG to provide opportunities for open and transparent stakeholder engagement
- educational, developmental or research purposes
- professional development and accreditation
- personal development as agreed as part of the appraisal process and agreed by the users line manage

CCG staff may also access social media for personal use outside of their working hours. Nevertheless where employees access the internet and social media, they need to be aware of any implications and impact on themselves, the CCG and the wider NHS where they choose to discuss or post information pertaining to work related matters, breaching copyrights and downloading or posting inappropriate material.

The policy sets out a framework for employees when using the internet and social media for both business and personal use and enables them to make effective use of technology for the benefit of the CCG and its organisational aims and objectives and to avoid any adverse impact. The purpose of this policy is to also ensure that your interests as an employee of the CCG are protected as well as that of the CCG. This policy is not intended to discourage you from participating in online activity but seeks to advise you on how to participate and engage in online activity safely.

2 Scope of the policy

The policy applies to NHS Bradford District and Craven CCG and all its employees and must be followed by all those who work for the organisation, including the governing body, those on temporary or honorary contracts, secondments, pool staff, contractors and students.

There are no exclusions, and this policy also covers equipment used to access the internet and social media including computers, mobile phones and tablet devices.

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

3 Associated documentation

Your conduct and behaviour whilst operating on the internet and social media is viewed in the same manner as your conduct and behaviour at work. The CCG therefore has a range of other related policies and procedures that should be read in conjunction with this policy.

- Acceptable Standards of Behaviour at Work Policy
- Code of Business Conduct
- Communications and Engagement Strategy
- Confidentiality and Data Protection Policy
- Content Policy and Procedure
- Disciplinary Policy and Procedure
- Equal Opportunities and Diversity Employment Policy
- Fraud and Bribery and Corruption Policy
- Incident Reporting Policy
- Information Governance Policy and Procedure
- Risk Management Policy
- Whistleblowing and Raising Concerns Policy

4 Policy statement

The purpose of this policy is to ensure that:

Employees of the CCG understand their obligations and responsibilities with regard to the use of the internet and social media for both business and personal use. As an employee of the CCG, you are expected to uphold appropriate standards at all times line with the CCG Code of Business Conduct.

Employees understand how legislation such as the Data Protection Act and General Data Protection Regulations 2018 places obligations on the CCG and its employees as to how information by the CCG can be used.

5 Definitions and explanation of terms

Internet

The global communication network that allows almost all computers worldwide to connect and exchange information.

Social media

The term used for website and applications and other mobile communications technologies that enable users to create and share content or to participate in social networking.

Twitter

Twitter is a free social networking microblogging service that allows registered members to broadcast posts called tweets.

Facebook

Facebook is a social networking service that allows registered users to create profiles, upload photos and video, send messages, broadcast live, create groups, pages and connect with other people.

Instagram

Instagram is a online photo sharing and social network platform that allows members users to upload, edit and share photos and video, and broadcast live, with other members.

LinkedIn

LinkedIn is a free social networking site designed specifically for the business community. It allows members to connect with other professionals and upload photos, video, upload professional information and send messages.

Pinterest

Pinterest is an online service that allows users to upload, save, sort, and manage images—known as pins—and other media content (e.g., videos) through collections known as 'pinboards'.

TikTok

TikTok is a social media platform for creating, sharing and discovering videos.

Direct messaging apps

Direct messaging apps, such as WhatsApp and Snapchat, allow users to send private messages, images, audio or video, directly to an individual or groups of individuals.

Blog sites

A blog is a website (or area of another website) that is used as a discussion or information site. Users 'post' content on blogs, usually displayed in reverse chronological order.

Interactive news sites

An interactive news site will allow users to interact with news content, such as posts or videos, typically through commenting or sharing with other internet users.

YouTube, video, vlogs and podcasts

YouTube is a site where video content can be uploaded, viewed and commented on. There are many other similar platforms including Vimeo. Vlogs are video based blogs often sharing opinions and views. Podcasts technically are audio/voice based blogs posted on a regular basis.

Spam and junk mail

Junk mail is usually sent to an email account by direct marketing or direct mail firms. Spam mail is defined as unsolicited emails.

Streaming

Streaming means listening to music or watching video in 'real time', instead of downloading a file to your computer and watching it later. It is called streaming as users receive a continuous stream of data.

Multimedia

Multimedia is text, graphics, drawings, pictures, video, animation, audio, and any other media where information can be represented, stored, transmitted and processed digitally.

Online meeting platforms

Online meeting platforms such as Zoom, Microsoft Teams and Google Meets are used for hosting virtual meetings, sharing presentations and commenting.

6 Duties, accountabilities, roles and responsibilities

6.1 Duties within the organisation

The associate director of the organisation effectiveness has overall responsibility for this policy.

All employees of the CCG are personally responsible for compliance with the law in relation to their use of the internet and social media that involve the use of work derived information. Accountabilities and responsibilities in relation to information governance are set out in the Information Governance Policy and Framework, compliance with this policy is an obligation for all staff. Any breach of this could result in disciplinary action.

All line managers are responsible for ensuring that the employees they manage are aware of this policy and of their individual responsibilities with respect to the policy. Managers must ensure that the employees they manage have signed the Internet Access Declaration, have read and signed for all the Information Governance related policies and procedures and are up to date with all Information Governance training.

All employees are responsible for reporting incidents and near misses including breaches of this policy, using the CCG Incident Reporting Policy.

6.2 Responsibilities for approval

The audit and governance committee are responsible for the approval of this policy document.

7 Policy and procedure details

7.1 Usage

This policy covers your business and personal activity online. The internet involves fast moving technologies and it is impossible to cover all circumstances. Online activity, apps and social media includes, but is not limited to the following:

- Twitter – including but not limited to the information on profiles, posts, retweets, quoted tweets, pictures / images and direct messages.
- Facebook – including but not limited to the information on profiles, posts, shares, groups and pages, likes, comments, pictures / images, events and messages.
- Instagram – including but not limited to the information on profiles, posts, photographs / images, comments, likes and shares
- LinkedIn – including but not limited to the information on profiles, posts, shares, groups and pages, images, comments, likes and direct messages
- Pinterest – including but not limited to posts, shared boards, comments, pins, pictures / images and profiles
- TikTok – including but not limited to posts, likes, comments and shares

- YouTube – including but not limited to profiles, channels, videos, pictures, comments, shares and likes
- Blog sites – including but not limited to information on profiles, posts, shares, images and comments
- Interactive new sites – including but not limited to sharing and commenting on articles
- WhatsApp – including but not limited to direct messages, images, videos and audio
- Zoom / Microsoft Teams – including but not limited to screen sharing, document sharing, comments and direct messages

If you have access to social media sites and the internet at work, this has been setup for business use only. The use of social media and internet sites at work for personal use is restricted to outside working hours (for example lunch breaks or before / after work) or with the express permission of your line manager, this also includes the use of 'toggling' in and out of internet sites. You should not allow your activity on social media to affect your work. This extends to the use of social media and the internet on devices that may have been provided by the CCG (for example, mobile phones). During designated working time, any browsing of internet sites by employees must be related to work purposes.

7.2 Blocked sites

There are specific sites that the CCG will have blocked for reasons of security and confidentiality and to prevent access to sites that contain illegal information, such as illegal gambling sites, pornography or sites relating to terror activity. Should an employee need to check which sites are blocked, they should contact the information technology provider via the helpdesk.

Blocked sites may include those that provide file transfers. Any transfer of information that is confidential and personal needs to comply with the CCG policy requirements and the Data Protection Act and General Data Protection Regulations 2018. Where an employee still wishes to use a particular file sharing site that has been blocked then they need to contact the appropriate information governance lead.

7.3 Conduct

7.3.1 - Employees must not post or comment on any clinical, commercially sensitive, damaging, derogatory or libellous information on social media about the CCG. This includes, but is not limited to, our operations, financial position or strategy.

7.3.2 - There are strict rules within the CCG around information sharing which are stated in the Confidentiality and Data Protection Policy and the Information Governance Policy and Procedure. Never post patient identifiable information on social media. Please refer to the CCG confidentiality and data protection policy to familiarise yourself with the correct procedure for sharing confidential information. It is important to remember that the Information Commissioner's Office has enforcement rights and individuals and / or organisations can be fined up to 20 million Euros or 4% of annual turnover (whichever is greater) for serious confidentially breaches.

7.3.3 - Accessing, creating, downloading or transmitting any obscene or indecent images or data that is designed to harass, bully, annoy or cause anxiety to other people. The use of ethnic slurs, personal insults, dishonourable or discriminatory content related to those protected under the Equality Act 2010 will not be tolerated by the CCG. As a rule, do not engage in online activity that would also be deemed as unacceptable behaviour in the workplace.

7.3.4 - The internet and social media should never be used as a mechanism for workplace bullying (known as cyber bullying). Any acts of cyber bullying will be treated by the same procedures outlined in the CCG Acceptable Standards of Behaviour at Work Policy.

7.3.5 - Should there be a requirement for the CCG to monitor your online activity due to inappropriate use, this will be undertaken in accordance with the CCG Disciplinary Policy and Procedure. If the CCG has cause to monitor your current or previous social media activity, you will be advised as to the circumstances, nature, how your data and information will be used and any safeguards that may apply.

7.3.6 - If you have posted on social media and you need to amend your post (for example, if you have posted incorrect information), you must make it clear that an amendment has been made.

7.3.7 - You should not edit online sources of information (for example Wikipedia) using your corporate email account as changes can be traced back to a government IP (internet protocol) address. The amendments you make could be interpreted as the official views of the organisation and a number of personal details can also be traced from an IP address. Should you wish to alter such websites, do not do so without the express permission of the CCG communications and engagement team. This includes derogatory or offensive comments about the organisation as it constitutes a genuine opinion that someone may hold. Such comments must be reported to the CCG communications and engagement team for action.

7.3.8 - Social media and online forums / websites should not be used as a mechanism for whistleblowing. You should refer to the CCG Whistleblowing and Raising Concerns Policy.

7.3.9 - Employees should not speak on behalf of the CCG on social media or online without approval from the communications and engagement team.

7.3.10 - Should an employee be approached to produce or share online content for a third party, you should be mindful of any potential conflicts of interest. Any conflicts of interest should be discussed with your line manager.

7.4 Monitoring of internet use and social media

7.4.1 - The Information Governance handbook specifically states that all employees are accountable for the safekeeping of their computer login and that all activity and internet traffic is logged automatically. These logs may be audited by the CCG and where inappropriate usage is identified, disciplinary action may be taken and referral to the relevant professional body.

7.4.2 - If any information is downloaded, accessed or transmitted unintentionally that is deemed as a breach of this policy then this must be reported to your line manager or information technology/information governance lead immediately. This is to give employees the assurance that the unintentional breach does not result in any disciplinary action.

7.4.3 - Employees should be aware that monitoring may reveal sensitive data about them and by carrying out such activities using CCG resources, employees are consenting to the CCG being party to any sensitive personal data about them which can be accessed through monitoring. All internet activity is monitored but should an employee want to check what specific type of information is recorded, they should contact The Health Informatics Service Desk on 0845 127 2600.

7.4.5 - The CCG communications and engagement team is responsible for the corporate social media accounts and online activity of the CCG. The following are some examples of when you should speak to the communications team about social media:

- items relating to the CCG that you would like us to share on social media or online in an official capacity
- any employee who wishes to use social media as an official channel of communication
- if you notice a patient or a member of the public making comment about organisations (positive or negative)
- if there is information on social media that you believe the organisation should be acting upon
- if you plan to set up a social media account on behalf of the CCG
- if you have posted information on social media or online and you believe that it contradicts the advice and guidelines set out in this policy

7.4.6 - The CCG social media accounts are monitored within working hours (Monday to Friday, 8am to 5pm, excluding bank holidays).

7.4.7 - Social media and online activity may be reviewed by journalists / news / media outlets. If you are contacted by a journalist / news / media outlet about activity that you have conducted online that relates to the CCG, you must speak to the communications and engagement team who will advise on how to proceed.

7.5 Identification and privacy

7.5.1 - You may post information online under your own name or a pseudonym. Should you identify yourself as an employee of the CCG you must make it clear that any views are your own and therefore do not reflect the official position of the CCG. This is typically in the form of a disclaimer stating “any views posted are my own and not necessarily those of my employer”.

7.5.2 - Employees must refrain from using their CCG email address on their social media profile. The exception to this rule is if the account has been set up as a CCG corporate account with the express permission of the CCG communications and engagement team. The communications team can be contacted on communications@bradford.nhs.uk

7.5.3 - Photographs or personal information about colleagues (including, but not limited to email address or telephone number) without their express permission should not be posted, in line with General Data Protection Regulations. If you need a copy of the CCG photograph consent form, please email communications@bradford.nhs.uk

7.6.4 - Employees of the CCG must not impersonate another colleague on social networking forums or internet sites.

7.6 Use of social media

7.6.1 - Social media encompasses a number of internet platforms such as Twitter, YouTube, Facebook and many more which allow organisations and individuals to share and publish information online. The CCG recognises that social media is used as a method of communication to raise its profile and interact with stakeholders and patients in line with the CCG strategic objectives.

There are risks associated with the use of social media and where employees use this for work and personal use they must comply with relevant legislation and make sure that copyright is not infringed and defamation of character does not occur.

7.6.2 - If you are responding to an existing post online (for example on an interactive news site), you must not do this when acting in an official capacity as an employee without the express permission of the CCG communications and engagement communications team.

7.6.3 - All corporate digital information may be subject to the Freedom of Information Act 2000 requests, subject access requests and/or legal proceedings. If writing on behalf of the organisation, you should only record facts which you are confident can be supported by other information. If you are providing an opinion, you may be asked to put it into context at a later stage.

7.6.4 - You must make sure you understand your obligations under the CCG's confidentiality and data protection policy. You are personally responsible for compliance with the law in relation to data protection and confidentiality. There is a non-disclosure of confidentiality information clause in the employment contract for all employees. Any breach of confidentiality will be treated in accordance with the Disciplinary Policy and Procedure.

7.7 Incident reporting

7.7.1 - All incidents whether actual, potential or suspicious involving the use of the internet and social media need to be reported and documented in line with the relevant policy, please refer to section three for related policies and procedures. Information Governance breaches, should be reported and documented in line with the Incident Reporting Policy. Incidents which may constitute employee misconduct should be reported in line with the CCGs disciplinary policy and procedure.

7.8 Advice and support

Where employees of the CCG are unclear about issues relating to the guidelines set out in the policy, they need to refer to their line manager in the first instance.

Further advice on and support on all aspects of the policy to ensure application can be obtained by contacting the information governance lead for the CCG by email at THIS.InformationGovernance@this.nhs.uk

Employees can also get in touch with the communications and engagement team about social media or online activity by email at communications@bradford.nhs.uk

8 Dissemination, implementation and training

The Audit and Governance Committee is responsible for formal approval and monitoring compliance with this policy. The first iteration of this policy, and any subsequent updates,will be disseminated to employees via established communications such as email, staff briefings, CCG intranet and the CCG weekly staff bulletin.

Incidents which are in breach of the CCG Information Governance procedures should be reported as detailed within the Information Governance Policy and Framework and the Incident Management and Reporting Policy. Incidents which are deemed to be employee misconduct should be reported in line with the CCG's disciplinary policy and procedure.

Any suspicion of fraud and bribery should be reported at the earliest opportunity to the NHS Fraud and Corruption line on 0800 028 40 60 or the local fraud counter fraud specialist using the following details:

- Lee Swift – Audit Yorkshire, telephone – 01274 228193 / 07825 110432 or email lee.swift1@nhs.net

- If Lee Swift is unavailable, contact Audit Yorkshire using the details on their website: https://www.audityorkshire.nhs.uk/

All employees will receive information governance training through the CCG statutory and mandatory e-learning platform. Managers must ensure that employees undertake and complete their mandatory information governance training which also forms part of the pay progression and appraisal process. It is important that employees understand the governance implications and responsibilities involved in the use of the internet and social media.

9 Review and monitoring

The policy and procedure will be reviewed every twelve months by the communications and engagement team in conjunction with the senior leadership team and information governance leads where applicable. Where review is necessary due to legislative change, this will happen immediately.

10 Public sector equality duty

The Equality Act 2010, available on the GOV.UK website, includes a general legal duty to:

- eliminate unlawful discrimination, harassment, victimisation and any other conduct prohibited by the Act
- advance equality of opportunity between people who share a protected characteristic and people who do not share it
- foster good relations between people who share a protected characteristic and people who do not share it

The protected characteristics are:

- age
- disability
- gender reassignment
- marriage or civil partnership (only in respect of eliminating discrimination)
- pregnancy and maternity
- race
- religion or belief
- sex
- sexual orientation

One of the aims of this policy is to ensure that the internet and social media are not used by CCG employees to discriminate against, bully, harass or victimise any individual or group of people with an Equality Act protected characteristic.

11 References

Should you wish to read more about the appropriate use of social media, the following websites may be useful to you:

- General Medical Council - http://www.gmc-uk.org/guidance/ethical_guidance/21186.asp
- NHS employers - https://www.nhsemployers.org/search-results?q=social+media

- Royal College of General Practitioners social media highway code - http://www.rcgp.org.uk/social-media
- Royal College of Nursing - http://www.rcn.org.uk/professional-development/publications/pub-004534
- Social media guide for civil servants - https://www.gov.uk/government/publications/social-media-guidance-for-civil-servants/social-media-guidance-for-civil-servants

Key legislation and common law related to the use of the internet, apps and social media is set out below.

- The Regulation of Investigatory Powers Act 2000 and Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Data Protection Act and General Data Protection Regulations 2018
- Common Law Duty of Confidentiality
- Freedom of Information Act 2000
- The Public Interest Disclosure Act 1998
- Human Rights Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988

12 Appendices

12.1 Best practice guidelines

1. Be aware of how you conduct yourself - you should not say anything online that you would not be comfortable saying in other forms of communication, such as face to face, emails or over the telephone. Any information that you post, share or like on social media or online, should be consistent with how you wish to present yourself to the public, patients and colleagues.
2. Although you are likely to be acting with the best intentions, it is important to remember that anything you post, comment or share online may not only harm your personal reputation but also the reputation of the CCG. Stakeholders, patients and members of the public may not always distinguish between content that you post independently and content you may post as a representative of the CCG.
3. Be respectful of other people's information – it is their choice to share their material on social media or online. Before you reuse someone else's material, you should check with the owner for their permission first.
4. In the interest of personal security, the CCG strongly advise against linking personal information about your family to your online profile and linking one social media account to another.
5. Make sure you understand and have set the correct privacy settings on your social media or other online accounts. It is important to check your privacy settings frequently as social media sites will update or add new options on a regular basis that may affect the level of security on your account.
6. You should be aware of your 'digital footprint'. Every time you add something about yourself online, you increase your digital footprint. You also increase the digital footprint of others each time you mention someone else, for example tagging another

person in a photo. Companies routinely collect information about your digital footprint to market goods and services but you should be aware that your digital footprint could also be monitored by individuals looking for information about you. You should be aware that even if you have deleted information from social media or online, you still leave a ‘digital footprint’.

7. Even if you believe that a comment you have made on social media has been set as private, it is worth remembering that once your message has been posted / sent, the recipient(s) have the ability to share that information, no longer deeming it as private.
8. A photo or video of a person is personally identifiable data, this includes screenshots of virtual meetings that you may be tempted to share on social media, you should have permission from everyone who features. The same rule also applies for recording meetings – this must be made clear before people join and you must have permission from all participants to share anything publicly.
9. If you are at all in doubt, don’t share.