Sheffield Health and Social Care NHS Foundation Trust

Proud to care in Sheffield

Policy:

CG 007 - Social Media Policy

Executive Director Lead	Director of Corporate Governance
Policy Owner	Director of Corporate Governance
Policy Author	Head of Communications

Document Type	Policy
Document Version Number	V4
Date of Approval by PGG	26/04/2021
Date of Ratification	18/05/2021
Ratified By	Audit and Risk Committee (ARC)
Date of Issue	05/05/2021
Date for Review	30/04/2024

Target Audience	All those working in the Trust in whatever capacity, including volunteers (including service user volunteers), Governors, students, casual and agency workers and secondees, who are collectively referred to as staff in this policy.

Keywords	Social media, Internet, staff

Storage and Version Control
The policy is available to all staff via the Sheffield Health & Social Care NHS Foundation Trust
Intranet. Hard copies will be distributed to each Clinical Directorate and also to Central Services.
An e-mail will be sent to all staff informing them that the policy is available.
Version control is the responsibility of the Director of Corporate Governance (Board Secretary).
This is Version 4 of the policy which is stored and available through the SHSC intranet/internet.
This version of the policy supersedes the previous version (V3 2019). Any copies of the previous
Policy held separately should be destroyed and replaced with this version.

Contents

Version Control and Amendment Log

Version No.	Type of Change	Date	Description of change(s)
0.1	Draft policy creation	October 2015	Previous guidance in operation updated to policy status.
1.0	Ratification and issue	August 2016	Amendments made during consultation, prior to ratification. Review undertaken prior to issue in order to comply with new Policy on Policies.
2.0	Policy updated	Septe mber 2016	Changed to reflect new terminology around social media use and new platforms in use.
3.0	Policy updated	August 2019	Changed to reflect the open access to social media channels for colleagues via managed service user accounts
4.0	Policy updated	March 2021	Changed following consultation with the BAME staff network group to ensure clear statement that sharing or liking content on social media, that is bullying or discriminatory, to anyone with protected characteristics is unacceptable.

Flowchart – *Where appropriate, a flowchart or diagram which summarises the policy and processes to be followed should be included here. It is recommended that this it is placed here at the start of the document for ease of access. However; this must not imply that staff should only refer to the flowchart and not the text of the policy. The flowchart should include references to sections of the policy to assist staff in finding the right place in the full document.*

Not required for this policy

1. Introduction

1.1 For the purposes of this policy, social media is defined as an interactive media that allows parties to communicate instantly with one another or to share data in a public forum. The type of platform may include (but is not limited to); blogs, messaging sites, social networking sites, image sharing sites, video hosting sites and discussion sites.

This policy is intended to help staff make appropriate decisions about the use of social media platforms, including but not limited to Facebook, Twitter, LinkedIn and Tumblr, as well as YouTube, Flickr, Instagram and other image and video-sharing sites. This list is not intended to be exhaustive as this is a constantly evolving area. Staff should adhere to this policy in relation to any form of social media with which they engage.

1.2 While it is recognised that all staff are entitled to privacy in their personal life, the Trust is committed to maintaining service user and staff confidentiality and safety at all times while also maintaining the reputation of the Trust and that of the relevant professions by ensuring that staff exhibit acceptable behaviour at all times.

1.3 The Trust recognises the positive intent of staff in using social media in their professional and personal lives. This policy is intended to support this by providing clarity of expectation and making staff aware of the potential risks associated with social media activity. Anyone posting on social media should assume their comments are public for all the world to see for many years to come.

1.4 All members of staff need to be aware that, even if they believe that they are using these sites with enhanced privacy settings applied, this does not exempt them from the guidelines which are outlined in this policy.

1.5 If a member of staff is concerned about something they read on a social media site, it is their professional responsibility to alert their line manager, complete an incident form and report the matter to the Communications Team. Line managers are responsible for ensuring staff adhere to this the social media policy.

1.6 This policy complements other Trust policies such as, but not limited to, Internet Acceptable Use Policy, Declaration of Interests and Business Standards Policy, Confidentiality Code of Conduct, and the Mobile Phones, Communication Devices and Internet Access for Service Users Policy.

2. Scope

2.1 The policy applies to all those working in the Trust in whatever capacity, including volunteers (including service user volunteers), Governors, students, casual and agency workers and secondees, who are collectively referred to as staff in this policy.

2.2 All staff are expected to comply with this policy at all times to protect the privacy, confidentiality and interests of the Trust and our services, employees, staff and service users.

2.3 Breach of this policy may be dealt with under the Trust's Disciplinary Policy or any

other policy guiding professional behaviour, including the Trust's Constitution and Code of Conduct. In serious cases, breaches may be treated as gross misconduct leading to summary dismissal.

2.4 This policy should be read with reference to any relevant professional/union code of conduct such as the General Medical Council, Nursing and Midwifery Council and Health and Care Professionals Council guidelines on social media usage.

- http://www.nmc-uk.org/Nurses-and-midwives/Regulation-in-practice/Regulation-in-Practice- Topics/Social-networking-sites/
- http://www.gmc-uk-org/Doctors_use_of_social_media.pdf_51448306.pdf
- http://www.hpc-uk.org/assets/documents/100035B7Social_media_guidance.pdf

2.5 This policy does not relate to service user access to social media. This is covered by the Mobile Phones, Communication Devices and Internet Access for Service Users Policy.

3. Definitions

Social media is a generic term which refers to websites, online tools and other interactive communication technologies which allow users to interact with each other in some way, by sharing information, files, opinions, knowledge and interests. As the name implies, social media involves the building of communities or networks, encouraging participation and engagement.

4. Purpose

4.1 The purpose of this policy is to outline the standards we require staff to observe when using social media in both a personal and professional capacity. The policy will also detail the circumstances in which we will monitor staff use of social media and the action we will take in respect of breaches of this policy.

4.2 This policy sets out the principles which staff are expected to follow when using social media both in their personal lives and professionally. The internet involves fast moving technologies and it is, therefore, impossible to cover all circumstances.

4.3 This policy aims to:

- outline to staff what is considered acceptable use of social media linked to their employment;
- make a clear distinction between acceptable usage of social media at work and in staff's personal lives;
- encourage staff to be mindful of what content they share on the internet;
- ensure that appropriate standards of confidentiality are maintained;
- ensure that professional boundaries with service users are maintained and protected;
- maintain and protect the reputation of the Trust.

4.4 If a member of staff identifies an association with the Trust, discusses their work and/or colleagues, or comes into contact, or is likely to come into contact with service users on any social media sites, they must behave appropriately and in a way which is consistent with the Trust's values and, where relevant, with their professional code of conduct. The duty to act in a manner that is in line with the conditions set out in this policy applies when staff are at work, and at all times when a connection to the Trust,

the NHS or their profession has been made, either explicitly or obliquely.

4.5 The intent of this policy is not to stop staff from conducting legitimate activities on the internet, nor to stifle constructive criticism, but serves to highlight those areas in which problems can arise for both individual employees and the Trust.

5. Duties

5.1 All leaders in the Trust are responsible for promoting and supporting the aims and objectives of this policy.

5.2 The Head of Communications has overall responsibility for the effective operation of this policy. Questions regarding the content or application of this policy should be directed to the Communications Team.

5.3 The Head of Communications is responsible for reviewing the operation of this policy and making recommendations for changes to minimise risks to Trust operations.

5.4 It is every manager's responsibility to ensure that staff are aware of this policy and to take appropriate action when informed of incidents where staff behaviour is not in accordance with this policy.

5.5 Managers are advised to ensure that a hard copy of this policy is available and accessible for those staff who do not have managed service user IT accounts.

5.6 Managers are required to ensure that any issues or concerns reported to them which involve social media use are acted upon in line with this policy and a record kept of the matter that has been raised along with any action taken.

5.7 The Volunteer Co-ordinator must ensure that all volunteers (including service user volunteers) are aware of this policy.

5.8 All staff are responsible for their own compliance with this policy and for ensuring that it is consistently applied. All staff should ensure that they take the time to read and understand this policy.

5.9 All staff must make sure that they conduct themselves online in the same manner that would be expected of them in any other situation – to uphold the reputation of the Trust and, where relevant, the reputation of their profession. Staff who use social media will be responsible for ensuring that they are aware of this policy and understand the content and principles of the policy.

5.10 If a member of staff is concerned about something they read on a social media site, it is their professional responsibility to alert their line manager, complete an incident form and report the matter to the Communications Team who will ensure that any appropriate action is taken.

5.11 If a member of staff becomes aware of any content posted on social media about the Trust (whether complimentary or critical) please report it to the Communications Team who will ensure that any appropriate action is taken.

5.12 The Trust does not routinely monitor social media sites for evidence of staff activity.

However, if it is brought to the attention of the Trust that inappropriate information, images or comments have been posted, then the allegation will be investigated.

6. Process – Social Networking

6.1 Summary of principles

6.1.1 When any member of staff uses social media it is expected that they will behave in a manner which acknowledges the duty of care they owe to their colleagues and the organisation regardless of whether they explicitly state they work for our organsation

6.1.2 Once information has been published on the internet it is no longer considered to be private. This means staff will be held accountable for any information posted, liked or in any way endorsed, which is compromises themselves, their colleagues and/or the Trust.

6.1.3 Staff are personally responsible for the content they publish on social media tools – what is published will be in the public domain for many years.

6.1.4 Staff should be aware that some social media sites have been known to make changes to users' privacy settings without warning and without the knowledge of the users concerned. All staff should regularly check their privacy settings.

6.1.5 It is also important to be aware that other staff or members of the public may, where appropriate, raise concerns with the Trust about content that they have viewed on social media to which they have access. They may also be able to share that data with others who would not otherwise be able to see it, without the original user's knowledge or permission, for example, by taking a screen shot.

6.1.6 Staff should also be mindful that connections could be made by members of the public between them making personal use of one site (such as Facebook) and identifying themselves as an employee of the Trust or NHS on another (for example, LinkedIn), particularly if both sites identify them by a photograph or some other unique personal data.

6.1.7 It should, therefore, **never** be assumed that something which is posted on a social media site is private and cannot be viewed by others online.

6.1.8 Within social media sites, individuals may post comments, pictures or phrases to which other individuals can indicate their support/agreement by clicking the 'like' button or by 'sharing' on Facebook or 'retweeting' on Twitter, for example. This action is seen to be attaching the staff's name and implied support to the material. This can be seen as being equivalent to posting the comment originally and, therefore, this action should be considered as a breach of this policy and the code of conduct

6.2 Use at work

6.2.1 Staff can access or contribute to social media sites using Trust-owned equipment.

6.2.2 The Trust understands that staff may wish to use their own devices such as mobile phones to access social media websites while they are at work, but staff must limit

the use of their own devices so not to interfere with their working day and this access must be limited to their allocated breaks.

6.3 Trust approved social media pages which promote or support Trust services

6.3.1 We recognise the importance of the internet in shaping the reputation of the Trust and our services, employees, partners and service users. We also recognise the importance of our staff joining in and helping shape health service conversation and direction through appropriate interaction in social media. Therefore, the Trust will support the use of social media for these purposes, provided the standards and procedures below are followed.

6.3.4 The majority of Trust approved social media activity is to take place using the corporate dedicated Twitter, Instagram and Facebook accounts which are managed by the Communications Team. Individual services or staff groups are permitted to run additional accounts for Trust purposes provided they seek advice from the Communications Team in establishing and running their channels so they can provide timely and relevant content for their target audiences. This will be monitored by the Communications Team to ensure the content remains relevant and suitable for the chosen channel. Individual members of staff may choose to have their own personal accounts and should follow the guidance in this policy when creating these and posting content.

6.3.5 On receipt of approval from the Communications Team, individual services are able to establish closed, private Facebook groups to communicate with service users and/or carers.

If approval is granted, the responsible staff must ensure that the following is adhered to:

- The group must be private and by 'invitation only'. The invitation must only be extended to relevant staff and service users and/or carers (if the group is for carers);
- A set of ground rules for the group must be established which every member must sign up to – the rules must cover confidentiality, appropriate behaviour and language and respect for others as a minimum;
- One member of staff must be designated as the 'moderator' and monitor postings for inappropriate use, behaviour, language, discussions etc.
- If photographs are to be posted, then signed consent from anyone appearing in the photographs must be obtained (prior to posting) using the Trust's photo consent form - for link see appendix C.
- If anyone in the group objects to the photographs, they must be taken down/deleted immediately.
- There should be a clear plan for the closure or deletion of the group, should the service decide (for whatever reason) that the group should not continue.

6.3.6 All services or staff groups wishing to promote their service, events or activities via social media should send the request and any relevant information to the Communications Team.

6.3.7 When posting to the corporate social media accounts, extreme care must be taken when making comments about the goods and/or services provided by a third party, especially when providing a hyperlink/link to another site. It is the responsibility of the individual to ensure that the link is valid, and the content of the site and the goods or

services provided by the third party will not bring the Trust into disrepute.

6.3.8 Where an image, photograph, video or audio recording of any individual is to be published on the corporate social media accounts, the consent of the individual must be obtained and a signed consent form (see Appendix C) must be held on file.

6.3.9 The use of social media as the sole means of contact or communication with any given individual or group must be avoided as this may discriminate against those who do not have access to such a facility.

6.3.10 Posts on the Trust's corporate social media accounts will follow the following guidelines:

- The Trust will not upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content;
- The Trust will never disclose commercially sensitive, anti-competitive, private or confidential information;
- The Trust will only upload, post or forward third-party content when we have assured ourselves that to do so is appropriate;
- The Trust will comply with the terms and conditions of any social media platform we use;
- The Trust will not post, upload, forward or post a link to chain mail, junk mail, cartoons, jokes or gossip;
- The Trust will always consider others' privacy and avoid discussing topics which may be inflammatory (e.g. politics or religion);
- The Trust will be honest and open. If we make a mistake in a contribution we will be prompt in admitting and correcting it;
- The Trust will correct any misrepresentations of the Trust with facts where we can do so;
- The Trust will not escalate heated discussions. We will be conciliatory and respectful. Where appropriate, we will aim to take sensitive, personal or contentious situations offline and offer the contributors an alternative means of contact.

6.4 Personal use

6.4.1 The Trust recognises that staff may want to access or contribute to social media sites using their own equipment outside their hours of work and during their authorised breaks at work.

6.4.2 Staff are responsible and personally liable for any comments, images and information they post.

6.4.3 While using social networking sites in a personal capacity and not acting on behalf of the Trust, it should still be recognised that staff's actions can damage the Trust's reputation. All communications that are made, even in a personal capacity, must not:

- Behave in a manner that would not be acceptable in any other situation;
- Bring the Trust into disrepute (e.g. anything which could impact negatively on the Trust's reputation or could cause embarrassment to the Trust, staff, service users or the public;
- Breach confidentiality (e.g. any personal information about service users or staff, or any confidential corporate information – refer to the Trust's

Confidentiality Statement);

- Make comments, post images, share content, like or retweet content that that could be considered to be bullying, harassment or discriminatory against any individual with protected characteristics including but not limited to ageism, racism, disability discrimination, gender discrimination. Leaders should refer to the Trust's Bullying and Harassment policy and the equality and human rights commission for a full list of protected characteristics: https://www.equalityhumanrights.com/en/equality-act/protected-characteristics
- Use offensive or intimidating language;
- Pursue personal relationships with current service users/patients/clients. Pursuing personal relationships (i.e. romantic or sexual relationships) with current service users, patients or clients is not acceptable under any circumstances. These actions will bring about possible disciplinary proceedings which could result in the member of staff's dismissal;
- Use social networking sites in any way which is unlawful;
- Post inappropriate comments about colleagues or service users/patients/clients (even if their names are not mentioned);
- Contain information that could potentially identify a service user (e.g. a service user's name, address, postcode, ID numbers, photograph, voice recording, rare condition, celebrity status etc.);
- Post images which contain recognisable signs or pictures relating to the Trust, or any pictures of staff or service users without their explicit, fully-informed consent;
- Like, support or endorse content which may unwittingly cause offence and constitute unlawful discrimination in the form of harassment or discrimination toward people with protected characteristics including (but not limited to), race, age, pregnancy, religion and sexual orientation.
- Comment on work related issues. Staff are reminded that any grievance should be raised using the Grievance Policy.

6.4.4 Staff are reminded that information they share on social media may be classified as online bullying. Online bullying is bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as mobile telephones, computers and tablets as well as communication tools including social media sites, text messages, chat and websites. This also includes use of the Trust's clinical IT systems and instant messaging facilities.

Examples of online bullying include mean text messages or e-mails, rumours sent by e-mail or posted on social networking sites and embarrassing pictures or videos. Bullying through this platform can include posting negative comments on pictures, posting abusive posts on a user's wall, using pictures or videos to make fun of another. Many of the acts of bullying on social media are similar to those that would take place in a real-life situation, only in digital form.

6.4.5 Professionally qualified staff may place their registration at risk if they fail to adhere to the guidelines identified in 2.4.

6.4.6 All staff should be mindful of the personal information they disclose on social networking sites, especially with regard to identity theft. Making information such as your date of birth, place of work and other personal information publicly available can be high risk in terms of identity theft.

6.4.7 There have been occasions when staff have had to take out restraining orders on service users who display obsessive behaviours, such as stalking, online bullying etc.

Staff should not register on a public social media site without taking adequate privacy precautions.

6.4.8 Where staff associate themselves with the Trust (through providing work details or joining a Trust or NHS network), they should act in a manner which does not bring the Trust, the NHS or their profession into disrepute. This applies to both open and private sections of a site if a member of staff has identified themselves as an employee of the Trust or has connections to work colleagues (i.e. as 'friends' or 'followers' for instance) within the Trust or other NHS and NHS-related organisations.

6.4.9 Staff should also be mindful that their user names on social media sites can demonstrate a connection to the Trust, the NHS or their profession.

6.4.10 Where a member of staff chooses to associate themselves with the Trust or the NHS on a social media site (for example, adding on Facebook or Twitter where they work or have previously worked) they must add a disclaimer statement in a prominent position (preferably on their profile) which clearly states that whatever is posted represents their personal views only and not necessarily the views of the Trust, the NHS or their profession.

6.4.11 The Trust's logo must never be used on personal webpages or social media sites (other than on approved Trust sites/pages).

6.4.12 Before posting images or joining any campaigns/causes, staff should be aware that it is not just friends who view these, but also service users, colleagues, managers and prospective employers.

6.5 Professional use

6.5.1 The Trust acknowledges that some staff may wish to have a professional presence on social media. In doing so, staff must ensure that their online conduct meets the expectations and standards set out in this policy and that it does not in any way conflict with their obligations to the Trust.

6.5.2 Staff must be clear when posting on social media that they are doing so in a personal capacity and that their views are their own and not necessarily the views of the Trust, the NHS or their profession. Staff should also ensure that any commercial interests that arise from professional social media use are declared to the Trust in accordance with the Declaration of Interests and Standards of Business Conduct Policy.

6.5.3 Staff must also ensure that they declare any potential conflicts of interest when writing about professional matters online, taking full account of the fact that members of the public, including other staff and service users/patients/clients, may place a high value on their opinions as a clinician/NHS professional. Conflicts of interest may include financial interests in other organisations or any secondary employment undertaken, for example, in private practice. As stated in the Declaration of Interests and Standards of Business Conduct Policy, staff must also ensure that any such interests are declared to the Trust. Any staff contact by members of the media for comment following a professional comment they have put on social media should seek advice from the Communications Team.

6.6 Interactions involving different affected groups

6.6.1 Service users/patients/clients

Confidentiality must be maintained at all times. No information which could lead to a service user and/or their carer being identified should be disclosed through social media.

6.6.2 It is accepted that some staff may have family members or friends who are service users of the Trust and that they may have contact with them via social media. In addition, some staff will be service users of Trust services and may have contact with colleagues on social media.

Staff should not send friend requests on Facebook, follow or initiate @mentions on Twitter to people they provide direct care to. The same principle applies to other social networks such as LinkedIn or Google+.

Staff may also wish to consider whether it is appropriate for them to be friends with or follow known carers or family members of people to whom they have provided care.

6.6.3 If a member of staff is contacted online by a someone they provide direct care to or a carer and/or family member of someone they provide direct care to, in order to protect both themselves and the service user or carer from any risk, they should politely decline to engage in any contact and report the matter immediately to their line manager.

6.6.4 Should a former service user or carer make contact with a member of staff through social media, the member of staff should consult their professional guidelines, speak to their line manager and seek advice from the Communications Team before accepting the contact.

6.6.5 Should a current or former service user or carer who is working as a Trust volunteer or peer support worker make contact with a member of staff through social media, the member of staff should consult their professional guidelines, speak to their line manager and seek advice from the Communications Team.

6.6.6 Please see further guidance for service users on the use of internet and social media on Trust premises in the Mobile Phones, Communications Device and Internet Access for Service Users Policy.

6.6.7 Work colleagues

When interacting with colleagues online, staff should be ever mindful of their responsibilities to be professional and courteous. They should never engage in any behaviour which attacks or abuses any colleagues or act in any way which may damage working relationships.
See 6.1.8 for guidance on what is deemed as staff showing support for content.
See 6.4.3 for guidance on unacceptable behaviors online.

6.6.8 When content is being uploaded which includes other members of staff, for example, pictures from a social event, then permission should be sought from all colleagues before the item is posted and no images or items should be posted when requests have been made for them not to be posted. Any item that a colleague has asked to be

removed which includes them should be removed immediately.

6.6.9 Staff should be aware of the consequences of using any social media site to post content of any kind that conflicts with information they have already provided to the Trust, for example, in relation to their health and fitness for work or any secondary employment that they undertake.

6.6.10 These actions will bring about possible disciplinary proceedings which could result in dismissal.

6.6.11 The Trust

In any instances where there are any comments, questions or observations which staff wish to raise in connection with their employment with the Trust, either positive or negative, these should be raised through the appropriate channels internally rather than the views being expressed on social networking sites. Additional guidance and support is available via line managers and/or the Human Resources Department.

6.6.12 Staff should be aware that this may also apply to 'private messages' exchanged between work colleagues as, although they may not necessarily be seen by a wider audience, they may still be brought to the attention of the Trust.

6.7 The use of social media data in investigations

6.7.1 The Trust reserves the right to monitor staff's internet use on any Trust device, in line with the Internet Acceptable Use Policy. Any data obtained about a member of staff's internet use may, therefore, form part of an investigation under the Trust's Disciplinary Policy.

6.7.2 If concerns are raised with the Trust by another member of staff or a member of the public about the online behaviour of any staff, the Trust will be required to investigate this. The Trust may, therefore, obtain copies of data posted on social media, and these may be kept electronically or in hard copy. This data will be retained by the Trust in line with the Trust's policies on records management.

6.7.3 The Trust reserves the right to view service user or staff social media accounts as part of any investigation where abuse of a vulnerable person or child is suspected.

6.8 Breaches of this policy

If there is an instance where the guidance set out in this policy appears to have been breached and the breach is brought to the attention of the Trust, then the matter should be investigated to ascertain the nature and extent of the concerns which have been raised. The investigation should be carried out in accordance with the Trust's Disciplinary Policy.

6.8.1 Complaints about the use of social networking sites or other online activity will be taken as seriously as 'real-world' events. Consideration will be given to any professional boundaries which may have been breached, 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, patients and clients, or potentially damaging to the reputation of any party to whom staff owe a duty of care as employees or volunteers of the Trust.

6.8.2 If any member of staff is concerned about another member of staff's behaviour online, then they should report this to their line manager along with any supporting evidence of their claim, so that the appropriate action can be taken in accordance with Trust policy. If you are unable to raise your concern with your line manager please contact HR for further advice.

6.8.3 Failure to follow this policy may result in the implementation of the disciplinary procedures and/or may constitute a breach of professional code of conduct. In serious cases, a breach may be regarded as gross misconduct and may result in dismissal.

7. Dissemination, Storage and Archiving (Control)

The policy will be made available to all staff via the Sheffield Health & Social Care NHS Foundation Trust intranet. An e-mail will be sent to all staff informing them that the policy is available

Previous versions of the policy will be deleted by the Director of Corporate Governance (Board Secretary), however, a hard copy of each previous version will be held by the Director of Corporate Governance (Board Secretary) in the relevant archive.

Version control is the responsibility of the Director of Corporate Governance (Board Secretary)

7.1 This policy will be implemented within the Communications Team by the Head of Communications.

Version	Date added to intranet	Date added to internet	Date of inclusion in Connect	Any other promotion/ dissemination (include dates)
3.0	30/08/2019	30/08/2019	Sept 2019	
4.0	April 2021	April 2021	April 2021	

8. Training and Other Resource Implications

8.1 Social Media Awareness raising is part of the mandatory Corporate Induction for new starters. It is also included in the Mandatory Training Update Day.

8.2 To facilitate continual improvement in communications, one-to-one training will be provided throughout the year for relevant managers involved in communications.

8.3 The Communications Team will be available to work with groups of staff to address their specific training and learning needs. Contact the Communications Team on 2716706.

8.4 Service Directors, Assistant Service Directors, Service and Team Managers are responsible for making sure that their staff are aware of and comply with this policy.

9. Audit, Monitoring and Review

Monitoring Compliance Template						
Minimum Requirement	Process for Monitoring	Responsible Individual/ group/committee	Frequency of Monitoring	Review of Results process	Responsible Individual/group/ committee for action plan	Responsible Individual/group/ committee for action plan monitoring and
2.10 Being Open	Review	Head of Communications Quality Assurance Committee Directorate Leads	Quarterly	Head of Communications	Head of Communications	Head of Communications
6.2 Patient Information	Review	Head of Communications Quality Assurance Committee Directorate Leads	Quarterly	Head of Communications	Head of Communications	Head of Communications

9.1 The implementation of the procedure and compliance with its guidelines will be audited by the Communications Manager on an annual basis.

9.2 Responsibility for monitoring national guidance (which may necessitate an early review) rests with the Communications Manager who will advise the Executive Directors' Group as required.

9.3 The Trust Board will receive regular updates on the Trust's Corporate Objectives and the business and clinical strategies which this policy supports.

9.4 This policy will be reviewed in April 2024.

10. Implementation Plan

Action / Task	Responsible Person	Deadline	Progress update
Put new policy onto intranet and website and remove old version	Communication Team	As soon as ratified.	
Make staff aware of new policy via Connect	Communications Team	First digest following ratification	
All Managers to ensure that they make their staff aware of the new policy and its implications	All Trust managers	Within a week of being informed of the new policy via the Communications Digest	
Dedicated webpage on staff intranet to be updated	Communications Team	Within a week of the policy being ratified	
Updated information to be provided to the Training Department for Corporate Induction and Mandatory Training Update Date	Head of Communications	Within a week of the policy being ratified	

11. Development, Consultation and Approval

This policy was developed by the Communications Team with advice and support from the Volunteer Coordinator, HR and Deputy Board Secretary.

12. Links to Other Policies, Standards and Legislation (Associated Documents)

Social Media Dos and Don'ts,
Communications Policy & Guidance,
Being Open Policy,
Complaints Policy,
Confidentiality Code of Conduct,
Declaration of Interests and Business Standards Policy,
Internet Acceptable Use Policy,
Disciplinary Policy,
Mobile Phones,
Communication Devices and Internet Use for Service Users Policy,
Safeguarding Adults Policy,
Safeguarding Children Policy,
Bullying and Harassment Policy,
Whistleblowing Policy and Procedure.

13. Contact Details

Title	***Name***	***Phone***	***Email***
Director of Corporate Governance (Board Secretary)	David Walsh	0114 305 0803	david.walsh@shsc.nhs.uk
Head of Communications	Holly Cubitt	0114 2711267	holly.cubitt@shsc.nhs.uk

14. References

NHS Constitution:
http://www.nhs.uk/choiceintheNHS/Rightsandpledges/NHSConstitution/Pages/Overview.aspx

NHS Brand Guidelines: http://www.nhsidentity.nhs.uk/

Appendix A – Stage One Equality Impact Assessment Form

Equality Impact Assessment Process for Policies Developed Under the Policy on Policies

Stage 1 – Complete draft policy

Stage 2 – **Relevance** - Is the policy potentially relevant to equality i.e. will this policy potentially impact on staff, patients or the public? If **NO** – No further action required – please sign and date the following statement. If **YES –** proceed to stage 3

This policy does not impact on staff, patients or the public (insert name and date)

Stage 3 – **Policy Screening** - Public authorities are legally required to have 'due regard' to eliminating discrimination , advancing equal opportunity and fostering good relations , in relation to people who share certain 'protected characteristics' and those that do not. The following table should be used to consider this and inform changes to the policy (indicate yes/no/ don't know and note reasons). Please see the SHSC Guidance on equality impact assessment for examples and detailed advice this can be found at http://www.shsc.nhs.uk/about-us/equality--human-rights

	Does any aspect of this policy actually or potentially discriminate against this group?	**Can equality of opportunity for this group be improved through this policy or changes to this policy?**	**Can this policy be amended so that it works to enhance relations between people in this group and people not in this group?**
AGE	No	N/A	N/A
DISABILITY	No	N/A	N/A
GENDER REASSIGNMENT	No	N/A	N/A
PREGNANCY AND MATERNITY	No	N/A	N/A
RACE	No	N/A	N/A
RELIGION OR BELIEF	No	N/A	N/A
SEX	No	N/A	N/A
SEXUAL ORIENTATION	No	N/A	N/A

Stage 4 – **Policy Revision** - Make amendments to the policy or identify any remedial action required (action should be noted in the policy implementation plan section)
Please delete as appropriate: no changes made.

Impact Assessment Completed by (insert name and date) Holly Cubitt – March 2021

Appendix B – Examples Of Online Racist Discrimination

Examples of online discrimination:

- Saying mean or rude things about someone because of their race or ethnic group
- Sharing a racist image online
- Making or sharing jokes about people of a particular race or ethnic group online
- Saying things that were untrue about people of a particular race or ethnic group
- Saying mean or rude things about a particular ethnic group online
- Excluding someone from a site/group because of my race or ethnic group online
- Making or sharing threats or threatening material aimed towards people because of their race or ethnic group

Appendix C (Consent Form)

Photography and filming consent form can be found on Jarvis here;

https://jarvis.shsc.nhs.uk/documents/photography-consent-form

Appendix D

Review/New Policy Checklist

This checklist to be used as part of the development or review of a policy and presented to the Policy Governance Group (PGG) with the revised policy.

		Tick to confirm
	Engagement	
1.	Is the Executive Lead sighted on the development/review of the policy?	x
2.	Is the local Policy Champion member sighted on the development/review of the policy?	x
	Development and Consultation	
3.	If the policy is a new policy, has the development of the policy been approved through the Case for Need approval process?	
4.	Is there evidence of consultation with all relevant services, partners and other relevant bodies?	x
5.	Has the policy been discussed and agreed by the local governance groups?	X
6.	Have any relevant recommendations from Internal Audit or other relevant bodies been taken into account in preparing the policy?	x
	Template Compliance	
7.	Has the version control/storage section been updated?	x
8.	Is the policy title clear and unambiguous?	No
9.	Is the policy in Arial font 12?	x
10.	Have page numbers been inserted?	x
11.	Has the policy been quality checked for spelling errors, links, accuracy?	x
	Policy Content	
12.	Is the purpose of the policy clear?	x
13.	Does the policy comply with requirements of the CQC or other relevant bodies? (where appropriate)	x
14.	Does the policy reflect changes as a result of lessons identified from incidents, complaints, near misses, etc.?	x
15.	Where appropriate, does the policy contain a list of definitions of terms used?	x
16.	Does the policy include any references to other associated policies and key documents?	x
17.	Has the EIA Form been completed (Appendix A)?	x
	Dissemination, Implementation, Review and Audit Compliance	
18.	Does the dissemination plan identify how the policy will be implemented?	x
19.	Does the dissemination plan include the necessary training/support to ensure compliance?	x
20.	Is there a plan to i. review ii. audit compliance with the document?	x
21.	Is the review date identified, and is it appropriate and justifiable?	x