NHS
Shropshire, Telford and Wrekin
Clinical Commissioning Group

Social Media and Digital Content Policy

Author(s) (name and post):	MLCSU HR Team
Version No.:	Version 1
Approval Date:	July 2021
Review Date:	July 2022

Document Control Sheet

Title:	Social Media and Digital Content Policy		
Electronic File Name:	STWCCG Social Media and Digital Content Policy - July 2021		
CCG document ref:	HR020		
Placement in Organisational Structure:	Corporate Affairs		
Consultation with stakeholders:	Staff and staff side representatives		
Equality Impact Assessment:	Completed and statement included in section 15		
Approval Level:	Audit Committee		
Dissemination Date:	27.07.21	**Implementation Date:**	21.07.21
Method of Dissemination:	Website, Staff newsletter		

Document Amendment History

Version No.	Date	Brief Description
Version 1.0	July 2021	New policy

The formally approved version of this document is that held on the NHS Shropshire, Telford and Wrekin CCG website: www.shropshiretelfordandwrekinccg.nhs.uk

Printed copies or those saved electronically must be checked to ensure they match the current online version.

Contents

1. Introduction

The Clinical Commissioning Group (the CCG) recognises that the use of social media and other digital messaging services and platforms are increasingly being used in everyday life and can be used to support communications as part of our employment. This is a rapidly changing area, and this policy supports our communication and engagement strategies with each other and the communities we serve.

The CCG uses 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 CCG can help by sharing these messages more widely with their networks.

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 engagement with sections of society and local communities that might not be reached through traditional media such as local newspapers and radio.

Social media facilitates two-way communication between service providers and service users while enabling more effective engagement with young people and seldom-heard groups.

Effective use of social media supports the CCG to discharge its duty to ensure that patients, carers and members of the public are involved, communicated with and consulted 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 Communications and Engagement team, the CCG currently operates corporate accounts on the Twitter, Facebook 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.

Although this policy refers to your CCG employment, it is by default, applicable to all staff as members of the NHS.

2. Purpose

The objective of this policy is to help protect the organisation, but also to protect the employees interests and to advise the employee of the potential consequences of the employees' behaviour and any content that the employee might post online, whether acting independently or in your capacity as a representative of the CCG.

It is also to to set out the clear expectation that, if a member of staff identifies an association with the CCG or NHS, discusses their work and / or colleagues, or comes into contact, or is likely to, with service users on any social media platforms, the employee will behave appropriately and in a way which is consistent with the relevant professional code of conduct and also- where relevant the CCG's values and Behaviour Charter.

The aims of this document are to:

- Provide clarity to all staff on the use of social media tools when acting independently or as a representative of the CCG and give them the confidence to engage effectively and appropriately.
- Ensure that the organisation's reputation is not brought into disrepute and that it is not exposed to legal risk as a result of comments posted on social media by NHS CCG staff
- Ensure that internet users are able to distinguish official corporate NHS Shropshire, Telford and Wrekin CCG information from the personal opinion of staff.

3. Scope

This Policy applies to all members of staff and those the CCG has legal responsibility for e.g. agency staff and relates to equipment provided by the CCG to allow you to carry out your role and your personal equipment.

This document is not intended as a social media strategy or guidance on how to use personal social media tools and platforms, guidance may be sought for assessing the value of using social media tools and platforms for each individual or business area if required via the CCG communication team.

4. Responsibilities

This policy and related procedures have been written and agreed through a partnership of managers, Trade Union representatives and Human Resources.

4.1 Responsibility of the CCG

The responsibility for the provision of an agreed Social Media and Digital Content Policy lies with the Director of Corporate Affairs.

The CCG holds a responsibility to inform all staff and users of social media tools and platforms of their responsibilities in relation to the use of social media tool and platforms. Specifically to posts made through personal accounts that are public and may breach organisational policy if they bring the organisation into disrepute and any actions the CCG may take as a result of such activity.

4.2 Responsibility of Human Resources

To provide advice and support to managers in relation to the application of this policy.

To ensure that the policy is applied fairly, equitably and consistently throughout the CCG.

4.3 Responsibility of Managers

It is the responsibility of all managers employed within the CCG 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 ensure that they are aware of the general standards and requirements of this policy and have to manage and engage in social media activity in the appropriate manner as outlined in this policy.

Employees are responsible for their own actions on social media and must comply fully with this policy, and their professional codes of conduct at all times. Cases of inappropriate, unacceptable and/or offensive content shall be investigated, and appropriate disciplinary action taken, in accordance with the Disciplinary Policy.

Employees have a responsibility to familiarise themselves with this policy and the general standards set within. There will be no justification for not having an awareness of this policy in times of inappropriate, unacceptable and/or offensive content being posted.

5. Definitions

5.1 Social Media

Social media is a computer-based technology that facilitates the sharing of ideas, thoughts, Photographic images 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 Social Media and 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, Twitter, Instagram and LinkedIn or any other application downloaded or used

5.3 Digital Content

Digital content can include news, information, photographic images, blogs, vlogs and entertainment distributed over the Internet and is accessed digitally by users.

5.4 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 examples of the most popular IM services.

This policy covers all forms of social, digital and messaging formats referred to as 'social media'. The above examples are not an exhaustive list and should be accepted as including other formats as technology evolves.

6. Principles

6.1 Participating in on-line activities

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 CCG wishes to embrace it as a demonstrable element of our commitment to a culture of openness and to empower staff to interact online in a way that is credible, consistent, transparent and relevant and appropriate. Staff are reminded that they will be seen as representing the CCG or wider NHS when posting personal comments on social media

We recognise that 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, or appropriate to make that distinction. For example, there is a tendency for people to maintain just one Twitter account, which is used to post a mixture of business related and personal content.

However, posts made through personal accounts that are public and can be seen may breach organisational policy if they bring the organisation into disrepute. This includes situations when you could be identifiable as a CCG employee whilst using social networking tools or occasions when you may be commenting on CCG related matters in a public forum.

Staff should use their own discretion and common sense when engaging in online communication to ensure they are acting appropriately at all times.

6.2 Best Practice

The following guidance gives some general rules and best practices which staff members are expected to abide by at all times:

- The same principles and guidelines that apply to staff activities in general also apply to online activities. This includes forms of online publishing and discussion, including blogs, images and file-sharing, user-generated video and audio, virtual worlds and social networks.

- Employees are personally responsible for the content they publish on any other form of user-generated media. Be mindful that items or posts published may be public for a long time. When online, the same principles and standards apply that would when

communicating in other formats with people you do not know.

- If acting on behalf of the CCG in an official capacity Identify yourself by giving your name and, where relevant, role at the CCG especially if you are discussing CCG related matters. If you are NOT acting in an official capacity, you must make it clear that you are speaking for yourself and not on behalf of the CCG and do not use the organisation's logo on personal web pages or social media accounts. Write in the first person.

- 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 CCG that could be perceived by anyone else to have a connection to the work you do or subjects associated with the CCG, it is suggested you display the following disclaimer:

  "My postings on this site reflect my personal views and do not necessarily represent the positions, strategies or opinions of NHS Insert name CCG"

- At all times employees must respect, consider and apply copyright, fair use, data protection, defamation, libel and financial disclosure laws by not revealing or disclosing confidential information of any kind but in particular about patients, staff, or the organisation.

- Social media should not be used to attack, cause distress or deliberately offend or abuse others.

- Be *appropriate* and non-judgemental of others.

- Do not provide or divulge confidential or other proprietary information on external websites.
- Do not publish or report on conversations that are private and confidential or internal to the CCG.

- Do not cite or reference partners or suppliers unless explicit consent to do so has been obtained.

- 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 or would breach code of conduct rules.

- Show appropriate and professional consideration for others' privacy or for topics that may be considered inflammatory, such as politics or religion

- Be aware of your association with the CCG when using social media. If you identify yourself, or are identifiable, as an employee of the CCG, ensure 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 NHSmail email address

- If you are asked to participate in a social network for commercial or personal gain, this could constitute a conflict of interest. Online social networking activity for commercial gain, that would conflict with the function of the CCG, you are required to declare the conflict and seek guidance from your line manager

- If someone from the media contacts you about posts you have made that relate to the functions of the CCG, you must notify and seek advice from the Communications and Engagement Team and also inform your line manager.

- Social media should not be used to air disputes or grievances with colleagues or the CCG, employees are required to raise any concerns through the proper channels. Employees can obtain advice and support from their line manager and/or HR Team

- Do not use social media to raise concerns sometimes described as 'whistleblowing'. All concerns should be raised through the appropriate channels. All staff should be aware that the Public Interest Disclosure Act 1998 which gives legal protection to employees who wish to raise any concerns.

7. 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 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.

7.1 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 CCG 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 attack 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, and date of birth, telephone contact numbers, and interests so ensuring that security settings are appropriate is important.

- Legal liabilities from defamatory postings by staff. When a person registers with a website they typically have to 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 toward 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:

- Do not 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 T&Cs of that site.

- Do not accept 'friend' requests from anyone you suspect to be underage.

- Avoid collecting, and do not 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 required for your job. If this is required for your job, then all appropriate CCG protocols should be followed.

- 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 or publish images of children, young people or adults - photographs and videos can and may be used to identify them to people who wish to groom them for abuse.

- Consider using models, stock photography or illustrations where appropriate

- 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 current 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.

7.2 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:

- 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 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 whilst using social media while acting on behalf of the CCG, that threatens to become antagonistic you should politely disengage and seek advice from your line manager or the Communications and Engagement or Human Resources Teams.

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 CCG 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 CCG 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

7.3 Reporting Safeguarding Concerns

Any content or online activity which raises a safeguarding concern must be reported to the CCG 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 CCG Safeguarding Policy.

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.

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 have concerns about or suspect a colleague is using the internet or social media in a way that raises safeguarding concerns including accessing concerning sites if concerns of 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 Team 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 the Human Resources Team. 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.

8. References and Endorsements

For social networking sites such as LinkedIn where personal and professional references are the focus, if you are representing yourself as a CCG 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 CCG employees, contractors, providers and contingent workers provided:

- the statements made and information provided in the reference are factually accurate; and
- you include the 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 Shropshire, Telford and Wrekin CCG."

9. 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 a CCG 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 CCG, 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 CCG you must refer the matter to the Communications and Engagement Team.

10. Representing NHS Shropshire, Telford and Wrekin CCG Online in an Official Capacity

Whilst we encourage individual members of staff to use social media to reflect positively on the work of the CCG, 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 Communications and Engagement Team to do so, you must not engage in social media activity that seeks to represent the official views of the CCG.

10.1 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 a CCG presence on a social media site you must discuss your proposal with the Communications and Engagement Team in the first instance, to ensure that it is appropriate and in-line with the organisation's social media strategy. 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.

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 strategy for a programme or business area and undergo appropriate stakeholder consultation and governance before being implemented i.e., approved by the Communication and Engagement Team 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 Communications and Engagement Team who will use the following acceptance criteria. Social media accounts must:

- Have clearly defined objectives and KPIs, defined 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 1 month or more
Frequency	less than one tweet/post a week over a 2 month period
Interest	account has been active for 6 months or more but has less than 100 followers
Relevance	programme or project has closed
Governance	account not managed through corporate process

Please note, requests for information made via Twitter 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.

10.2 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 a CCG employee, please discuss your proposal with the Communications and Engagement Team 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 Communications and Engagement Team.

11. 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's important that CCG all public video content is placed on the CCG YouTube channel from where it can be shared, embedded on CCG 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, CCG content it 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 the Information Governance or Communications and Engagement Team.

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 Communications and Engagement Team.

12. On-line surveys, Slides and Presentations

If you wish to run an externally facing online survey, please contact the Communications and Engagement Team. It is important that the CCG 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.

12.1 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 CCG projects and documents, you must carefully consider security. In the majority of 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 commercially sensitive material reaching the public domain.

All information stored on internal or external websites must be held in accordance with the CCG Information Governance Policies.

If you have a requirement to set up a new collaboration, community of practice or consultation space, you must contact the Communications and Engagement and Information Governance Teams to discuss your needs in the first instance. They will be able to advise on the tools available which fit your requirements.

13. Non compliance

This policy apply 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 the policy above and ask yourself why that is. If you are in doubt or in need of further guidance, please contact the Communications and Engagement Team to discuss.

Non-compliance with this policy may lead to disciplinary action in accordance with the CCG 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.

14. Monitoring

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. Equality Impact Assessment

The CCG aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, patients and the public. The purpose of the assessment is to improve service delivery by minimising and if possible, removing any disproportionate adverse impact on employees, patients and the public on the grounds of their protected characteristics as defined in the Equality Act (2010).

The Equality Impact Assessment has been completed to support this policy