

Document level: Trustwide
Code: COR072
Issue number: 3

Social Media Policy

Ratified Date	11/07/2022	Version No	3	Expiry Date <i>Max. 3 years edfrom ratification</i>	11/07/2025
Reason(s) for change (if not new at this edition)					
Reviewed and updated – previously known as COM006					

Chief Officer	Chief Strategy Officer
Lead Author	Digital Communications Manager (Becky Taylor-Rossall)

Document Type:	Policy	Reference No:	COR072	Document level:	Trust wide
Document purpose:	The purpose of this policy is to provide guidance for all employees about the appropriate use of social media.				
Applicable to	To all staff, volunteers, people working in and with services across the Trust.				

People/Groups Consulted:	Director of Communications and Engagement (Alexa Traynor) Digital Communications Manager (Becky Taylor-Rossall) Senior Corporate Support Officer (Sarah Harrison) Senior Workforce Business Partner HR (Angela Ogden) Staff side committee, Unison Branch Secretary, partnership lead, staff side chair person and AFC lead (Lee Morgan) Deputy Chief People Officer and Director of Organisational Development and Inclusion (Robert Cragg) Equality, Diversity and Inclusion Manager (Joanna Harrison)
Governance oversight group (if applicable)	Workforce & Education Sub-committee
Approval Group:	HR Policy Group/JNCC

Other documents to be read in conjunction	Code of Conduct for Employees Grievance Policy & Procedure Data Protection & Confidentiality Policy Disciplinary Policy Equality in Employment policy Freedom to Speak Up Policy Information Management and Technology Security Policy.
--	---

Version Control and Change Summary

Version	Date	Section	Author	Comments
1	Oct 2014			New Policy
2	Oct 2016			Reviewed and Updated
3	July 2022			Reviewed and Updated

Contents	Page No
Procedural Document Governance	1
1.0 Introduction and Purpose	3
2.0 Scope	4
3.0 Definitions	4
4.0 Duties	4
5.0 The Policy/Procedure	5
6.0 Monitoring	13
7.0 References (including applicable NICE publications)	14
8.0 Implementation Plan	14
Appendices	
Appendix 1	n/a
Appendix 2	n/a
Standard Appendices	
Appendix i. – Equality Impact Assessment	15

IMPORTANT

At all times use the Procedural Document Handbook to help you with your approach to reviewing an existing or producing a new policy or get in touch with policies@lscft.nhs.uk

1.0 Introduction and purpose

This policy sets out the standards and procedures that all staff within Lancashire and South Cumbria NHS Foundation Trust (LSCFT) must adhere to when using social media sites and associated tools.

Examples of Social Media sites and services include (but are not limited to):

- Popular social networks like Facebook and Twitter
- Professional social networks like LinkedIn
- Photograph and video-sharing social networks like Instagram and TikTok
- Sharing and discussion sites like Reddit
- Instant messaging applications such as WhatsApp

The Trust acknowledges that staff can improve their personal knowledge, skills and experience through relevant interactions with others outside the organisation. The purpose of this policy is not to deter employees from using social media sites nor to create or encourage any form of surveillance culture, but to ensure the operational effectiveness of the Trust and to help protect employees and prevent them from bringing the NHS and/or the Trust into disrepute either inadvertently or intentionally. This involves ensuring confidentiality and maintaining security in accordance with the Trust's policies, relevant privacy laws and good practice.

Where someone's association with the Trust can be identified and/or they are discussing work-related issues on social media, they must behave professionally and in a way that respects patients and colleagues confidentiality and is consistent with the Trust's values and policies, their individual responsibility as a Trust employee and the Trust Code of Conduct for employees, and with the relevant professional codes of conduct for healthcare professionals. (Council, 2012)

Employees who are found to breach the Trust's policy on Social Media may be managed in line with the Disciplinary Policy & Procedure and or any other appropriate policy and procedure.

The Trust's communications department has authority to speak on behalf of the Trust and is responsible for managing the Trust's official sites. Social media, like other communication tools, can potentially be used to improve the public's understanding of the Trust and its work, promote health, and engage with the general public.

It is the policy of the Trust that no one will be discriminated against on grounds of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation. The Trust will provide interpretation services or documentation in other media as requested and necessary to ensure natural justice and equality of access.

The principles outlined in this guidance will be applied to other kinds of online communication, such as personal websites and blogs, discussion boards and general content shared online, including text, photographs, images, video and audio files.

All clinical and medical staff may put their registration at risk if they act in any way that is unprofessional or unlawful on social media.

Further to this policy, staff should also refer to social media guidance issued by the relevant professional bodies e.g. Nursing and Midwifery Council, Health & Care Professions Council, General Medical Council and the British Medical Association for additional advice.

2.0 Scope

This policy applies to all staff employed by Lancashire and South Cumbria NHS Foundation Trust. It also applies to all people working in the Trust as volunteers and in any capacity paid or otherwise.

The policy applies to the use of social media within their role at Lancashire and South Cumbria NHS Foundation Trust and also that of any personal use whilst associated with the Trust.

3.0 Definitions

Social media describes web-based applications that allow people to create and exchange content. This includes but is not limited to blogs and microblogs (such as Twitter), internet forums (such as doctors.net), content communities (such as YouTube and Flickr), and social networking sites (such as Facebook and LinkedIn).

Personal use is defined as individuals using social media for recreational purposes outside of their working hours or during allocated break times on personal devices.

Professional use is defined as professionals using social media in their professional capacity. This includes but is not limited to opportunities for research, raising awareness of topical health issues, public engagement and the chance to establish a wider and more diverse professional network.

Trust use describes the Trust use of social media as part of a communication strategy. The communications department has authority to speak on behalf of the Trust and is responsible for managing the Trust's official sites.

4.0 Duties

All staff have a responsibility to:

- Use social media responsibly and to act in way that would not bring the NHS/Trust into disrepute.
- Only use social media for personal use outside of work or during allocated break times on their own personal devices. Staff may use social media for professional use during work hours.
- Maintain confidentiality by not using social media to discuss patients, staff or other confidential or personal information.
- Alert their Line Manager if there are any concerns regarding use of Social Media and/or Social Media posts.
- Staff must not take and/or upload photos that contain images of patients.
- Act professionally when using social media sites and not make comments that are likely to cause offence to staff, patients, public or the Trust.

The communication department has a responsibility to:

- Act respectfully towards patients, members of the public and Trust employees.
- Not reveal confidential or sensitive information about patients, staff or the Trust.
- If and once set up, update the channels on a regular basis and respond to users posts.
- Monitor and remove any content posted on Trust Social Media sites by other users that is considered offensive or derogatory.
- Immediately inform the Information Governance Department of Freedom of Information Requests received directly through social media.

Line Managers must:

- Ensure staff, who they are responsible for, are aware of and adhere to this policy.
- Ensure staff are updated in regard to any changes in this policy.
- Any incidents regarding Social Media are reported via the Trusts reporting system.

5.0 The Policy/Procedure

5.1 Use of Social Media

Staff must respect confidentiality when using social media and not discuss patients under any circumstances - to do so would be a breach of the Trust's Data Protection & Confidentiality Policy and may result in disciplinary action.

All staff are reminded that the disclosure of patient or staff personal data on social media may be considered a criminal offence and reported to the relevant enforcement body.

Nothing written by staff should comment on, or provide additional information about, cases already in the public eye – for example, any incident that has been reported in the media.

While individual pieces of information may not alone breach patient confidentiality, the sum of published information online could be sufficient to identify a patient. Staff should only share information about the Trust that is in the public domain i.e. Trust visiting times. Staff must not add derogatory comments on these issues, to do so may bring the service into disrepute. This could also impact on the staff member professionally and may affect their professional registration.

Example Scenario 1 – A doctor posted on Facebook “saw a patient today with [name of condition], it’s a really rare condition so I am interested to see if new trial drug works”.

This in itself seems unidentifiable; however, other members of staff or other people with knowledge of the patient may be able to identify the individual. This would be classed as a breach of Confidentiality and may be investigated and result in disciplinary action in line with the Trust's Disciplinary Policy.

Example Scenario 2 – a member of staff has a relative or friend who recently accessed our services and has positive feedback. The staff member posts in the Staff Facebook Group, “Thanks to all the staff, especially Vicky on the Orwell Ward at the Harbour for looking after my brother James last week”.

This would be a breach of patient confidentiality and could result in disciplinary action as per the policy.

Staff must not comment on, view, contact or search for patients via social media sites; action of this kind will be viewed as a breach of confidentiality (see note 1).

Note 1: This excludes where a staff member knows a patient personally through a method outside of the Trust, i.e. the staff member was friends with the individual prior to their contact with the hospital. Nonetheless, discussions and contact with patients about their condition and care should not be conducted via social media sites.

It is important to note that confidentiality extends to information about Trust staff and other stakeholders i.e. contractors. Staff must not post confidential / personal information about colleagues or other third parties.

Example Scenario - A member of staff Tweets, “crazy day at work, can’t believe Jane is still off sick she needs to go back to her GP again!”

In this scenario the staff member has disclosed personal information about her colleague who is ill, including the fact she has already been to her GP.

If a member of the public contacts a staff member for medical advice in a public forum, the staff member should politely direct them to an appropriate channel for such advice – such as NHS 111, NHS.uk or their local GP Practice. If a staff member receives a request from one of their patients, they should direct them to the hospital website, telephone, and email or appointment system, as appropriate.

Occasionally staff may receive an urgent request for help from a patient that requires an immediate response. As with all ‘Good Samaritan’ acts, staff must act in the best interests of the patient and follow their professional obligations at the earliest opportunity.

5.2 Personal Use

Social media has blurred the boundaries between a person’s private and professional lives. Staff who use social media in their personal life should therefore be mindful that inappropriate use could damage their own reputation and that of the Trust.

The duty to act in line with the conditions set out within this policy applies wherever a connection to the Trust or NHS can be made, not just when a member of staff is at work or using social media for work purposes.

Whenever a staff member’s association with the Trust can be identified, they are expected to behave professionally and in a way that is consistent with the Trust’s values and policies, and relevant professional codes of conduct. (Health, 2013)

Even if a staff member does not directly publicise their association with the Trust themselves, it could become known through images on friends’ sites or on the Trust website – it may be apparent from information posted on different social media accounts or when someone searches for names via internet search engines. For that reason, staff should never post anything that may reflect poorly on their professionalism or the Trust.

The key principle is to presume that anything posted online can be read by anyone, anywhere in the world. Others may share information that was initially posted to be 'private'. You can never totally delete something from the internet – once posted, it is potentially out there forever (e.g. it could have been reproduced on someone else's blog).

Staff should not air grievances with the Trust, colleagues or service users on social media. Posting any such comments even on a personal social media page (e.g. Facebook) can still be considered as part of an investigation. There have been cases of professional misconduct for posting information on the internet where the individual wrongly thought social media was a private domain. Posts must not contain anything contrary to the Trust's Equality, Diversity and Human Rights policy. Anything containing racist, sexist, homophobic, transphobic, xenophobic, sexually explicit, threatening, abusive, disrespectful or other unlawful comments must not be published.

If an employee posts under a pseudonym and at a later stage these posts are associated with their real name, all previous posts may be considered in any subsequent disciplinary process.

5.2.1 Official Trust/departmental sites

All official Trust social media sites require authorisation by the Communications Department. No other teams/staff within the Trust should set up corporate-related sites without the authorisation of the Communications Department.

Staff must not set up sites that are made to resemble an official site and may not use Trust logos in social media activity except with express permission from the Trust Communications Department.

Please note that, following authorisation, Trust social media pages will be monitored on an ad hoc basis by the Communications Department and may be closed due to inactivity, infrequent posts, breach of social media policy or poor interest (if, for example, the account has been active for 6 months or more but has less than 100 followers).

5.2.2 Communicating as yourself

If a member of staff associates themselves with Lancashire and South Cumbria NHS Foundation Trust on their social media site, they are expected to post under their real name. This demonstrates openness and honesty, and accountability. Even if you can't have your own full name as your username (e.g. because there is already an @johnsmith on Twitter), you should use your real name when registering the account and describing yourself.

If an employee posts under a pseudonym and at a later stage these posts are associated with their real name, all previous posts may be considered in any subsequent disciplinary process.

5.2.3 Respecting others

Lancashire and South Cumbria NHS Foundation Trust is committed to providing an organisation free from bullying and harassment in all its forms and will take all steps, to achieve this objective including, where necessary, appropriate action in accordance with the agreed disciplinary policy.

Under no circumstance should offensive comments be made online about colleagues, patients or anyone else. This may amount to cyber-bullying or 'trolling' and could be deemed a disciplinary offence. Where appropriate, action could be taken where individuals no longer work for the Trust.

Staff must seek permission from colleagues before posting personal details or images that may link them with the Trust and must not post anything about someone if they have been asked not to. Staff must always remove information about a colleague or another individual if they have been asked to do so.

5.2.4 Privacy Settings

Staff should be aware of privacy limitations when posting material using social media, and the extent to which information can be in the public domain.

Whatever is posted on a social media site could be in the public domain immediately. Even if initially shared with a limited group of followers or friends, it could still be copied and shared or published elsewhere.

Staff should carefully consider what they want to say before they publish anything, and work on the basis that anything they write or post could be shared more widely without their knowledge or permission. Staff should configure their privacy settings and review them regularly because social media sites cannot guarantee confidentiality, and do sometimes change their settings.

This means the public, employers or any organisation that staff have a relationship with may be able to access a staff member's personal information - and once information is online, it can be difficult to remove it.

Staff should be careful when sharing or retweeting posts, as they could be seen to be endorsing someone else's point of view.

5.2.5 Factual accuracy

When posting information, staff must ensure it is factually correct. If they discover they have reported something incorrectly, they should amend it and make it clear they have done so.

5.2.6 Ensuring comments are legal

All comments must be legal and must not incite people to commit a crime. There are legal requirements around privacy and confidentiality that staff must not breach – for example, the Data Protection Act 2018. Any confidentiality breaches of the Data Protection Act 2018 are a breach of contract of employment. All staff must complete their annual Data Security Awareness Training and ensure that all Trust policies are adhered to.

5.2.7 Understanding the implications of defamation

Staff could face legal proceedings for posted comments aimed at named individuals or an organisation that are considered to harm reputation.

Staff should not post information or comments which contain judgments in relation to the Trust, our services, contractors, their role or performance that could reasonably be considered to be derogatory or defamatory.

The Trust does not routinely monitor social media sites for staff activity. However, if it is brought to the attention of the Trust that inappropriate activity, information, images or comments have been posted, then allegations will be investigated.

5.2.8 Respecting copyrights

Staff must not use the Trust brand or use the NHS logo anywhere on their social media sites, or copy photos from internet or intranet sites. Similarly, staff must respect copyright laws and for that reason should not copy content or images from other websites or others' social media accounts due to the potential risk of breaching someone's copyright.

5.2.9 Work-related issues

In the course of their work, staff may have access to confidential or privileged information. When using social media, however, staff should only share information about the Trust that is in the public domain, and should not add derogatory comments on these issues.

Posts made by staff using their personal social media accounts may breach organisational policy if they bring the Trust into disrepute – for example, if people can identify the 'poster' as a member of Trust staff or the 'poster' is commenting on Trust-related matters. If the account is public, then posts are automatically open to be seen by everyone but even if a staff member restricts access to their account there is no guarantee that those people who do have access to it won't share posts more widely.

Staff must also respect patient confidentiality, and must never disclose information that could identify a patient.

5.2.10 Photography

If staff post any photos of themselves or colleagues in uniform or in an identifiable work setting, they must ensure that these represent a professional image of the Trust and adhere to relevant Trust policies, including uniform and infection, prevention and control. Staff must not post any work-related photographs of colleagues without their consent and must remove any photos if later asked to do so. Staff must not use a photo of themselves in uniform as their profile picture; this could give the impression that their site is an official site.

Staff must not post images containing patients on personal social media accounts. This does not prevent staff sharing, retweeting or linking to images that have been published on official Trust sites. (In these cases, the Trust has obtained the patient's written consent.)

Staff must take care to ensure that any photos taken in a work setting do not inadvertently include patient or staff identifiable data (for example on monitors or notice boards).

5.2.11 Respecting safeguarding issues

Posts made by staff must not encourage behaviour that could be linked to safeguarding issues, for example:

- Bullying
- Luring and exploitation
- Theft of personal information
- Encouraging self-harm or violence
- Glorifying activities such as excessive drinking or drug-taking

These kinds of posts may be investigated and result in disciplinary action in line with the Trust's Disciplinary Policy.

5.3 Professional Use

Using social media in a professional capacity has many benefits for staff including; opportunities for research, raising awareness of topical health issues, public engagement and the chance to establish a wider and more diverse professional network.

Staff using social media in a professional capacity should be mindful that inappropriate use could damage their own reputation and that of the Trust.

Staff must ensure that anything shared via social media is factually correct and if they discover otherwise, they should immediately amend it and make it clear they have done so.

Posts must not contain anything contrary to the Trust's Equality in Employment policy. Anything containing racist, sexist, homophobic, sexually explicit, threatening, abusive, disrespectful or other unlawful comments must not be published.

Staff must not set up social networking to resemble the Trust or any of its departments.

The Communications Team has responsibility for external communications at the Trust and are the only people authorised to set up social media accounts and campaigns for the Trust.

Anyone who wants to launch a social media account or campaign for the Trust must contact the Communications Team.

They will need to provide details of: the social media platform they plan to use, the aim of the account, the audience, how it will be resourced and managed (e.g. who will produce content, who will have access to upload content), a risk analysis, and how information on it will be stored (e.g. for FOI). The Communications Team will consider the request.

Where appropriate, the Communications Team will liaise with Information Governance before deciding whether to approve the request.

5.4 Use by patients/visitors

Patients/visitors are welcome to use social media sites while on our premises or in relation to our services and care, as long as they are not breaching another patient/visitor's confidentiality or posting comments that are offensive, illegal or defamatory.

Patients and visitors to Trust sites will be able to access guest wifi where installed. The appropriateness of accessible content will be automatically managed by the IT team using existing security protocols.

Patients and visitors may be able to access social media and internet sites via their mobile phone networks whilst at Trust sites, which are not subject to the same security protocols.

This does not prevent patients/visitors from commenting openly about our care and services, including expressing dissatisfaction – we welcome feedback and it is important that people can share their views in this way. Patients/visitors must, however, respect other people's rights to privacy, dignity and confidentiality.

1. Where staff suspect inappropriate use of social media or internet content by patients or visitors, they should alert their line manager in the first instance.
2. The Trust requires all users of mobile devices to use them in a courteous, considerate and non-intrusive manner to help maintain a caring environment and effective working environment for staff.
3. Mobile devices must not be used to photograph staff, patients or facilities without the explicit permission of the individual and the ward/department manager.
4. Patients may take photos of themselves and/or their relatives for personal reasons, and for their own personal use only. Patients and visitors must ensure that other patients are not visible in any part of such photography, to ensure confidentiality and to protect privacy and dignity.
5. Express permission is needed for photographs to be taken of the inside of hospital premises, particularly wards and clinical areas (including Trust staff). This should be obtained from the ward manager or Matron in the first instance. Taking photographs on our site of other patients, staff or visitors without their informed consent is not permitted.

We understand that our patients will want to stay in touch with their friends and family while in our care. We also have a duty to protect patient confidentiality and a responsibility to safeguard vulnerable patients in our care. The following guidelines apply to all our patients:

- You may overhear conversations about other patients while in our wards or departments. Please respect the confidential nature of these conversations by not sharing details about others in our care without their prior consent. If we obtain evidence of internet or social media activity that shares such confidential information, we will ask you to remove that content.
- Defamatory comments about members of our staff should not be shared in any public forum. Legal advice will be sought and action taken where necessary.

[We encourage you to download, print and display our no photography or video poster in your service area.](#)

5.5 Organisational Use

The Trust may choose to communicate with service users and other stakeholders via social media. Only individuals with permission to communicate via social media on behalf of the Trust may use such sites. Staff must not establish their own social media forum purporting to be on behalf of the Trust e.g. the “Information Governance Team at LSCFT Facebook” page is not permitted without appropriate approval.

For further advice on official use of social media on behalf of the Trust please contact the Communications Team.

Social media can be used to make Freedom of Information Requests, should the Trust receive a request via the Trust’s official social media the Information Governance Department and the Communications Department must be informed immediately.

5.6 Reporting Inappropriate Behaviour on Social Media

If a member of staff comes across information contained in Social Media sites that contravenes this policy, they should:

- a) raise it with their line manager in the first instance or
- b) if the line manager is implicated in the issue in any way, they should raise it with the manager at the next level above.

The issue will then be investigated in line with the appropriate policy.

Complaints about the use of social networking sites or other online activity will be taken as seriously as ‘real-world’ events by the Trust. Consideration should be given to:

- Any professional boundaries that have been crossed;
- Any breach of confidentiality;
- Whether an association to the Trust has been identified; and/or
- Whether any of the material is offensive to colleagues or service users or potentially damaging to the reputation of the Trust or any party to whom the member of staff owes a duty of care as an employee of the Trust.

In any instances where there are any comments or concerns which staff wish to raise in connection to use of social media sites by patients or visitors to the Trust these should be also be raised through the appropriate channels outlined in the Trust’s Freedom to Speak Up Policy and Incident Reporting process.

Staff should be aware that not maintaining appropriately rigorous passwords and IT security on social media accounts may leave them open to being hacked. This may mean their accounts are used to send offensive or inappropriate material. In such cases, the Trust may investigate and take appropriate action under the relevant policies.

5.7 Bullying and Harassment

If staff believe they are being harassed, bullied or victimised as a result of a social media post by another member of staff, patient or a member of the public, they can take action. Staff should raise

any such concerns with their line manager. They can also access the Trust's Grievance Policy & Procedure which outlines the informal and formal action that can be taken in relation to another member of staff. Alternatively, they can inform an adviser in HR,

Any incident which cannot be addressed internally, such as a post by a member of the public including patients and those close to them, can and should be reported to the Head of Security via Datix and to the police and the social media site. All incidents of this nature will be dealt with under the appropriate policies around protecting our staff and appropriate support will be offered by line managers and the HR dept.

5.8 Responding to Queries and Complaints

If someone raises an issue via social media which we would usually expect to be dealt with by the PALS Team then the Communications Team will issue a response via that social media site, provided the information sought is general in nature.

The Communications Team will monitor the site regularly and pass any more specific queries onto the PALS Team.

People may choose to discuss their own confidential health matters in a public forum or use social media sites to complain about a service experience.

In this event the PALS Team and/or Communications Team will send a private message response(s) to the individual to try and assist them. The person may wish their complaint to be answered through the traditional channels or through a private message to their social media account. If they want to use their account, then we will use the same protocols for answering a complaint using email. The Communications Team will update the site to let other users know that the issue is being dealt with and give any general guidance appropriate regarding the issue.

Staff must not disclose any personal information or answer any questions that could lead to the disclosure of personal information, via social media, unless they have taken steps to ascertain the identity of the person they are speaking to and are satisfied that the information is being communicated securely.

6.0 Monitoring

Standard	Time frame/ format	How this will be monitored	By whom
Monitor accounts representing the Trust	At all times	The main Trust accounts (Twitter , Facebook , LinkedIn and Instagram) which are the only accounts managed by the comms teams follow all other accounts linked to the Trust, we will monitor those as and when they post.	Communications Team

Policy/procedure documents are in date	Monthly	Live tracking system function of the online active library.	Policy Officer
Policy/procedure documents will be accessible	Published online – unrestricted access for all staff	Monitoring the online site for numbers of 'hits' as a proportion of total staff population. Monitoring the site for numbers of hits on policy update section – same.	Policy Officer

7.0 References (including applicable NICE publications)

Bibliography

Council, N. a. M., 2012. *Social networking sites*, s.l.: NMC.

Health, D. o., 2013. *Social Interaction – Good Practice*, s.l.: DoH.

8.0 Implementation plan

Category	Action(s)	Target date	Responsible person
Engagement	Share the policy via internal communications including The Update. Highlight the policy in the new 'Policy of the month' feature.	November 2021	Digital Communications Manager
Training	The communications team are able to offer social media training to any colleagues who request it.	Ongoing	Digital Communications Manager
Other (e.g. resources)	Promote in the staff Facebook group	November 2021	Digital Communications Manager

Appendix i: Equality Impact Assessment: this MUST be done in collaboration with the Trust Equality and Diversity Lead

When completing, remove all guidance text like this but do not alter or delete any elements of this assessment

LSCFT puts equality, inclusion, and human rights at the centre of the design and delivery of inclusive services for the diverse communities we serve, and the empowering culture we create for our staff.

The legal case is set out in the Equality Act 2010 and the practice is embodied by our staff every day, without exception.

We are stronger together.

Equality@lscft.nhs.uk



This assessment applies to any Trust policy document, or activity required in a Policy, which will have an impact on people.

Please refer to the Equality Impact Assessment (EIA) Form Guidance and the Equality and Diversity Lead. This assessment must be done in collaboration with the E&D Lead











1. What is the title of the Policy and purpose of the activity in requires or involves that needs to be considered and assessed for its impact on people?

Social Media Policy – outlines requirements and standards in relation to use of social media by all staff.

2. Which group/s of people is/are being considered?

☒ Patients / Service Users ☒ Staff ☒ Public ☒ Partner agencies
☐ Other (please specify here)

3. Which of the following protected characteristics may or are likely to be affected by this policy? (* in any box as needed)

Age	Disability	Gender-reassignment	Marriage/Civil Partnership <i>in employment only</i>	Pregnancy & Maternity	Race	Religion or Belief	Sex	Sexual Orientation	Other <i>detail below</i>
									
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Other:

4. What engagement is taking place or has already been undertaken with those who are likely to be affected?

The policy applies to staff only and will not disproportionately impact any groups.

The ED&I team viewed the policy and made minor amendments.

5. What impact or potential impact has been identified through the consultation?

Racism referenced in the policy would also be inclusive of xenophobia.

6. What further steps are needed to mitigate or safeguard against the impact/potential impact identified?

N/A

Outcome of the assessment	Action/s Required	Timescale	Accountability
---------------------------	-------------------	-----------	----------------

<p>Outcome 1: No change(s) required</p> <p><i>When the scoping exercise has not identified any potential for discrimination or adverse impact and all opportunities to promote equality have been taken.</i></p>	No further steps required		
<p>Outcome 2: Adjustments to remove barriers that were identified in the consultation</p> <p><i>We need to be satisfied that the proposed adjustments will remove the barriers identified.</i></p>			
<p>Outcome 3: There is still potential for adverse impact or missed opportunities to promote equality.</p> <p><i>This requires the consideration of 'reasonable adjustments' under the law to adapt and enable people to engage in or access the activities/practices required by the policy. In this case, the justification for continuing must be described here and should also be in line with the duty to have 'due regard'. For the most important relevant policies, compelling reasons will be needed. We need to demonstrate that there are sufficient plans to reduce the negative impact with 'reasonable adjustments' and/or plans to monitor the actual impact</i></p>			
<p>Outcome 4: Stop and rethink.</p> <p><i>When an EIA shows actual or potential unlawful discrimination you will now need to make changes to the policy and practices it requires.</i></p>			

<p>How will we monitor this and to whom will we report outcomes?</p> <p>The Chief Officer of the policy must be made aware of this assessment and any monitoring or rewriting in relation to outcomes 2,3 or 4</p> <p><i>Risks identified throughout the assessment process and controls designed to address them, must be described and rated and recorded on Datix or in service risk registers in line with Trust processes. Assurance mechanisms should be developed for each activity to ensure that equality and diversity compliance is achieved on an ongoing basis</i></p>	
--	--

7. Who undertook this assessment and when?

Name: Joanna Harrison	
Job Title: Equality, Diversity and Inclusion Manager	Date assessment started: 11/10/2021
Service: ED&I	Date assessment completed: 11/10/2021