NHS

City Hospitals Sunderland NHS Foundation Trust
South Tyneside NHS Foundation Trust

SOCIAL MEDIA POLICY

Document Reference	C2.SM.V1.0
Document status	FINAL
Target Audience	This policy applies to all staff working at City Hospitals Sunderland NHS Foundation Trust and South Tyneside NHS Foundation Trust and their respective subsidiary companies including: all Trust staff (both permanent and non-permanent), agency staff, Trust governors, volunteers, students undertaking education and training and staff from other organisations working on the Trusts' premises.
Date Ratified	14 June 2018
Ratified By	Joint Policy Committee
Release Date	28 June 2018
Review Date	June 2021
Sponsor	Liz Davies, Head of Communications

City Hospitals Sunderland NHS Foundation Trust

Version	Date of Amendments	Author	Update comments
1.0	December 2011	Catherine Fisher, Trust Librarian and Simon Joyce, Network Services Manager	Create Draft Policy
1.1	December 2011	Catherine Fisher, Trust Librarian	Comments from Information Governance Steering Group incorporated
1.2	January 2012	Catherine Fisher, Trust Librarian	Comments from HRSG on Section 5.1 incorporated.
1.3	March 2012	Jan Armstrong, Deputy Director of Human Resources	Comments from Joint Consultative Group on Section 5.1 incorporated
1.4	April 2012	Jan Armstrong, Deputy Director of Human Resources	Comments from Executive Committee on pp 7, 9,10,12,13 incorporated

Version	Date of Amendments	Author	Update comments
1.5	June 2012	Jan Armstrong, Deputy Director of Human Resources	Guidance received from the General Medical Council incorporated
South Tyneside NHS Foundation Trust			
IM0033_v1	June 2013	Mike Robson Executive Director Finance	
IM0033_v1.2	March 2015	JC	Policy reviewed and re-issued
South Tyneside and Sunderland Healthcare Group			
1.0	June 2018	Liz Davies Head of Communications	Social media policy revised and updated for both FTs

CONTENTS

1 INTRODUCTION

Social media is now part of everyday life for millions of people and has a significant impact on organisational, professional and individual reputations. This policy outlines the appropriate use of social media by employees of both Trusts including staff employed in Trust subsidiary companies (all Trust staff); agency staff, Trust governors, volunteers, students undertaking education and training and staff from other organisations working on Trust premises.

It sets out the responsibility of individuals when using social media, both in a personal and professional capacity, in order to maximise benefits and minimise risks and is in line with national guidance from the NHS and a number of professional bodies.

2 PURPOSE & SCOPE

The social media policy outlines expected behaviours and personal responsibilities for all Trust staff (and others listed above) when using social media. Staff should follow the same behaviour standards online as they would in their everyday roles and abide by their legal and ethical duties to protect patient/service user and colleague confidentiality.

The policy applies to Trust staff when accessing social media either on computers, laptops, tablets or smart phones owned or controlled by the Trust or connected to the Trusts network, or on their own personal laptops, tablets or smart phones.

Both Trusts acknowledge the right of all staff to freedom of expression and recognise that all staff are entitled to use social media in a personal capacity. This policy is not to stop the use of social media but provides up-to-date guidance to avoid potential problems arising for both individual staff members and both Trusts.

3 DUTIES

3.1 Board of Directors
The Board of Directors is responsible for ensuring there is a robust system of corporate governance within the Trusts. This includes ensuring that the Trusts' policies comply with all legal, statutory and good practice requirements in relation to social media.

3.2 Chief Executive
The Chief Executive is accountable for ensuring the proper application of this policy through effective management arrangements.

3.3 Head of Communications
The Head of Communications for the Trusts has delegated responsibility on all issues relating to media and social media, including the development, upkeep and sharing of this policy via internal communications across both organisations.

3.4 Caldicott Guardian

The Trusts' Caldicott Guardians have a strategic role which involves representing and championing patient confidentiality and issues at senior management level. As such, the Caldicott Guardian will be called upon for advice in relation to social media usage and any circumstances where staff may have contravened this policy in relation to patient confidentiality.

3.5 Data Protection Officer

The Data Protection Officer for both Trusts has a responsibility for all Trust information and advises on options for lawful and ethical processing of information. As such, the Data Protection Officer will be called upon for advice in relation to social media usage and any circumstances where staff may have contravened this policy in relation to Trust information.

3.6 Line Managers/Supervisors/Matrons/Ward Managers

All managerial staff across both Trusts are responsible for ensuring adequate implementation of this policy amongst all Trust staff and those within the scope of this policy.

3.7 Corporate affairs / Trust Secretaries

Corporate affairs and the Trust Secretaries are responsible for ensuring adequate implementation of this policy amongst Trust governors.

3.8 All Trust staff (including locum, agency staff, honorary contract holders and volunteers)

All staff are responsible for complying with this policy. Everyone who chooses to use social media, either for personal of professional use, must adhere to this policy and report any potential misuse of social media to line managers.

4 DEFINITION OF TERMS

Social media supports social interaction and, by definition, is highly accessible via data enabled devices. It involves online communities or networks of people sharing information, ideas and engaging in dialogue. Examples of 'social media' which are included in this policy are (but not limited to):

- social networking sites (Facebook, LinkedIn, Google+)
- blogs and micro-blogs, (Twitter, WordPress)
- content sharing websites, (Flickr, YouTube, Instagram, Prezi.com, Pinterest)
- 'wikis' (Wikipedia, LinkedIn) - websites which allow users to add, modify or delete content
- audio and video podcasts
- message or discussion applications (WhatsApp / Snapchat)
- dating websites

Further definitions of social media terms are provided in **Appendix A**.

Caldicott principles – The Caldicott Principles were developed in 1997 following a review of how patient information was handled across the NHS. The Review Panel

was chaired by Dame Fiona Caldicott and it set out six Principles that organisations must follow to ensure that information that can identify a patient is protected and only used when it is appropriate to do so. In 2013, Dame Fiona completed her second Information Governance Review and introduced a seventh principle:

- justify the purpose
- don't use personal confidential data unless it is absolutely necessary
- use the minimum necessary personal confidential data
- access to personal confidential data should be on a strict need-to-know basis
- everyone with access to personal confidential data should be aware of their responsibilities
- comply with the law
- the duty to share information can be as important as the duty to protect patient confidentiality.

5   SOCIAL MEDIA REQUIREMENTS

5.1 Standards for Trust employees

This policy applies to staff use of social media both in a personal and professional capacity and has been produced in accordance with social media guidance from a range of professional bodies (see references in section nine). All staff are reminded of their ethical duties as qualified health and social care professionals and as representatives of the NHS and should never compromise their own professional codes of conducts when using social media.

5.2 Legal responsibilities

The use of social media to share information and comment must always take account of principles outlined in the Data Protection Act 1998 (and the General Data Protection Regulation from May 2018) for personal or individually identifiable information relating to patient/service users, carers, staff or other individuals. Content posted will remain online indefinitely and, as published information, is subject to the same laws and legislation as traditional media, e.g. libel.

5.3 Organisational use of social media

Both Trusts are increasingly using social media in an organisational capacity to share information and gain valuable feedback about services and experiences. This activity is coordinated and managed by the Trusts' communication team at a corporate level. Teams must not set up social media accounts which purport to represent the views of the Trust. Any departments wishing to use social media to promote their work must liaise with the communications team via trustcomms@stft.nhs.uk or chscomms@chsft.nhs.uk.

5.4 Requirements for staff

As social media blurs the lines between personal voice and organisational voice, the following requirements for staff clarify how best to enhance and protect personal and professional reputations when using social media:

5.4.1 Responsibility as an employee

When posting on social media sites, whether or not staff have identified themselves as an employee of the Trust[1], staff must behave appropriately and in line with the Trust's wider values and policies, taking account of all relevant legislation covering personal confidentiality, e.g. The Data Protection Act 1998 (and the General Data Protection Regulation from May 2018). Every member of staff carries individual responsibility as an NHS employee, or when representing the NHS, and in line with professional codes of conduct when using social media, staff must:

- **never** reveal confidential information about patient/service users, staff or organisational business
- **never** engage in activities or comment which might bring the Trust directly into disrepute
- **never** post defamatory, derogatory or offensive comments about colleagues, patient/service users or the Trust

Staff must not display work email addresses unless in a professionally related capacity. Staff who do not directly identify themselves as Trust employees when using social media, must be aware that the content they post could still be considered as relevant to their employment with the Trust (for example by posting any racist, sexist or other derogatory remarks).

Any member of staff who brings the Trust into disrepute when using social media, for example by engaging in comments or activity which could potentially damage or undermine the reputations of other staff, the Trusts and / or public confidence in the NHS, could potentially face disciplinary action in line with the Trust's Disciplinary Procedure.

All staff should be aware that the Public Interests Disclosure Act 1998 gives legal protection to employees who wish to 'whistleblow' any concerns. The Act makes it clear that the process of 'whistleblowing' or 'speaking up' involves raising the issue internally first. Using social media to whistleblow is not considered appropriate and all staff should raise concerns through established internal channels.

Both Trusts have clear channels in place for staff to raise concerns through Freedom to Speak Up Guardians and Ambassadors. In CHSFT, employees are supported with a free, confidential Employee Assistance Programme (First Assist) and at STFT 'Listening Advisors' are in place to support colleagues. Further details can be found on both Trust intranets.

5.4.2 Think twice before posting content

Privacy does not exist in the world of social media and photographs, videos and comments can be shared easily ,even when privacy settings are set appropriately. Staff must consider what could happen if something they post becomes widely

---

[1] *For example by making reference to the Trust as your employer, by displaying **@chsft.nhs.uk**, **@stft.nhs.uk** or **@nhs.net** e-mail addresses.

known and how that may then reflect on them personally, professionally, and on the Trust. Comments can be easily forwarded, copied or photographed and staff should not post comments online that they would not say in public or in the workplace.

When attending events, awards, conferences and even in day-to-day business, the role of social media is integral, however staff must always be considerate to other colleagues by seeking verbal consent for any content to be shared and must not post information if they have been asked not to. Staff must also remove information about a colleague if that colleague asks them to do so or could potentially face disciplinary action in line with the Trust's Disciplinary Procedure.

5.4.3 Be respectful

Content on social media sites can easily encourage follow on comments or discussion of opposing ideas and staff should consider carefully how any resulting debate would reflect on them personally, professionally and on the Trust. Under no circumstance should derogatory, abusive or personal comments be made about patient/service users, Trust colleagues, Trust business, or Trust partners. This may amount to cyber-bullying and could be subject to disciplinary action.

5.4.4 Social networking sites

Social networking sites like Facebook and Twitter provide a great way for people to keep in touch but also provide opportunities for third parties to collate vast amounts of information and share ideas. Staff should be mindful of the personal information they disclose on social networking sites. Where staff associate themselves with the Trust (through providing work details or joining a Trust or NHS network/fan page), they should also act in a manner which does not bring the Trust or their profession into disrepute. This applies to both open and private sections of a site if staff identify themselves as employees of the Trust.

If anyone within the scope of this policy is contacted by the media about posts they have made on a social networking site in relation to their role, or the NHS, they must inform the communications team before responding. Equally, if an individual is contacted by a journalist who has found their contact details online and wishes to discuss their role, or the NHS, they must inform the communications team before responding.

5.4.5 Use of social media in a personal capacity during working hours

We recognise that some staff may use social media as part of their professional roles, however, personal use of social media is not permitted during working hours. The use of social media on Trust IT equipment is restricted as these sites can contain vulnerabilities that negate the effectiveness of security software and take up a lot of bandwidth on the Trust's networks.

If there is a specific business need to access such social media sites via Trust equipment, approval should be sought from the communications team and via the IT helpdesk. Authority will only be given where a clear business need is identified.

Staff using their own personal smart phone devices to access social media during working hours for personal reasons must restrict this to designated break times only i.e. during a lunch or comfort break, or outside of normal working hours (before or after a shift).

5.4.6 Commenting in online discussions

Many staff may already be actively involved with social media and comment in online discussions to give their point of view or share ideas about various areas of work. This positive professional involvement is encouraged by the Trusts but employees must always act in accordance with this policy.

5.5 Editing websites

If staff find any errors about the Trust on websites such as Wikipedia or LinkedIn please alert the communications team to agree an appropriate response before making any changes. Please note:

- If staff edit an entries themselves from Trust equipment, the source of the correction may be recorded as a NHS IP address and staff should therefore be aware of the tone and language used and not post any derogatory or offensive comments.   If correcting an error, staff must also be transparent about who they are and the capacity in which they are responding.
- Criticism of the Trust must never be removed but instead reported to the communications team who will agree an appropriate response.
- Any derogatory or offensive comments relating to the Trust must not be removed but instead reported to the communications team who will agree an appropriate response.

5.6 Professional and personal blogging

Any staff who have professional or personal blogs in relation to health and social care must inform the communications team and ensure any content is in line with this policy and the responsibilities outlined in section 5.4.1. In these cases, if a blog makes it clear that the author works for the Trust and/or the NHS, it should include a clear disclaimer such as "these are my personal views and not those of my employer". The Trust logo must never be used on personal web pages.

Personal blogs and websites must not reveal confidential information about patient/service users, other staff, or organisational business of the Trusts, for example, any aspects of the Trusts' plans, or details of internal discussions. This would be treated as a breach of confidentiality and staff could potentially face disciplinary action in line with the Trust's Disciplinary Procedure. If in doubt about what might be confidential, staff must consult the communications team. If a staff member thinks something on a blog or website gives rise to a conflict of interest or has particular concerns about impartiality or confidentiality, this must be raised via the communications team and corporate affairs. If a staff member is offered payment to produce a blog for a third party this could constitute a conflict of interest and must be discussed the communications team and corporate affairs.

5.7 Guidance around instant messaging apps

As yet, there is no clear guidance from national NHS bodies on the use of instant messaging platforms such as WhatsApp for the sharing of clinical information in a professional capacity. Work is ongoing between NHS England, NHS Digital, the Department of Health and Social Care and Public Health England to prepare guidance that will enable NHS organisations to implement policies balancing the potential risks to privacy against improvements in patient safety when using instant messaging technologies. Until this guidance is available and made clear to the NHS, under **no circumstances** should patient identifiable data or information be shared in this way.

The Trust acknowledges that many staff use tools like WhatsApp in a personal capacity and that instant messaging can have great value, however this does not replace other formal routes of communication with colleagues.

All staff are reminded that it is against the law to reveal any detail that could identify a patient via these channels and could result in the Trust receiving a large fine and the member of staff facing disciplinary action.

6   MONITORING COMPLIANCE/EFFECTIVENESS OF THE POLICY

Area for monitoring	Method	Frequency	Responsibility	Responsible group/ committee for review of results (who)	Responsible individual/ group/ for development of action plan	Responsible individual/ group/ committee for monitoring of action plan
Adherence of policy across both FTs	Review of any HR issues related to social media	Quarterly	Director of Human Resources and Organisational Development	Executive Committee (by exception through quarterly workforce report)	Deputy Director of Human Resources	Workforce Committee

7   DISSEMINATION, IMPLEMENTATION AND TRAINING

This policy will be shared via Team Brief, on both Trust intranets and via internal e-bulletins. The policy will also be promoted on desktop screensavers across both Trusts and via an easy read leaflet for staff of the 'do's and don'ts' **(see Appendix B)** which will be available on both Trust intranets, shared via internal channels and promoted through a series of staff roadshows to help people learn about social media. The HR Department will promote the awareness of policy at induction and through any relevant training programmes for managers

Whenever the policy is revised, the version published on the Trusts' Intranets will be regarded as the latest copy. All printed copies should be destroyed and then replaced. There is no specific training required in order for staff to implement this policy effectively. Any staff interested in developing their social media skills should contact the communications team.

8   CONSULTATION, REVIEW AND APPROVAL/RATIFICATION

8.1 Consultation
The following key groups, committees and departments have been consulted as part of the approval process:

- Joint Management Group
- Staff side at both Trusts
- Head of Information Governance at both Trusts
- Executive Committee

8.2 Review
The policy will be reviewed after three years following approval or earlier if any significant changes are required. The review and any revisions will be coordinated by the Communications Team.

8.3 Approval
The Trust Executive Committee approved the policy.

8.4 Ratification
The Joint Policy Committee ratified the policy.

9   REFERENCES

- General Medical Council (2013) Doctors' use of social media (click here)
- Royal College of Nursing (2015) Getting started on Twitter (click here)
- Nursing and Midwifery Council (2016) Guidance on using social media responsibly (click here)
- Royal College of GPs (2013) Social media highway code (click here)
- Health and Care Professions Council (2012) (click here)
- Public Health England (2015) Social Media Use (click here)
- Department of Health Digital guidance and best practice for the health and care system (click here)
- NHS Employers (2013) HR and Social Media in the NHS (click here)

- NHS Employers (2016) Social media guidelines and tools (click here)
- NHS Confidentiality Code of Practice (2003) – click here
- NHS Caldicott Principles (2013) – click here
- Public Interests Disclosure Act 1998
- The Data Protection Act 1998
- General Data Protection Regulation from May 2018

10 ASSOCIATED DOCUMENTATION

- IM & T Security Policy (CHSFT and STFT)
- Internet and Email Policy (CHSFT and STFT)
- Confidentiality Policy (CHSFT and STFT)
- Disciplinary Policy (CHSFT and STFT)
- Raising Concerns at Work (Whistleblowing) Policy (CHSFT and STFT)
- Telephone and Mobile Phone Policy (CHSFT and STFT)
- Media Relations Policy (CHSFT and STFT)
- Standards for Business Conduct Policy (CHSFT and STFT)

11 APPENDICES

- Appendix A (Glossary of social media terms)
- Appendix B (Do's and don'ts for staff)

Appendix A – Glossary of Social Media Terms

Avatar	A picture or graphic used to represent you
Blogs	A publishing platform that allows you to post content. WordPress and Blogger are such platforms
Bitly	A URL shortening service, particular used for Twitter
Engagement	The interaction between people and brands on social networks. For example on Facebook it would be comments, likes and shares
Facebook	The world's most popular social networking site allowing you to connect with friends and businesses all over the world and post a range of content, including photos and videos
Facebook Live	Allows you to share live video with followers and friends
Facebook Messenger	Sometimes called 'Messenger'. An instant messaging service that allows you to chat with friends
Filter	A photographic effect that can be used to enhance images on social media. Popular filters can be found on snapchat and instagram
Flikr	An image and video hosting website
Friends	People you connect with on Facebook. You can also connect with friends on Snapchat
Follow / Follower	When you follow someone you subscribe to their posts and updates
GIF	Graphics Interchange Format – a file that supports both static and animated images
Hashtag	A single word or phrase preceded by # to group messages by subject or topic. Originally used on Twitter, but now used on most other social platforms
Handle	On Twitter your handle is the name you choose to represent yourself. It starts with a @
Hootsuite	A dashboard that allows you manage various social media accounts in one place
Influencer	A social media user that has credibility on a topic, trend or product. Usually can access large audiences
Instagram	A platform to share pictures and videos and apply filters to them
Instagram stories	A series of photos or videos that appear on your Instagram feed for 24 hours
Like	A like is an endorsement. You can like a page, post, photo, video etc
LinkedIn	Social network platform for businesses and professionals to make connections and share content
Lists	A curated group of Twitter accounts. You can make your own lists or subscribe to lists created by others
Live Streaming	Live broadcasting through social media
Mention	Tagging another user's handle or account in a social media message
Messenger Bots/Chatbots	Chatbots are computer programs that mimic conversation with people using artificial intelligence
Newsfeed	A list of posts on a particular social media platform

Notification	A message or update sharing new social media activity e.g. like / comment
Paid Social Media	When you pay to advertise on social media
Pinned Tweet / Post	Content that can be pinned to the top of your profile page. Great for important information or announcements
Retweet	A tweet that is re-shared to the followers of another user's Twitter account
Share	The main focus of social media is to share content. Sharing options can also be added to websites as a way of allowing people to forward information
Snapchat	Image messaging app where images sent only last up to 10 seconds
Snap	An image sent via snapchat
Snapchat story	The "My Story" section allows users to post a replayable Snap for up to 24 hours to their friends and followers.
Trending	Refers to a topic that is especially popular on social media. Users add hashtags to particular words to join in discussions
Troll	Someone who deliberately tries to offend or abuse people on social media
Tumblr	A popular microblogging platform
Twitter	A platform for posting messages with up to 140 characters.
Tweet	A message posted on Twitter
Viral Marketing	A marketing technique where information is passed electronically from one online user to another
Virtual Reality	**A three-dimensional, computer generated environment** which can be explored and interacted with by a person
Vlogger	Someone who creates and broadcasts a video blog
Whatsapp	A free instant messenger app for smartphones
YouTube	A video sharing website where you can view, upload and share video clips

Appendix B – Do's and don'ts for staff

DOs

- Do think before you post and ask yourself 'is this something that I would be happy to say in front of my colleagues and line manager?'

- Do follow the general standards of behaviour expected by all Trust employees. Familiarise yourself with our IT and social media policies, as well as those that cover respect and consideration, safeguarding and equality and diversity. These can all be found on the intranet. Abuse of these policies could lead to disciplinary action or even dismissal.

- Do feel free to get involved in local and national NHS communities that discuss healthcare. You can build strong professional networks, share best practice and get new ideas for your own role.

- Do like and follow our corporate social media accounts and get involved in the conversation or tag us if you want us to share something.

- Do familiarise yourself and regularly review your privacy settings for different social media sites and ensure your content is protected so that patient/service users do not have unrestricted access to personal information about you.

- Do look at the guidance available from your own professional body or regulator. Much more specific advice for most NHS professions can be found on the NHS Employers website [here.](#)

- Do understand the policy around accessing social media sites from Trust PCs. Some sites will be blocked or restricted. This will be outlined in our IT acceptable use policy.

- Do contact the communications team for advice if you are contacted by the media/journalists about any of your social media posts. (Please refer to the Trust's Media Relations Policy).

- Do be aware of the risk of posting content on the web (whether in a personal or professional capacity) as the information is in the public domain and anything you post could be used by the media.

- Do be conscious at all times of who has access to your personal material online and how widely this content may be shared.

- Do be aware of your own ethical obligations as a qualified health or social care professional under the code of conduct of your own professional body when using social media.

- Do be aware that inappropriate photographs, videos, comments or descriptions of your personal activities could bring both you and the Trust into disrepute and

that this could be considered a disciplinary matter and impact your professional standing.

DON'Ts

- Don't accept friend requests from current or former patient/service users outside of your normal personal social circle. Instead politely refuse and explain that it would be inappropriate.

- Don't post any personal identifiable information about patient/service users or colleagues on social media sites – this includes any relatives whilst they are patients/service users of the Trust without their verbal consent. If asked to remove content after it has been posted please do so.

- Don't post any derogatory, defamatory, abusive or inflammatory comments about the Trust, colleagues, patients or others who work for the Trust because this will potentially lead to disciplinary action. If you are unhappy about someone else's post, don't respond just report it to the Communication Team. Similarly, if you have an issue about any aspect of your working life or working area, please discuss it with your line manager and not online.

- Don't access social media for personal reasons at work unless you are on a break.

- Don't portray that you are speaking on behalf of the Trust in any post online. You should make it clear that your views are personal and purely your own. The Trust will not be held liable for any repercussions that your own content generates.

- Don't engage in any informal discussions with patient/service users about their care on social media sites.

- Don't post any photographs or videos of patient/service users or colleagues without their verbal consent. If asked to remove content after it has been posted please do so.

- Don't post any photographs or videos of yourself in situ at work unless you have verbal consent from those in the picture or video. Please ensure there is no patient identifiable information.

- Don't allow patients/service users to take or post any photographs or videos of you at work without your full verbal consent and your full understanding of the context of the post. If you are concerned, contact the communications team via switchboard.

Tips when using instant messaging apps for personal use
- ✓ Do – set your device to require a passcode
- ✓ Do – switch on additional security settings such as two-step verification

- ✓ Do – be aware when signing up to WhatsApp or other instant messaging apps that your personal information will be gathered and may be shared with other third parties
- ✓ Do – set message notifications to private and disable banners on your device's lock-screen
- ✓ Do – ensure you are communicating with the correct person or group, especially if you have many similar names stored in your personal device's address book
- ✓ Do – take care when selecting the membership of the group if you are an instant messaging group administrator, and review the membership periodically

Appendix C – Equality Impact Assessment Screening Form

City Hospitals Sunderland NHS Foundation Trust
South Tyneside NHS Foundation Trust

Equality Impact Assessment Screening Form

The following screening document will ask you to identify any potential risks or negative impacts to each of the equality strands. Background data will help to identify these potential risks. If there is no data available then you cannot assume that there is no risk. In these circumstances you may need to carry out some further investigations before you can carry out the Equality Impact Assessment.

New		Proposed		Existing		Date of implementation		Date of Review	
Name of policy:						Social Media Policy			
Aim of policy:						This policy outlines the procedures which must be followed with regard to social media use.			
Directorate:						Communications			
Manager(s) completing assessment:						Liz Davies			
Date:						14 June 2018			
Does this policy have a direct impact on service users/public or staff? Yes or No						Yes			

Patients, Community or staff groups by equality strands	Impact/Risk (Yes/No)	Comments
Age Is there a risk that older people or younger people would have problems adhering to this policy?	No	
Disability Is there a risk that staff with a disability would have problems adhering to this policy?	No	
Gender Reassignment Is there a risk that the policy discriminates against employees who may be starting or have completed a process to change their gender?	No	
Marriage and Civil Partnership Is there a risk that the policy discriminates against employees on the grounds of their marital status / civil partnership?	No	
Pregnancy and Maternity Is there a risk that women who are pregnant or who have recently given birth would not be able to adhere to the policy?	No	
Race Is there a risk that the policy discriminates on the grounds of race, including colour, nationality, ethnicity or national origin?	No	
Religion or belief Is there a risk that people practicing different religions or beliefs would have problems adhering to this policy?	No	
Sex Is there a risk that the policy discriminates on the grounds of sex?	No	
Sexual orientation Is there a risk that people who are lesbian, gay or bisexual would have problems adhering to this policy?	No	

If the response to any of the above is "Yes" please contact the Trust's Equality and Diversity lead for further guidance: CHSFT – austin.omalley@chsft.nhs.uk   STFT – sonia.atkinson@stft.nhs.uk

(**Please tick as appropriate**):

[X] Full EIA is not required to be carried out on this policy as it is not relevant to any of the equality duties

[   ] Full EIA is required to be carried out on this policy as it is relevant to some/all of the equality duties