Humber Teaching
NHS Foundation Trust

Social Media and Website Policy
(C-004)

Version Number:	1.5
Author (name & job title)	Rachel Kirby, Head of Marketing & Communications
Executive Lead (name & job title):	Michele Moran, Chief Executive
Name of approving body:	Executive Management Team (EMT)
Date full policy approved:	25 June 2024
Date Ratified at Trust Board:	31 July 2024
Next Full Review date:	June 2027

Date approved by Lead Director:	
Date EMT as approving body notified for information:	

Policies should be accessed via the Trust intranet to ensure the current version is used

Contents

1. Executive Summary

This policy sets out the roles, responsibilities and procedure for managing Trust social media accounts and provides guidance on social media/networking on the internet and the external use of other tools such as blogs and interactive news websites. It seeks to give direction to staff in the use of these tools and support them to utilise the platforms for the benefit of their services and in pursuit of their goals. This policy aims to ensure the Trust is proactive in managing its reputation online and that it has a consistent approach to its how it manages service social media accounts and other digital spaces.

2. Introduction and Aims

This document provides guidance to staff on social media/networking when using them in a professional and personal capacity. It outlines our approach to running an office Trust account and dealing with online comments on social networks, blogs, forums and news websites.

It also outlines the Trust's approach to using websites to ensure a consistent approach to promoting the services that we provide ensuring that all patients have access to accurate, secure and up to date information throughout their treatment.

The purpose of this policy is to help protect the interests of the Trust and its employees. It advises of the consequences of behaviour on social media or any content posted online, whether acting in a personal or professional capacity.

This aims of this document are to:

- Provide guidance to employees on the use of social media to allow employees to feel enabled to use these online platforms to support strategic and operational goals.
- Ensure the Trust's reputation is not brought into disrepute and that the Trust is not exposed to any legal risk.
- Ensure that members of the public are able to distinguish between corporate information from the Trust and the personal opinion of an employee.
- Provide guidance to the commissioning and management of Trust service websites to ensure continuity of provision, appropriate use of technology, value for money and safety and security.

Social media is constantly developing and this policy will therefore be continually updated in line with changes.

This document is not a guide to using social media for your service. Each individual or service should consider the value of using these tools and the time required to make them a useful and beneficial communications tool and follow this policy if they choose to do so

3. Social Media

3.1. Trust Official Accounts

Social media management is the process of creating, scheduling, analysing, and engaging with content posted on social media platforms, like Facebook, Instagram, and Twitter. The role of the team is to respond to comments and develop strategy on how to achieve long term marketing and communications goals by publishing original content.

The Trust Marketing and Communications team are the social media managers for the Trust corporate accounts. These include but are not limited to:

- Facebook
- Twitter
- Instagram
- Linked In

Our audience includes the general public in the areas we operate, patients, carers, stakeholders, partners, commissioners and the media operating in both a personal and professional capacity. Customers interact with brands via Twitter, Facebook, Instagram, LinkedIn and more, and they expect fast and professional responses that solve their problem or query. Therefore engaging with our audience through social media is more important than ever and is a key role of the Marketing and Communications Team.

Social media allows the Trust to connect and engage directly with thousands of people and organisations. It allows us to share important information from the Trust and the wider NHS/health partners, create awareness about events and campaigns and engage and listen to understand and take on board the viewpoints of our stakeholders.

The Marketing and Communications Team manages social media between 9am-5pm, Monday-Friday. During this time they will respond to messages, posts and comments as soon as possible. Messages, posts and comments made on a weekday evening will be responded to the next morning; those shared at weekends and on bank holidays will be responded to by the next working day. An automated response on Facebook makes it clear when the platform is monitored and how to seek urgent mental health help. From time to time social media platforms may be unavailable and we accept no responsibility for lack of service due to social media service downtime.

By sharing other social media users' content, our organisation does not endorse the information or others' views of that organisation or individual. We aim to share information which adds to any debate or topic we are involved in.

3.2. Types of Social Media Account

Some services choose to operate official Twitter accounts for their service and some individual members of staff choose to use social media in their role within the Trust whether that's on a separate account or as part of their personal social media account. The following guidance must be followed for operating these accounts. Any deviation from this guidance will result in the removal of the account as a Trust communications tool.

Please note we will not approve other service accounts other than a Twitter account.

3.2.1. Service Twitter Accounts

- Applications for service Twitter accounts can be made via the Marketing and Communications team by requesting the 'Twitter Account Proposal' form which can be found on the Intranet. This is important to ensure that a record of the account name and password. Not having this information means that should a member of staff move on or be subject to disciplinary action there would be no way to control content from the account putting the Trust at risk
- Service Facebook sites are not permitted
- A designated service social media manager (SMM) must be named for any service Twitter account. It is the responsibility of this person to ensure that the account is populated with frequent and relevant content that will support the service to communicate with its designated target audience. Most studies agree that once per day is optimal but no less than three

times per week is recommended to ensure that an account is useful. Accounts that are found to be inactive will be requested to be removed or temporarily deleted until such time as they can be regularly populated with content.

- Accounts may be deleted for the following reasons:
  - Inactive – e.g. no original posts made for one month or more
  - Frequency – e.g. less than one post a week over a two month period
  - Interest – e.g. an account has been active for six months or more or more but has less than 100 followers
  - Relevance – programme or project has closed
  - Governance – the account has not gone through the correct procedure
- The Marketing and Communications team must be provided with accurate login information at all times.
- If the designated social media manager resigns from their position their role as SMM should be replaced immediately on receipt of resignation and the new SMM shared with the Marketing and Communications Team.
- Content posted from Trust accounts should be credible, consistent, transparent and relevant.
- Ensure you have permission for all images/video content shared on your account and that you have used the Trust consent forms available on the Intranet.
- No service social media accounts or websites should be listed on printed materials. The Marketing and Communications Team run the official Trust accounts which should always be linked from Trust materials
- If a member of the media contacts you about any posts on your service account you must contact the Marketing and Communications Team in line with the Trust Media Policy.
- It must be clear when the account is monitored e.g. Monday – Friday 9am – 5pm
- When responding to comments you must follow the flowchart for managing online comments (see Appendix 1)
- The process for handling complaints or negative comments must be followed as per section 3.5 to ensure a consistent approach for dealing with comments.
- The use of social networking sites and the internet are useful tools to engage and share information with children, young people and adults. However they also have the potential, if used inappropriately to pose a potential safeguarding risk.

  Potential safeguarding risks could include (not exhaustive):
  - Online bullying
  - Grooming/ Exploitation
  - Introduction into terrorist activities
  - Encouragement of risk taking behaviours such as self-harm.

  Staff should be mindful when using social media/ networking to:
  - Keep their privacy settings up to date
  - Not to share personal information about themselves including work details
  - To consider separate accounts for personal and work related activity
  - Not to engage in a way that may be seen as trying to develop a relationship with a child, young person or adult at risk
  - Maintain professional boundaries
  - Not to share information about people without their consent

- To not post or comment on any content that may be deemed offensive or inappropriate
- To ‘Think before you post’.

If any staff member has concerns regarding a potential safeguarding issue, they should contact the Safeguarding Team for advice and support and follow the Humber Teaching NHS Foundation Trust Safeguarding Adults and Children Policy’s and also report concerns to the designated Local Authority Safeguarding Teams.

If a child, young person or adult at risk is in immediate danger, staff should contact the Police using 999 to report the immediate concern.

3.2.2. Professional discussion groups

Staff members requiring access to online professional discussion groups in a work capacity must submit their request by email to the IT Service Desk. The request must detail the name of the online site/service, the business need for the access and confirmation from their line manager supporting the request. The request must be authorised by a senior informatics manager. IT Services will verify that the site is safe and appropriate for business use and if necessary request further information for audit purposes from the user or their supporting manager.

Personal/business sensitive data must not be shared in the discussion group. All posts to the discussion group must comply with this procedure.

Granting access to facilities such as cloud storage (e.g. Dropbox) may also give access to other facilities such as web mail (e.g. Gmail, Outlook.com) and vice versa. If it is necessary for business purposes, web mail may be used to receive non-confidential and non-business sensitive information. However, staff must use Trust email accounts for any emails sent in relation to Trust business.

3.2.3. Personal Accounts

Humber Teaching NHS Foundation Trust understands the value social media platforms can bring to its staff. Please remember that whenever or however you may be using these sites, as Trust employees, staff are expected to maintain standards of professionalism and will be held to account in accordance with the Trust's Disciplinary Policy and Procedure for any inflammatory, derogatory, slanderous or abusive statements. Just as we don’t tolerate bullying in real life, we will not tolerate it online.

- Posts through personal accounts that are public can be seen to breach organisations policy if they bring the Trust into disrepute. This includes situations where you could be identifiable as an employee of Humber Teaching NHS Foundation Trust.
- It is important that staff members do not give the impression that their comments represent the views of the Trust unless specifically authorised by the Marketing and Communications team.
- Staff are advised to familiarise themselves with the relevant guidance for their profession where appropriate. Employees are reminded that professional codes of conduct must be adhered to in respect of social media. Examples include, but are not limited to, Nursing and Midwifery Council: Social Networking Guidance, Health and Care Professions Council: Standards of Conduct, Performance and Ethics and Guidance on the Use of Social Media and General Medical Council: Doctor’s use of social media.
- The NHS Employers website (www.nhsemployers.org) also shares helpful guidance on using social media.
- If publishing content to any website that could be perceived to be a connection to the work you do or the subjects associated with Humber Teaching NHS Foundation Trust you must displace a disclaimer such as:

"My posts on this site reflect my personal views and don't necessarily represent the positions, strategies or opinions of Humber Teaching NHS Foundation Trust"

- Employees must not use the Trust's logo or name on social media accounts to give the impression that they are communicating on behalf of the Trust
- If the media contacts you about any posts you have made online you must contact the Marketing and Communications Team in line with the Media Policy.
- Users must be mindful of Purdah (the period shortly before an election or referendum) guidance during the elections period. NHS employees are free to undertake political activism in a personal capacity but should not involve their organisation or create the impression of their organisation's involvement. This also includes comments and posts placed online or on social media.
- In the unusual event of an emergency or incident response (such as a fire or riot/protest) do not use your own personal social media accounts to provide public updates. Any official updates must come directly from the Trust's social media channels and be managed by the Communications team to negate any confusion.

3.3. Accessing Social Media

If you feel that using social media sites has a significant benefit to your role in the Trust, you must discuss this with your line manager who will agree how you should be using these sites during work time. Usage must be in line with the Electronic Communications and Internet Acceptable Use Procedure. If you have any concerns, please seek clarification with your line manager or the Marketing and Communications team.

A request to access the sites should be made via the IT Helpdesk.

3.4. Inappropriate Use of Social Media

When using social media in a personal or work capacity, employees must not:

- Identify the Trust as their employer on social network sites used for a personal use. This does not apply to professional networking sites such as LinkedIn and professional discussion groups authorised in 3.2.2.
- Use social networking sites in any way which is unlawful
- Use social networking sites to pursue personal relationships with patients
- Steal personal information or use someone else's identity
- Accept payment of gifts in kind in return for promotion on a blog or social network which could constitute a conflict of interest.

- Post comments on social network sites, discussion forums, blogs etc. which contain:
  - Personal identifiable information (patient and staff data)
  - Inappropriate comments or personal criticism of colleagues or patients
  - Names of other staff without their permission
  - Statements by or on behalf of the organisation
  - Information about work related issues
  - Information or language that could be considered bullying, intimidating, harassment or discriminatory against any individual
  - Criticisms of the organisation or would bring the organisation into disrepute
  - Defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material.
  - Material that is designed to annoy, harass, bully, inconvenience or cause needless anxiety to other people, as detailed in the Bullying and Harassment Policy.
  - Pornographic images, data, or other material, or any data capable of

being resolved into obscene or indecent images or material.
- Any copyrighted material in a manner that violates that copyright.
- Any material for the purpose of corrupting or destroying the data of other users.
- Junk mail or spam.

If an employee has concerns regarding any content they have seen themselves on social media they must inform their line manager and/or the HR Team and the Marketing and Communications Team.

If a member of staff feels they have been the victim of a social media attack from a patient or a member of the public in connection with their employment at the Trust, they should contact their line manager, HR and, or their Local Security Management Specialist (LSMS) as soon as possible. This should be reported on Datix and any available evidence should be retained, e.g. copies of messages or screen shots.

Managing Comments, Filming and Photography of Staff on Social Media Occasionally members of the public may choose to use social media channels to raise concerns about a service they or a member of their family or friend has used or attempted to access.

The management and response to the concern raised is dependent on the nature and profile of the concern, however the below information and the flowchart in Appendix 1 of this policy provide an overview of the principles followed.

The Marketing and Communications Team manage social media between 9am-5pm, Monday-Friday. During this time comments will be responded as soon as possible. Concerns shared on a weekday evening will be responded to the next morning, while concerns shared at weekends and on bank holidays will be responded to the next working day. It is clear on our accounts when they are monitored.
When a concern is shared via social media the individual receives a response from a member of the Marketing and Communications Team, usually apologising for their experience and providing them with the contact details for the Complaints and Patient Advice Liaison Service. It is the individual's choice as to whether or not they decide to contact the Complaints and PALS department and formally raise their concern or complaint. On occasions the individual may have already made contact with The Complaints and PALS department on other occasions they may choose not to escalate their concern further. Employees must not respond to individuals on behalf of the Trust. This could lead to confusion for the individual concerned.

On occasion comments may be posted which indicate a person may be at risk to themselves or others. If these comments are seen by a member of Trust staff they must contact a member of the Marketing and Communications Team. The Marketing and Communications team will liaise with clinical staff for advice and support to respond to the comment.

If comments are seen outside of the time that accounts are monitored (Monday-Friday 9am-5pm) then the Manager on Call should be contacted on 01482 301700. They will provide advice on responding to the comments, where appropriate liaising with clinical staff for advice and support.

If staff or patients are filmed or photographed on Trust premises without consent and posted on social media, please refer to Media/Social Media Process Model PO-SPTG-BTB-1723-D02.00 on the Trust Intranet for advice.

You can also refer to this model if comments or posts are made attacking a member of staff.

Posting photographs, videos or other content of any staff member or patient, service user or carer without consent, may breach identity and consequentially cause safeguarding risks.

Please note, the Communications Team does not have the power to remove comments, photographs or videos from social media channels – this rests with the social media platforms.

However, they can advise on the best course of action for limiting impact and reporting to the social media channel(s) in question with a view to removal.

Staff are reminded that actions online can be in breach of the harassment/IT/equality/safeguarding policies and any online breaches of these policies or actions that may be viewed as harming the Trust's reputation may be treated as conduct issues in accordance with the Trust's Disciplinary Policy and may result in dismissal.

4. Websites

4.1. Trust Website

The Marketing and Communications team manage the official Trust website humber.nhs.uk.

It is in the best interests of our patients and service users that all information on our website is as up to date and accurate as possible. It is the responsibility of the Service Manager to ensure that the Marketing and Communications team are made aware of any changes to the service as soon as possible to update the relevant pages.

Requests to change website content should be made to the Marketing and Communications team and the changes clearly communicated by email – requests by telephone are not accepted. These changes are usually actioned within five working days. If changes are urgent or require special attention this should be marked on your email or followed up by telephone.

Requests for new page/website sections should be made to the Marketing and Communications Manager. It is at the discretion of the Chief Executive with the advice of the Marketing and Communications Manager if pages are created and what information is present on the navigation bar and on the homepage.

4.2. Service Websites

The Trust website is the central information resource for service information. Services can request new sections, pages or changes to current pages by contact the Marketing and Communications team at HNF-TR.communications@nhs.net

There may be occasion where a service website is appropriate due to the audience or technical requirements. These websites are an exception to the usual procedure of services including information within the central Trust website.

If a service website is required a paper outlining the following must be submitted and approved by the Digital Delivery Group.

- Reason service required a standalone web site
- Evidence of patient/service user/carer engagement
- Supplier/web hosting providers details and any accreditation they hold
- Ensure appropriate consideration has been given to ensure that the platform meets the trusts cyber security, patient safety and information governance requirements.

On approval but prior to signing any supplier contracts the following must be completed/agreed.

- Liaise with the Communications, Informatics and Information Governance Teams to ensure the appropriate procedures are followed and the site is safe to use.

- Contact the IT team to request an official *.nhs.uk website address, ideally relating to Humber as a trust, for example servicename.humber.nhs.uk
- Contact the Communications Team to discuss web hosting requirements. If alternative web hosting is required, services will need to provide technical details of the hosting platform. Cyber security procedures to must reviewed for compliance with current NHS national requirements and suppliers must provide details of their cyber security procedures to give assurance that they can maintain a secure web hosting platform to the standards of Cyber Essentials Plus accreditation
- The supplier must agree to provide the trust with an annual penetration and/or similar web site security test to ensure compliance.
- Details of how the site will be managed including two members of staff who will be responsible for ensuring content is up to date at all times. A written record of the process must be created and shared with the IT and Communications team including details of regular content review meetings including attendees required.
- All websites must have a content management system allowing the service to edit and update the site content. The Communications Team must be provided with login information for the CMS.

Prior to go live the following must be completed.

- A completed Data Protection Impact Assessment (DPIA) approved by the trusts Information Governance Group.
- The supplier/web hosting provider must provide details of their cyber security procedures to give assurance that they can maintain a secure web hosting platform to the standards of Cyber Essentials Plus accreditation.

4.3. GP Websites

Our GP surgeries operate websites to provide information about services and offer access to online services such as online consultations.

Practice Managers have responsibility for ensure these websites are up to date with relevant and accurate information.

The Marketing and Communications team can access these sites to post updates and can support if they require specialist support e.g. images or changes to navigation.

4.4. NHS.uk

The Marketing and Communications Team are also responsible for updating all Trust information on the NHS.uk website. This site is an important source of objective and trustworthy information and guidance on all aspects of health and healthcare. It is crucial that Trust information is up to date to ensure that we are providing the best service to our patients, their carers, families and loved ones.

It is the responsibility of the Service Manger to ensure that the Marketing and Communications team are made aware of any changes to the service as soon as possible to update the relevant pages.

4.5. Cookies

All Trust websites must provide users with the option to accept or change cookie settings. The website must contain information about what cookies are used and why, being clear which are essential for the operation of the website and which are optional. It must also include information on how to block/restrict cookies.

5. Other Relevant Policies

- Media Policy
- Safeguarding Policies
- Disciplinary Policy and Procedure
- Freedom to Speak up Procedure
- Information Governance Policy
- Information Security and Risk Policy

6. Non-compliance

Humber Teaching NHS Foundation Trust policies apply to all forms of communication, whether verbal, printed or online. Staff should remember that they are ultimately responsible for what they publish online and 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 what it is. If in doubt and you need further guidance, please contact the Marketing and Communications team for advice.

Non-compliance with the policies associated with this guidance may lead to disciplinary action in accordance with the Humber Teaching NHS Foundation Trust Disciplinary Policy.

Staff are also reminded that actions online can be in breach of the harassment/IT/equality policies and any online breaches of these policies or actions that may be viewed as harming the Trust's reputation may be treated as conduct issues in accordance with the Trust's Disciplinary Policy and may result in dismissal.

The process for staff raising concerns at work/whistleblowing is set out in the Freedom to Speak Up policy. In line with that policy, social media should not be used to raise such concerns.

7. Accountability and responsibilities

Overall accountability for this document lies with the Chief Executive.

Overall responsibility for the social media and attributed content policy lies with the Marketing and Communications Manager, who has delegated responsibility for managing the development and implementation of social media and attributed content.

Staff can contact the Marketing and Communications team for advice and guidance on all elements of the policy.

All staff are responsible for adhering to this policy when using social media platforms and for following the guidelines when setting up a social media account on behalf of a Trust service.

All managers for non-clinical services must ensure that employees within their area are aware of this document; able to implement the document and that any superseded documents are destroyed.

The Information Technology Team works alongside the Marketing and Communications team to support in the management of Trust websites e.g. creating .nhs.uk domain.

8. Monitoring and review

The Marketing and Communications team monitor performance indicators (e.g. number of followers) and captures feedback via the corporate social media channels to support patient experience activity across the Trust.

This policy and guidance will be reviewed in accordance with the following on an ‘as and when required’ basis: legislative changes, good practice guidance, case law, significant incidents reported, new vulnerabilities and changes to organisational infrastructure. If this results in any changes, the document will be amended. Otherwise the review date will provide the timeframe for review.

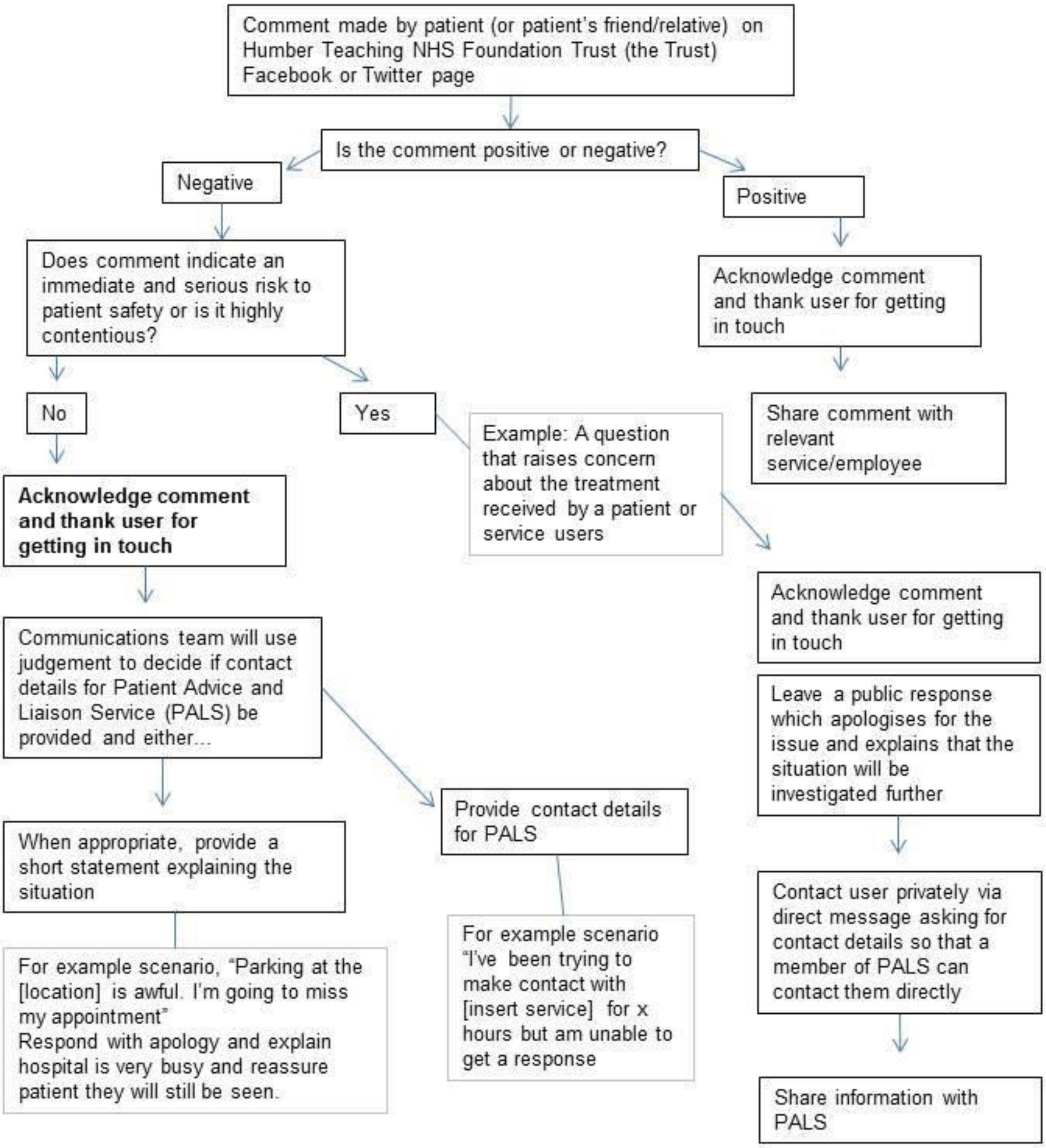
9. References

Nursing and Midwifery Council: Social Networking Guidance
Health and Care Professions Council: Guidance on the use of social media. General Medical Council: Doctor’s use of social media.

Appendix 1 – Flow chart for managing social media comments

Flow Chart for Managing Social Media Comments

Below is a flow chart for managing concerns raised through social media.



Comment made by patient (or patient's friend/relative) on Humber Teaching NHS Foundation Trust (the Trust) Facebook or Twitter page
Is the comment positive or negative?
Negative
Positive
Does comment indicate an immediate and serious risk to patient safety or is it highly contentious?
Acknowledge comment and thank user for getting in touch
No
Yes
Example: A question that raises concern about the treatment received by a patient or service users
Share comment with relevant service/employee
Acknowledge comment and thank user for getting in touch
Acknowledge comment and thank user for getting in touch
Communications team will use judgement to decide if contact details for Patient Advice and Liaison Service (PALS) be provided and either...
Leave a public response which apologises for the issue and explains that the situation will be investigated further
Provide contact details for PALS
When appropriate, provide a short statement explaining the situation
Contact user privately via direct message asking for contact details so that a member of PALS can contact them directly
For example scenario "I've been trying to make contact with [insert service] for x hours but am unable to get a response
For example scenario, "Parking at the [location] is awful. I'm going to miss my appointment" Respond with apology and explain hospital is very busy and reassure patient they will still be seen.
Share information with PALS

Appendix 2 - Document Control Sheet

Document Type and Title:	Policy		
Document Purpose:	This policy sets out the roles, responsibilities and procedure for managing Trust social media accounts and provides guidance on social media/networking on the internet and the external use of other tools such as blogs and interactive news websites. It seeks to give direction to staff in the use of these tools and support them to utilise the platforms for the benefit of their services and in pursuit of their goals. This policy aims to ensure the Trust is proactive in managing its reputation online and that it has a consistent approach to its how it manages service social media accounts and other digital spaces.		
Consultation/ Peer Review	Date	Group / Individual	
list in right hand columns consultation groups and dates	Jan-Feb 2020	IT, IG, Legal, Complaints & PALS, Safeguarding, HR	
	March 2020	EMT	
	Dec-Feb 2023	IT, Digital	
Approving Body:	EMT	Date of Approval:	25 June 2024
NB All new policies and policies subject to significant amendments require approval at EMT and Board ratification.		*(see document change history below for minor amendments and dates)*	
Ratified at:	Trust Board	Date of Ratification:	31 July 2024
Training Needs Analysis: *(please indicate training required and the timescale for providing assurance to EMT as the approving body that this has been delivered)*	There are no training requirements for this document	Financial Resource Impact:	There are no financial resource impacts
Equality Impact Assessment undertaken?	Yes [√]	No [ ]	N/A [ ]
	If N/A, state rationale:		
Publication and Dissemination	Intranet [√]	Internet [ ]	Staff Email [√]
Master version held by:	Policy Management Team [√]	Author to send final document to HNF-TR.PolicyManagement@nhs.net	
Implementation:	*Describe implementation plans below - to be delivered by the author:* Implementation will consist of: The policy will be placed on Trust intranet as a resource and the update proactively shared with all staff to ensure there is awareness.		
Monitoring and Compliance:	Monitoring and compliance of the policy will be evidenced through the process of consultation, approval and ratification of policies		

Document Change History:

Version Number / Name of procedural document this supersedes	*Type of Change i.e. Review / Legislation*	*Date*	*Details of Change and approving group or Executive Lead (if done outside of the formal revision process)*
1.0	*New Policy*	*Jan-2020*	*New policy drafted*
1.1	*Minor review*	*Feb-2020*	*Minor revisions pre approval*
1.2	*Minor review*	*March-2020*	*Minor revisions and approval at EMT 4 March 2020 with ratification at Broad 25 March 2020* *Year review date as initial policy approval*
1.3	*Minor*	*8/11/21*	*Bullet point added to end of section 3.2 re use of personal media*
1.3.1	*N/A*	*June-22*	*EIA added to document and republished on intranet* *No changes to policy content. (Policy Management Team)*
1.4	*Review*	*Feb-23*	*Minor changes* *Changes to service website section (4.2)* *Approved at EMT (22-Feb-23)*
1.5	*Review*	*Jun-24*	*Reviewed with minor amends. Approved at EMT (25 June 2024) and ratified at Trust Board (31 July 2024).*

Appendix 3 - Equality Impact Assessment (EIA)

For strategies, policies, procedures, processes, guidelines, protocols, tenders, services

1. **Document or Process or Service Name:** Social Media and Website Policy
2. **EIA Reviewer (name, job title, base and contact details):** Rachel Kirby, Head of Marketing & Communications
3. **Is it a Policy, Strategy, Procedure, Process, Tender, Service or Other?** Policy

Main Aims of the Document, Process or Service *To set out the requirements that must be met for approval, ratification and dissemination of all Humber Teaching FT policies*.
Please indicate in the table that follows whether the document or process has the potential to impact adversely, intentionally or unwittingly on the equality target groups contained in the pro forma

Equality Target Group . Age . Disability . Sex . Marriage/Civil Partnership . Pregnancy/Maternity . Race . Religion/Belief . Sexual Orientation . Gender re-assignment	Is the document or process likely to have a potential or actual differential impact with regards to the equality target groups listed? **Equality Impact Score** Low = Little or No evidence or concern (Green) Medium = some evidence or concern(Amber) High = significant evidence or concern (Red)	How have you arrived at the equality impact score? 1. who have you consulted with 2. what have they said 3. what information or data have you used 4. where are the gaps in your analysis 5. how will your document/process or service promote equality and diversity good practice

Equality Target Group	**Definitions**	**Equality Impact Score**	**Evidence to support Equality Impact Score**
Age	Including specific ages and age groups: Older people, Young people, Children, Early years	**Low**	
Disability	Where the impairment has a substantial and long-term adverse effect on the ability of the person to carry out their day to day activities: Sensory, Physical, Learning, Mental Health (and including cancer, HIV, multiple sclerosis)	**Low**	
Sex	Men/Male, Women/Female	**Low**	
Married/Civil Partnership		**Low**	
Pregnancy/ Maternity		**Low**	
Race	Colour, Nationality, Ethnic/national origins	**Low**	
Religion or Belief	All Religions Including lack of religion or belief and where belief includes any religious or philosophical belief	**Low**	
Sexual Orientation	Lesbian, Gay Men, Bisexual	**Low**	
Gender re-assignment	Where people are proposing to undergo, or have undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attribute of sex	**Low**	

Summary

Please describe the main points/actions arising from your assessment that supports your decision above			
EIA Reviewer	Rachel Kirby, Head of Marketing and Communications		
Date completed;	25 June 2024	Signature	*Rachel Kirby*