

# Social media and digital content policy

Ref:	LSCICB_Corp05
Version:	V3
Purpose	This policy is for day-to-day use by the communications and engagement (C&E) function of NHS Lancashire and South Cumbria Integrated Care Board. It primarily supports C&E colleagues, but also all ICB staff in relation to their work-related social media usage.
Supersedes:	Any previously agreed policies
Author (inc Job Title):	Mark Britton, digital communications manager
Ratified by: (Name of responsible Committee)	Executive Committee
Cross reference to other Policies/Guidance	
Date Ratified:	08 July 2025
Date Published and where (Intranet or Website):	21 July 2025 intranet and website
Review date:	01 November 2027
Target audience:	All LSC ICB Staff

*This policy can only be considered valid when viewed via the ICB website or staff intranet website. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one published.*

Document control:		
Date:	Version Number:	Section and Description of Change
17/6/25	3.0	Updated brand name of X (formally known as Twitter). Updated monitoring arrangements to reflect updated ICB committee arrangements. Added reference to social media use during incidents / emergency situations. Added reference to the use of generative AI.

## Contents

<b>Section No.</b>	<b>Section Heading</b>	<b>Page No.</b>
1	Introduction	5
2	Purpose	6
3	Scope	7
4	Responsibilities	7
5	Definitions	8
6	Principles – participating in online activities	8
7	Best practice	9
8	Safeguarding	10
9	References and endorsements	14
10	Dealing with emergency situations	18
11	Generative AI use	18
12	Equality impact	18
13	Implementation and dissemination	19
14	Training requirements	19
15	Monitoring and review arrangements	20
16	Consultation	20

## 1. Introduction

This policy is for day-to-day use by the communications and engagement (C&E) function of NHS Lancashire and South Cumbria Integrated Care Board (from this point referred to as the ICB). The C&E function manages the corporate social media accounts for the ICB and the Lancashire and South Cumbria Health and Care Partnership, as well as supporting other ICB and partner colleagues (for example primary care) to manage other professional social media accounts. This policy supports C&E colleagues and all ICB staff in relation to their work-related social media usage.

The ICB recognises the use of social media and other digital messaging services and platforms are part of everyday life. They can also be used to support communications and engagement as part of our employment. This is a rapidly growing area and this policy also supports our engagement strategy.

We use social media to provide opportunities for genuine, open, honest and transparent engagement with stakeholders, giving them a chance to participate and influence decision making. Everyone working at the ICB can help by sharing these messages more widely with their networks.

Corporate social media platforms are centrally managed by the communications and engagement directorate and all posts will be carried out by them in line with corporate demands and priorities.

These platforms are:

- Facebook: [@LSCICB](#)
- X: [@LSCICB](#)
- LinkedIn: [@LSCICB](#)
- Instagram: [@LSCICB](#)
- Youtube: [Lancashire and South Cumbria ICB](#)

NHS organisations use social media to engage with members of the public and other stakeholders and to share key messages around patient services and promote positive health and wellbeing. Social media enables greater engagement with parts of society and local communities which might not be reached through traditional media such as local newspapers and radio. Social media facilitates two-way communication between commissioners and providers, and service users.

Effective use of social media supports the ICB to discharge its duty to make sure patients, carers and members of the public are involved, engaged, communicated with and consulted, in general and more formally, with in the following areas:

- Development and consideration of proposals for any changes in the way services are provided.
- Any decisions affecting the operation of services.

Via the C&E function, the ICB operates corporate accounts on X, Facebook, Instagram, LinkedIn and YouTube. This policy provides guidance on social media/networking and the external use of other online tools such as blogs, discussion forums and interactive 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.

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.

## **2. Purpose**

The objective of this policy is to help protect the organisation and you as a colleague. It will protect your interests and advise you of the potential consequences of your behaviour and any content you might post online - whether acting independently or in your capacity as a representative of the ICB.

It is also to set out the clear expectation that if a member of staff identifies an association with the ICB or NHS as a whole, discusses their work and/or colleagues, or comes into contact, or is likely to, with service users on any social media platforms, they will behave appropriately and in a way which is consistent with their professional code of conduct.

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.
- Make sure the organisation's reputation is not brought into disrepute and that it is not exposed to legal risk.
- Make sure internet users can distinguish official corporate ICB information from the personal opinion of staff.

### **3. Scope**

This policy applies to all employees working for and on behalf of the ICB. This includes contractors, agency staff and those seconded in or out of the ICB. The policy also relates to equipment provided by the ICB to allow you to carry out your role and your personal equipment.

This document is not a social media strategy, or guidance on how to use individual social media tools and platforms, and each individual or business area should assess the value of using these tools in an official capacity following advice and guidance from the ICB's communications and engagement directorate and follow this policy if they decide to do so.

### **4. Responsibilities**

#### **4.1 Responsibility of the ICB**

The responsibility for the provision of an agreed social media and digital content policy lies with the ICB director of communications and engagement reporting into the ICB executive. The ICB executive accepts it will have responsibility for the smooth running of the organisation, and to ensure that any social media activity on behalf of or that relates to the ICB is managed in the appropriate manner.

#### **4.2 Responsibility of human resources (HR)**

To provide advice and support to managers in relation to the application of this policy. To make sure the policy is applied fairly, equitably and consistently throughout the ICB.

#### **4.3 Responsibility of managers**

It is the responsibility of all managers employed within the ICB to make sure they are aware of this policy and how to support staff with their social media activity.

Managers should ensure that they follow the guidelines of this policy and advise staff in their teams appropriately.

#### **4.4 Responsibility of employees**

Employees should make sure they are aware of the general standards of this policy. If they have to manage and/or engage in social media activity, they must do so in the appropriate manner as outlined in this policy.

## **5. Definitions**

### **5.1 Social media**

Social media is a computer-based technology that facilitates the sharing of ideas, thoughts, and information through the building of virtual networks and communities. By design, social media is internet-based and gives users quick electronic communication of content.

### **5.2 Digital platforms**

Social media and digital platforms are the same. They are defined as a web-based and mobile-based internet applications that allow for the creation, access and exchange of user-generated content. Examples of social media platforms are Facebook, X, Instagram, LinkedIn and YouTube.

### **5.3 Digital content**

Digital content can include news, information, blogs, video and entertainment distributed over the internet and is accessed digitally by users.

### **5.3 Instant messaging (IM)**

Instant messaging is a form of text-based communication in which two or more people participate in a single conversation over their computers or mobile devices within an internet-based chatroom. WhatsApp and Snapchat are the popular IM services. This policy covers all forms of social, digital and messaging formats referred to as social media throughout. The above examples are not an exhaustive list and should be accepted as including other formats as technology evolves.

## **6. Principles – participating in online activities**

Our staff are our best ambassadors. Many already use social media, interactive and collaborative websites and tools, both in a personal and professional capacity. Rather than try to restrict this activity, the ICB wishes to embrace it. This demonstrates our commitment to a culture of openness and to empower staff to interact online in a way that is safe, credible, consistent, transparent and relevant.

There is an increasingly blurred line between what was previously considered 'corporate social networking' (which could be useful to the business) and 'social networking' (which is for personal use), to an extent where it may no longer be possible, or desirable, to make that distinction. For example, there is a tendency for people to maintain just one X account, which is used to post a mixture of business related and personal content.

However, posts made through personal accounts that are public can be seen and may breach organisational policy if they bring the organisation into disrepute. This



includes situations when you could be identifiable as an ICB employee while using social networking tools or occasions when you may be commenting on ICB related matters in a public forum. Staff should use their own discretion and common sense when engaging in online communication.

## **7. Best practice**

The following guidance gives some general rules and best practices which you should always abide by:

- The same principles and guidelines that apply to staff activities in general also apply to online activities. This includes forms of online publishing and discussion, e.g. blogs, images and file-sharing, user-generated video and audio, virtual worlds and social networks.
- When online, use the same principles and standards that would when communicating in other formats with people you do not know - if you wouldn't say something in an email or letter, don't say it online.
- Identify yourself by giving your name and, where relevant, role at the ICB if you are discussing ICB related matters. Write in the first person. You must make it clear that you are speaking for yourself and not on behalf of the ICB and must not use the organisation's logo on personal web pages or social media accounts.
- Be aware that people who join your networks and participate in groups that you are a member of may be colleagues, clients, journalists or suppliers. It is also possible that people may not be who they say they are, and you should bear this in mind when participating in online activities.
- If you publish content to any website outside of the ICB that could be perceived to have a connection to the work you do or subjects associated with the ICB, you must display a disclaimer such as this: "My postings on this site reflect my personal views and don't necessarily represent the positions, strategies or opinions of NHS Lancashire and South Cumbria ICB."
- Respect copyright, fair use, data protection, defamation, libel and financial disclosure laws and do not reveal confidential information about patients, staff, or the organisation.
- Never post any information that can be used to identify a patient's identity or health condition in any way.
- Social media should not be used to attack, deliberately offend or abuse others.
- Be friendly and non-judgemental of others.
- Do not provide confidential or other proprietary information on external websites.

- Do not publish or report on conversations that are private or internal to the ICB.
- Do not cite or reference partners or suppliers.
- Respect your audience. Do not use personal insults, obscenities, share indecent posts or images or engage in any conduct that would not be acceptable in the workplace.
- Show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory, such as politics or religion.
- Be aware of your association with the ICB when using social media. If you identify yourself, or are identifiable, as an employee of the ICB, make sure your profile and related content is consistent with how you wish to present yourself to colleagues and stakeholders. Be aware that you may be identified as an employee by any public use of your NHS email address.
- If you are asked to participate in a social network for commercial or personal gain, this could constitute a conflict of interest. You should refrain from entering any online social networking activity for commercial gain.
- If someone from the media contacts you about a post you have made, you must notify and seek advice from the communications and engagement function immediately.
- Correct your own mistakes and don't change previous posts without indicating that you have done so.
- Don't use social media to 'whistle blow'. All staff who wish to raise concerns have legal protection under the Public Disclosure Act 1988.

## **8. Safeguarding**

During the course of your work 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 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, steal their identity or commit other crimes.
- 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 considered.

## 8.1 Mitigating the risk

The use of social media by an NHS organisation and its staff can expose both the organisation and the member of staff to unexpected information risks or liabilities, even where these social media sites are not accessed directly from work.

There are a range of potential risks and impact consequences that the ICB and its staff should be aware of:

- **Unauthorised disclosure of business information and potential confidentiality breach.** Once loaded to a social media platform, organisational information enters the public domain and may be processed, stored and re-used anywhere. Information published online is almost impossible to remove and can remain in the public domain indefinitely. Consequently, organisational control can be lost, and reputational damage can occur.
- **Malicious attacks associated with identity theft.** Most sites encourage users to create a personal profile. People often place a large amount of personal information on social media platforms, including photographs, details about their nationality, ethnic origin, religion/faith, addresses, date of birth, telephone contact numbers, and interests.
- **Legal liabilities from defamatory postings by staff.** When a person registers with a website, they typically must indicate their acceptance of the site's terms and conditions. These can be several pages long and contain difficult to read and understand legal jargon. Such terms and conditions may give the site 'ownership' and 'third party disclosure' rights over content placed on the site and could create possible liabilities for organisations that allow their employees to use them.
- **Reputational damage.** Ill-considered or unjustified comments may adversely affect public and professional opinion towards an individual, their employer or another organisation, contractor, service provider or business partner.
- **Staff intimidation or harassment.** In extreme cases a negative reaction to a social media post could lead to anxiety, distress and personal safety issues.

To help prevent incidents that could lead to reputational, legal or financial damage to the organisation and/or individual(s), it is important that potential risks are managed by adopting a consistent approach. The main defence against threats associated with the use of social media is user awareness. Steps you can take to promote safety online include:

- 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 that site.
- Do not accept 'friend' requests from anyone you suspect to be underage.
- Avoid collecting and never ask users to divulge any personal details, including email, address, school information, phone numbers, other social media profiles.
- You should not use any information in an attempt to locate and or meet a child, young person or vulnerable adult, that is not explicitly required for your job.

The Sexual Offences Act (2003) combats increasing sexual approaches to access children and young people online. 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.
- Promote safe and responsible use of social media use 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 users, always follow the requirements set out in the Data Protection Act 1998.

Collecting personal data should be done via alternative means, e.g. by signposting to a form on the website.

## **8.2 Safeguarding yourself**

In addition to the behaviours outlined above, if you are using corporate or personal social media accounts for work related activity, you should also:

- Make sure your privacy settings are set up so that personal information you may not want to share is not available to members of the public.
- Have a neutral picture of yourself as your profile image.
- Only use your work profile and contact details (email or telephone) for your work-related activity. They should not be used on a personal account.
- If you are not sure, do not proceed without advice and support.
- Do not engage in intimate or sexual conversation or share intimate, compromising, sexual, indecent or pornographic or socially offensive images or material.

Should you encounter a situation while using social media that threatens to become antagonistic you should politely disengage and seek advice from your line manager or the communications and engagement function or HR.

While using social networking sites in a personal capacity, it should still be recognised that the actions of staff can damage the reputation of the ICB and all communications that are made, even in a personal capacity must not:

- Behave in a manner that would be unacceptable in any other situation.
- Bring the ICB into disrepute.
- Breach confidentiality.
- Make comments that could be considered to be bullying, harassment or discriminatory.
- Use offensive or intimidating language.
- Use social media platforms in any way which is unlawful.
- Post inappropriate comments about colleagues.
- Post remarks which may unwittingly cause offence and constitute unlawful discrimination in the form of harassment.

- Comment on work-related issues.

### **8.3 Reporting safeguarding concerns**

Any content or online activity which raises a safeguarding concern must be reported to the ICB safeguarding lead. As a minimum you should ensure you have completed your statutory and mandatory safeguarding e-learning and be aware of your responsibilities to safeguarding children, young people and adults as outlined in the ICB safeguarding policy.

Any online concerns should be reported as soon as identified as law enforcement and child/adult safeguarding agencies may need to take urgent steps to support the person. Where a child, young person or adult is identified to be in immediate danger, dial 999 for police assistance. 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. If you suspect a colleague is using the internet or social media in a way that raises safeguarding concerns, including accessing sites concerning radicalisation, or accessing illegal materials, you should seek advice from your line manager or the safeguarding team.

You should also report this activity to your line manager and the safeguarding directorate as consideration may need to be taken regarding continued use of that platform. You should report any harassment or abuse in the course of your duties or from other employees to your line manager and HR. 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.

## **9. References and endorsements**

For social networking sites such as LinkedIn where personal and professional references are the focus, if you are representing yourself as an NHS Lancashire and South Cumbria ICB employee, you may not provide professional references about any current or former employee, contactor, provider or contingent worker. You may provide a personal reference or recommendation for current or former ICB employees, contractors, providers and contingent workers provided:

- the statements made and information provided in the reference are factually accurate; and
- you include the following disclaimer below: "This reference is being made by me in a personal capacity. It is not intended and should not be construed as a reference from NHS Lancashire and South Cumbria ICB."

## **9.1 Responding to the media**

As an organisation, we do not encourage staff to engage in unofficial or spontaneous exchanges in response to published media comment such as newspapers, newsfeeds, blogs etc. If you intend to do so, you must identify yourself as an ICB employee and make it clear that you are speaking for yourself. Wherever possible include the following disclaimer:

“These views are entirely my own and not those of my employer.”

When acting in your official capacity as an employee, on behalf of the ICB, you must not engage in responding to content published by third parties by adding comments. If you read something online that you feel is factually incorrect, inaccurate or otherwise needs an official response from the ICB you must refer the matter to the C&E function.

## **9.2 Representing the ICB online in an official capacity**

While we encourage individual members of staff to use social media to share and reflect positively on the work of the ICB, it is important that the organisation maintains a coherent online presence through the strategic use of official communication channels. Therefore, without having developed a business case, and gained approval from the C&E function to do so, you must not engage in social media activity that seeks to represent the official views of the ICB.

## **9.3 Establishing an official presence on social media sites**

Using social networking sites to communicate with stakeholders in a professional capacity is in many cases entirely appropriate. However, it is important that the time and effort staff spend on them is justified by the value to the business, and that the inherent risks are considered before this type of media is used. Social networking platforms can offer many opportunities to reach a specific audience but there are also potential pitfalls which staff must be careful to avoid.

If you wish to establish an ICB presence on a social media site you must discuss your proposal with the C&E function in the first instance, to make sure it is appropriate. The team will provide advice on the things you will need to consider such as: project management, time and resources needed to implement, editorial and approvals policy, evaluation process and timeframes, risks and issues, exit strategy, how to link this activity to the overall business plan for a programme or business area, and stakeholder consultation and approvals. In many cases the best choice is to develop usage of the existing corporate channels.

Before establishing a social media presence, a business case must be prepared, outlining how this activity will benefit the programme or business area and the benefits to be realised, compared to the costs in time and resources of doing so. The

business case must be closely aligned to the overall communications plan for a programme or business area and undergo appropriate stakeholder consultation and governance before being implemented i.e. approved by the C&E directorate and appropriate director. Given the time and resource involved in effectively managing a presence in social networking media, there must be a clearly evidenced demand from an audience for engagement activity using a particular channel, rather than engagement using existing online networks.

New social media accounts must be approved by the C&E directorate which will use the following acceptance criteria. Social media accounts must:

- Have clearly defined objectives and KPIs as part of an approved communications plan.
- Have a content plan, editorial purpose and requirement to communicate regularly with a specific group of stakeholders on an ongoing basis.
- Be based on clear evidence of user needs and their use of that channel (not hearsay).
- Be sufficiently resourced to allow accounts to be checked multiple times a day with responses to questions/comments provided as appropriate.
- Not be used for promoting internal initiatives.

Please note that accounts may be closed for the following reasons:

Inactivity	No original posts made for one month or more
Frequency	Less than one tweet/post a week over a two-month period
Interest	Account has been active for six months or more but has less than 100 followers
Relevance	Programme or project has closed
Governance	Account not managed through corporate process

Also note, requests for information made via X or other online channels can be considered as freedom of information (FOI) requests where the real name of the requester is discernible. These should be passed to the FOI Team and/or the C&E directorate.

## 9.4 Official blogs

Blogs are a great way to share engaging content, written using an informal and personal tone, and stimulating discussion. If you wish to set up a blog to write in your capacity as an ICB employee, please discuss your proposal with the C&E directorate in the first instance. The team can provide advice on the types of things you will need to consider, such as content; timing; newsworthiness; time and resources to manage



and maintain; editorial policy; whether this is the best medium for your message and how it might fit into the bigger engagement picture. Opportunities occasionally arise for employees to blog, in an official capacity, on alternative platforms or websites. To ensure that they are appropriate, and provide benefit to the organisation, these opportunities must be discussed, and agreed, with the C&E directorate.

## **9.5 Video and media file sharing**

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

To reach the widest audience, it is important that ICB public video content is placed on the ICB YouTube channel from where it can be shared, embedded on ICB owned websites and those owned by others. 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 must be branded appropriately, and be labelled and tagged accordingly. It must not be credited to an individual or production company. People's images are classed as personal data and permission must be sought from the individual prior to publishing them in the public domain. For further information and advice please contact information governance or the C&E directorate.

As an organisation we have a moral and legal responsibility to ensure that accessibility guidelines are met and that we provide material that is usable by all, regardless of disability or access to the latest technology. When publishing video closed captions should be added. For further guidance on appropriate multimedia file formats, legal and accessibility considerations, contact the C&E directorate.

## **9.6 Online surveys, slides and presentations**

If you wish to run an externally facing online survey, please contact the C&E function. It is important the ICB takes a joined-up approach to contacting stakeholder groups, so survey activity may need to be considered in the context of other pieces of work.

## **9.7 Participation in collaborative communities of practice**

If you wish to participate in online collaboration using externally facing web-based tools, with NHS colleagues or suppliers, on ICB projects and documents, you must carefully consider security. In most cases, when involved in collaborative working, discussion and the sharing of work-related information and documents must take place in a closed environment, behind a secure login, to minimise the risk of unapproved or sensitive material reaching the public domain. All information stored on internal or external websites must be held in accordance with the ICB information governance (IG) policies. If you have a requirement to set up a new collaboration,

community of practice or consultation space, you must contact the C&E function and IG to discuss your needs in the first instance. They will be able to advise on the tools available which fit your requirements.

## **10. Dealing with Emergency Situations**

The use of social media as a tool to warn and inform people in the event of a major disaster or emergency situation is covered in the organisation's emergency plan.

## **11. Generative AI use**

The ICB is committed to embracing responsible use of generative AI technology to deliver effective, engaging and increasingly relevant communications to the public. The ICB follows official guidance on [using artificial intelligence in the public sector](#) and the recommendations: [Artificial intelligence use in NHS communications: insights, risks and recommendations for safe and effective adoption of AI in NHS communications](#)

### **The ICB will:**

- Always use generative AI in accordance with the latest official guidance.
- Uphold factuality in the use of generative AI. This means not creating content that misleads, in addition to not altering or changing existing digital content in a way that removes or replaces its original meaning or messaging.
- Engage with appropriate partner organisations, strategic suppliers, technology providers, and civil society, around significant developments in generative AI, and the implications for its use in government communications.
- Continue to review reputable research into the public's attitudes towards generative AI and consider how this policy should evolve in response.

### **The ICB will not:**

- Use generative AI technologies in ways that conflict with our values or principles.
- Use generative AI to deliver communications to the public without human oversight, to uphold accuracy, inclusivity and mitigate biases.
- Share any private, protected, or sensitive information with third-party AI providers without having appropriate data sharing and security agreements in place.

## **12. Equality impact**

The ICB aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, making sure none are placed at a disadvantage to others.

A stage 1 Equality and Health Inequalities Impact and Risk Assessment (EHIRA) in relation to this policy has been completed. There is no requirement for a stage 2 (EHIRA)

### **13. Implementation and dissemination**

The policy will be implemented by the ICB communications and engagement function and shared with wider ICB staff via the social media section of the intranet and line managers.

### **14. Training requirements**

Whilst there are no specific training requirements, there are specific roles who need to be familiar with the document:

- Members of the communications and engagement directorate.
- Members of the HR function.
- Line managers.
- Anybody wishing to establish an official presence on social media.

## **15. Monitoring and review arrangements**

This policy will be monitored and reviewed by the communications and engagement function. Its impact will be monitored and measured through regular insight reports which will be presented to the executive committee.

Because of the rapidly evolving nature of digital communications this policy will be reviewed on an annual basis, and in accordance with the following on an as and when required basis:

- Legislative changes
- Good practice guidance
- Case law
- Significant incidents reported
- New vulnerabilities
- Changes to organisational infrastructure

### **15.1 Non-compliance**

This policy applies to all forms of communication, whether it be verbal, print or online. Staff should remember that they are ultimately responsible for what they publish and that there can be consequences if policies are not adhered to. If you are considering publishing something that makes you even slightly uncomfortable, review this policy and ask yourself why that is. If you're in doubt or in need of further guidance, please contact the C&E function to discuss.

Non-compliance with this policy may lead to disciplinary action in accordance with the ICB's disciplinary policy. You are also reminded that actions online can be in breach of the related policies listed on the front page of this policy and any breach may be treated as misconduct.

## **16. Consultation**

The policy has been shared for consideration by ICB communications and engagement professionals to ensure it meets best practice standards. The policy aligns with best practice set out in other NHS organisations.