Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

SOCIAL MEDIA AND RECORDINGS FOR NON-CLINICAL PURPOSES POLICY

POLICY

Reference	GV/009		
Approving Body	Executive Team Meeting		
Date Approved	8th June 2022		
For publication to external SFH website	**Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:**		
	YES	**NO**	**N/A**
	x		
Issue Date	June 2022		
Version	3		
Summary of Changes from Previous Version	New version of the current Social Media Policy which follows the correct protocol and guidance.		
Supersedes	Version 2.2		
Document Category	Governance		
Consultation Undertaken	Director of Corporate Affairs		
Date of Completion of Equality Impact Assessment	21/04/22		
Date of Environmental Impact Assessment (if applicable)	Not Applicable		
Legal and/or Accreditation Implications	None		
Target Audience	All Staff		
Review Date	30/05/25		
Sponsor (Position)	Associate Director of Communications and Chief Executive		
Author (Position & Name)	Head of Communications, Richard Brown		
Lead Division/ Directorate	Corporate		
Lead Specialty/ Service/ Department	Communications Department/ Human Resources / Information Governance Manager		
Position of Person able to provide Further Guidance/Information	Head of Communications		

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
Not Applicable	*Not Applicable*

CONTENTS

Item	Title	Page
1.0	INTRODUCTION	3
2.0	POLICY STATEMENT	4
3.0	DEFINITIONS/ ABBREVIATIONS	4
4.0	ROLES AND RESPONSIBILITIES	5
5.0	SCOPE	6
6.0	APPROVAL	6
7.0	DOCUMENT REQUIREMENTS	6
8.0	REPORTING INAPPROPRIATE BEHAVIOUR ON SOCIAL MEDIA	10
9.0	EVIDENCE BASE	10
10.0	MONITORING COMPLIANCE AND EFFECTIVENESS	11
11.0	TRAINING AND IMPLEMENTATION	11
12.0	DISTRIBUTION	11
13.0	COMMUNICATION	11
14.0	IMPACT ASSESSMENTS	11
15.0	EVIDENCE BASE (Relevant Legislation/ National Guidance) and RELATED SFHFT DOCUMENTS	12
16.0	APPENDICES	12

APPENDICIES

Appendix A	*Potential Risks to the Trust of Staff Using Blogging and Social Networking*	13
Appendix B	*Staff Guidance on the Use of Social Media Sites*	15
Appendix C	*Communications by Employees*	17
Appendix D	*Consent Form for Non-Clinical Recordings*	19
Appendix E	*Social Media Account Request Form*	20
Appendix F	*Equality Impact Assessment*	22

1.0 INTRODUCTION

1.1 Sherwood Forest Hospitals NHS Foundation Trust (the Trust) aims to be a dynamic organisation embracing new technologies and ways of working. The rise of social media is changing the way we, and every organisation in the world, conduct our business. Millions of people use social media responsibly every day and it is an increasingly important communications tool.

1.2 In recent years the Trust has increased its use of social networks to engage with staff, patients, service users and other stakeholders, and to deliver key messages for good healthcare and services. Online digital communications are used by the Trust's Communications Team to further extend its interactions and their use is likely to be further extended as new communications channels become available.

1.3 There is a large range of social media platforms available, including but not limited to Facebook, Instagram, LinkedIn, WhatsApp, Snapchat and Twitter. Many staff use these in their own time, using their own computers and smartphones. In addition to personal use, for many, this is an important channel for professional communication.

1.4 The Trust wishes to continue to encourage use of social media as a way to engage with patients, carers, the public, staff and stakeholders. Use of personal devices, as well as Trust devices, is permissible by staff but they should be aware that existing professional codes of conduct and terms and conditions of employment apply to the publishing and sharing of potentially sensitive, confidential information about the Trust and our patients.

1.5 Fundamentally, existing information governance rules apply. Sensitive personal and confidential information about patients and their care should never be revealed to third parties unless it is necessary to ensure safe, effective and appropriate care. This principle is already part of your terms and conditions of employment and applies to all forms of communication – not just social media.

1.6 This policy is necessary, as many employees enjoy sharing their knowledge, learning and experience with others of similar roles and interests. The Trust acknowledges these online activities and staff and contractors can improve their personal skills and experience through relevant interactions with others outside the organisation.

1.7 This policy documents that every staff member has permission to use social media at work for work purposes. It sets out our expectations of you when you do so and what you can expect from us.

1.8 This policy is provided so that all staff, either directly employed or employed by the Trust on behalf of a third party organisation, are aware of their personal responsibilities for appropriate use of social media facilities they may access.

1.9 The Trust has a responsibility to ensure the operational effectiveness of its business, including its public image, reputation and for the protection of its varied information assets. This involves ensuring confidentiality, appropriateness and maintaining security in accordance with the Trust's information governance policies, human resources policies, UK legislation and best practice guidance.

1.10 This policy is issued and maintained by the Head of Communications on behalf of the Trust, at the issue defined on the front sheet, which supersedes and replaces all previous versions.

2.0 POLICY STATEMENT

2.1 This policy is provided so that all staff, either directly employed or employed by the Trust on behalf of a third party organisation, are aware of their personal responsibilities for appropriate use of social media facilities they may access.

2.2 The Trust is committed to preventing discrimination, valuing diversity and achieving quality of opportunity. No employee will receive less favourable treatment on the grounds of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation or on the grounds of trade union membership.

2.3 The following policies are relevant to this policy and should be read in conjunction with this policy:

- Confidentiality Policy
- Whistle-blowers Policy
- Acceptable Use of the Internet and Email Policy
- Disciplinary Procedures
- Information Governance Policy
- Information Governance Management Framework
- Information Security Policy
- Electronic Remote Working Policy
- Photography and Video Recording Policy (Camera Policy)
- Media policy

3.0 DEFINITIONS/ ABBREVIATIONS

3.1 Definitions for specific terms used in the policy are clarified below:

The Trust: Means Sherwood Forest Hospitals NHS Foundation Trust

Staff: Means all employees of the Trust including those managed by a third party organisation on behalf of the Trust

NHIS: Nottinghamshire Health Informatics Service

Social Networking: The term commonly given to websites and online tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests. It involves building communities or networks, encouraging participation and engagement. Popular examples include Facebook, Twitter and Linkedin, WhatsApp, Snapchat and Instagram.

Social Media: The term commonly used for web-based and other mobile communications technologies that enable messages and opinions to be shared in dialogue with others who often share the same community interests.

Clinical recordings: These are made as part of a patient's care and should not be divulged to third parties unless it is necessary for their care.

Non-clinical recordings: These are any recordings (photographic, video, audio) that are not directly related to a patient's care – that is, for promotional, editorial, marketing purposes.

Social Engineering: The method whereby an attacker uses human interaction (social skills) to deceive others to obtain information about an organisation and its information assets. An attacker may potentially masquerade as a respectable and plausible person claiming bona fide interest in the information concerned e.g. posing as a member of the organisation or maintenance contractor etc.

Blogging or Tweeting (micro-blogging): Using a public website to write an online diary (known as a blog) or sharing thoughts and opinions on various subjects. Blogs and tweets are usually maintained by an individual with regular entries of commentary, descriptions of events, and may include other material such as graphics or video.

4.0 ROLES AND RESPONSIBILITIES

4.1 All members of staff will read and note the contents of this policy and must have access to and must follow the guidance outlined in the Trust's policies and procedures.

4.2 All staff are responsible for ensuring that no actual or potential information breaches occur as a direct result of their actions.

4.3 The Trust will investigate all suspected/actual information breaches and report through their incident reporting procedures.

4.4 Staff who become aware of an actual or potential information breach or communications that has the potential to damage the reputation of the Trust, have a responsibility to report it immediately to their line manager, HR and the Communications Team.

4.5. The Communications Team is responsible for updating this policy.

5.0 SCOPE

5.1 The policy applies to all employees employed on Agenda for Change terms and conditions of service, to temporary workers/contractors/agency workers, students on placement, apprentices, volunteers, and staff covered by Medical & Dental conditions of service.

6.0 APPROVAL

6.1 The consultation process for this policy is as follows:

Staff Communications and Engagement group

7.0 DOCUMENT REQUIREMENTS

7.1.1 Duties and Responsibilities – Private Use of Social Media

7.1.2 Staff should be aware that the Trust reserves the right to use legitimate means to scan the web, including social networking sites for content that it finds inappropriate. The Trust also reserves the right to monitor staff usage of social networking sites during work time.

7.1.3 Staff are encouraged to support the Trust by re-tweeting or sharing social media content published by the Trust's social media channels. However, if doing so, in line with the Royal College of Nursing (RCN) guidelines "RCN Legal Advice on using the internet" staff should state that they are tweeting/blogging etc. in a personal capacity. All staff are expected to behave in accordance with their professional duties standards, which may also offer guidance around acceptable media and social media behaviours when representing the Trust. For example the Nursing and Midwifery Council, Health and Care Professions Council and General Medical Council all have standards they expect their representatives to adhere by. There are also the SFH specific values and behaviours which all of us in #TeamSFH should display, and there may be other professional guidelines which may apply to you. At all times staff must consider how their behaviour may impact on their colleagues, their patients and their patients' families.

7.1.4 Staff are ultimately responsible for their own online behaviour both during and outside of designated working hours. Staff must take care to avoid online content or actions that are inaccurate, libellous, defamatory, discriminatory, harassing, threatening or may otherwise be illegal. Staff should be aware that failure to adhere to this policy may be viewed as gross misconduct and action will be taken in line with Trust disciplinary procedures, which may lead to dismissal. It is also possible for staff to be subject to civil proceedings or criminal prosecution.

7.1.5 Staff are not authorised to communicate by any means on behalf of the Trust unless this is an accepted normal part of their job, or through special arrangement that has been approved in writing in advance by the Head of Communications. No social media sites or pages relating to the Trust should be set up by staff without prior approval from the Communications Team (See Appendices B and C).

7.1.6 Staff who use social media must not disclose information that is of a sensitive or confidential nature e.g. person identifiable information regarding other staff or patients, or that is subject to a non-disclosure contract or agreement. This applies to information about patients, service users, other staff and contractors, other organisations, commercial suppliers and other information about the Trust and its business activities.

7.1.7 Corporate logos or other visible markings or identifications associated with the Trust may only be used for official business related to the Trust.

7.1.8 Staff must not share details of the Trust's implemented security or risk management arrangements. These details are confidential, may be misused and if circumvented could lead to a serious breach of security.

7.1.9 Staff who may not directly identify themselves as Trust staff members when using social networking sites for personal purposes at home should be aware that the content they post on social media sites could still be construed as relevant to their employment with the Trust.

7.1.10 Unauthorised disclosure of confidential information would constitute gross misconduct and will be dealt with in accordance with the Trust's disciplinary procedure which may lead to dismissal.

7.1.11 When using social networking sites, staff should respect their audience. Staff should not make any detrimental comments about anyone while using social media sites, e.g. failing to show dignity at work (harassment), discriminatory language, personal insults and obscenity
.

7.1.12 If employees are contacted directly or indirectly by the press about a post in a group or other social media environment, they must notify their line manager as soon as possible and contact the Communications Team directly. Members of staff should not respond in any way to media requests that they receive directly. These must be referred to the Communications Team.

7.1.13 The Trust may also take disciplinary action, if necessary, against any staff member who brings the organisation into disrepute by inappropriate disclosure e.g. comments and photographs on social networking sites or personal internet sites.

7.2 Non Clinical Recordings – Photographs / Audio / Video

7.2.1 Clinical recordings are made as part of a patient's care and should not be divulged to third parties unless it is necessary for their care.

7.2.2 For all non-clinical recordings (that is, recordings other than those required for clinical purposes or those listed in section 5.9 of the trust's Photography and Video Recording Policy Camera Policy), consent from the subject of the recording needs to be obtained using the consent form below in Appendix D.

7.2.3 The consent form (Appendix D) should be completed before recordings take place. Advice and guidance is available from the communications team.

7.2.4 If in clinical areas (e.g. wards, out-patient clinics and waiting areas), patients, friends and relatives, as well as staff, should only take non-clinical recordings (including photographs for social media purposes) after seeking permission from the Communications Team. Care must be taken that no inappropriate information is

included in the recordings (patient records and other identifiable material) and no one is featured in a photograph unless they have completed a consent form and are fully aware of the reason for the recording and its use under GDPR guidelines.

7.2.5 Non-clinical areas of the hospital include the main entrance, grounds and other areas open to the general public. If in these areas, patients, friends and relatives, as well as staff, should only take recordings (including photographs for social media purposes) after seeking permission from the Communications Team. Care must be taken that no inappropriate information is included in the recordings (patient records and other identifiable material) and no one is featured in a photograph unless they have gained appropriate consent and are fully aware of the reason for the recording and its use.

7.2.6 Confidentiality and the right to privacy. Trust staff are already required to adhere to confidentiality and privacy rules and conditions in their professional codes of conduct and those stated in terms and conditions of employment. All these apply when using social media. That is, patients should be treated with dignity and existing rules of confidentiality apply at all times.

7.2.7 There will be times when it is appropriate for the Communications Team to take recordings at Trust sites for social media purposes. Everyone involved should be made aware of the purpose and context of the recording and if they do not wish to take part this must be respected. This applies to anyone pictured and is identifiable without their knowledge (in the background of a photograph, for example) who might not wish to be featured on social media. Accidental recordings of patients who have not given appropriate consent are not acceptable. The Communications Team will review any content in recordings before posting.

7.2.8 It is up to individual members of staff to ensure they are fully conversant with this social media policy.

7.2.9 Consent from members of staff must not be assumed. You must obtain their written agreement explaining how the material will be used and keep a record of their consent where possible and they must be given an opportunity to make a choice and any refusal should be respected.

7.2.10 Freelance professional photographers / videographers may only be introduced to the Trust by the Communications Team. It will be the responsibility of the member of that team introducing them to ensure they behave in line with all Trust policies.

7.2.11 The Trust has no control over the use of material taken by external agencies, such as newspapers and TV companies, either now or in the future. All copyright belongs to the external agency, which retains the right to re-use, broadcast, publish and re-distribute the material worldwide in the future, without seeking further consent.

7.2.12 The use of cameras, or the camera and recording facility available on most modern mobile phones, is strictly forbidden on Trust premises without the explicit approval of the Communications Team, as this could inadvertently breach patient confidentiality. Patients and visitors are not permitted to use their mobile telephone (or any other recording device) to photograph or record other patients, staff or the Trust's premises during their stay/visit in hospital, without the permission of the Communications Team. Members of the public found filming inappropriately either inside or on the Trust's

ground will be asked to delete any content and will then be escorted from the premises by security.

7.2.13 Sometimes patients or relatives may film, or threaten to film, their surroundings and threaten to take the footage to the media and/or post on social media sites. This obviously poses a patient confidentiality risk to others around them. If staff become aware of this it is advised they should approach the person, with a colleague if they prefer, to ask them politely to stop filming and/or to ask them to delete the footage from their camera/phone. They should explain that others are entitled to patient confidentiality and this may be breached. On no account should staff put themselves at risk or take the phone/camera from the person and attempt to delete it themselves. Afterwards note in the patient notes the conversation has taken place and inform the clinical lead and Communications Team.

7.3 Duties and Responsibilities - Trust Use of Social Media

7.3.1 The Trust has a corporate presence on social media. If staff wish to convey news stories, events or messages through these channels, they should contact the Communications Team. Requests for any new team specific accounts must come through the Communications Team, and areas will need to demonstrate that they have a clear strategy for implementing, growing and managing accounts they request, including succession planning and managing risk (see Appendix E).

7.3.2 It is acknowledged that the use of closed social media groups including (but not limited to) WhatsApp and closed Facebook Group accounts are useful for communicating within teams. However, please adhere to the following NHSI guidance: “Don't put patient, sensitive or security classified information on social media [which includes messaging apps like WhatsApp]; this would breach data protection laws or patient confidentiality and result in a security incident." It is also expected that within closed social media groups that staff keep to the Trust’s values and behaviours as on other social media outlets.

8.0 REPORTING INAPPROPRIATE BEHAVIOUR ON SOCIAL MEDIA

8.1 If a member of staff witnesses information contained on social media sites that contravenes this policy, including closed social media sites such as (but not limited to) WhatsApp or closed Facebook groups, they should report the issue through the Trust incident reporting process and their line manager and the Communications Team.

8.2 All incidents will be investigated by the appropriate division with support provided by the information governance team and the human resources department where necessary.

9.0 EVIDENCE BASE

9.1 The legal obligations of the Trust and the NHS as a whole can be found in the NHS Information Governance Guidance on Legal and Professional Obligations (DH, 2007) which is available on the internet and this policy must be read in the context of and with reference to these legislations and guidance.

10.0 MONITORING COMPLIANCE AND EFFECTIVENESS

10.1 The Trust reserves the right to use legitimate means to scan the web, including social media sites for content that it finds inappropriate.

10.2 The Trust reserves the right to monitor the use of social media sites during working hours.

10.3 A review of this policy will be conducted every two years or following a change to associated legislation and/or national guidance or national/local terms and conditions of service.

10.4 The responsibility for this policy and staff guidance is delegated to the Head of Communications.

11.0 TRAINING AND IMPLEMENTATION

11.1 It is the responsibility of the Trust to ensure that mandatory training and induction programmes are implemented to ensure the awareness of all staff with regard to Trust policy and procedure.

11.2 It is the responsibility of all line managers to ensure that their staff attend mandatory information governance training on an annual basis, and pro-actively encourage compliance with this policy.

12.0 DISTRIBUTION

12.1 The policy, once approved, will be included within the Corporate Information section of the Trust's intranet.

13.0 COMMUNICATION

13.1 On approval the policy will be communicated to all existing staff via Staff Brief, the weekly staff bulletin and the Trust's intranet for implementation purposes.

13.2 New members of staff will be informed of the policy at induction and by their line managers.

14.0 IMPACT ASSESSMENTS

This document is not subject to an Equality Impact Assessment or Environmental Impact Assessment.

15.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:

- Not Applicable

Related SFHFT Documents:

- Not Applicable

16.0 APPENDICES

- Appendix A – Potential Risks to the Trust of Staff Using Blogging and Social Networking
- Appendix B – Staff Guidance on the Use of Social Media Sites
- Appendix C – Communications by employees
- Appendix D – Media recording consent form
- Appendix E – Social Media account request form
- Appendix F – Equality Impact Assessment

APPENDIX A - POTENTIAL RISKS TO THE TRUST OF STAFF USING BLOGGING AND SOCIAL NETWORKING

1. A range of potential risks and impact consequences exist that staff should be aware of:

Unauthorised disclosure of business information and potential confidentiality breach Blogging and social networking sites can provide an easy means for sensitive or confidential information to leak from an organisation, either maliciously or otherwise. Once loaded to a blogging or social networking site, Trust information enters the public domain and may be processed, stored and reused anywhere globally. In short, Trust control can be lost and reputational damage can easily occur. Although closed groups can be created in some social media applications and can prove useful for work-related discussion and communication, they should not be regarded as secure and so should never be used for communicating sensitive, confidential or patient identifiable information.

2. Malicious attack associated with identity theft

Most blogging and social networking sites allow users to create a personal profile. People often place a large amount of personal information on social networking sites, including photographs, details about their nationality, ethnic origin, religion, addresses and date of birth, telephone contact numbers, and interests. This information may be of use to criminals and others who are seeking to steal or reuse identities or who may use the information for social engineering purposes.

3. Legal liabilities from defamatory postings etc. by staff

When a person registers with a website they typically have to indicate their acceptance of the sites terms and conditions. These can be several pages long and contain difficult to read and understand legal jargon. Such terms and conditions may potentially give the site ownership and third party disclosure rights over content placed on the site, and could create possible liabilities for the Trust. For example, where a staff member is registering on a website from a computer/electronic device within the Trust, it may potentially be assumed that the user is acting on behalf of the Trust and any libellous, inflammatory or derogatory comments may result in civil litigation or

criminal prosecution. In addition, information being hosted by the website may be subject to other legal jurisdiction overseas and may be very difficult to correct or remove.

3.1 Reputational damage

Ill-considered or unjustified comments left on sites may adversely affect public and professional opinion toward an individual, their employer or another implicated organisation, contractor, service provider or business partner etc. This can lead to a change in social or business status with a danger of adverse consequential impacts and possibility of legal proceedings.

3.2 Malicious code targeting social networking users causing virus infections and consequential damage to end user devices

Blogging and social networking sites may encourage or require the download and installation of additional code in order to maximise the sites functionality and potential values. Where such sites have weak or ineffective security controls it may be possible for its operating system or application code to be changed to contain malicious content such as viruses and trojans, or to trigger unintended actions such as phishing – a way of obtaining sensitive information through bogus impersonation as a trustworthy entity.

3.3 Systems overload from heavy use of sites with implications of degraded services and non-productive activities

Blogging and social networking sites can pose threats to an organisation's own information infrastructure. Particularly as the use of rich media (such as video and audio) becomes the norm in such sites, the network bandwidth consumption generated by these sites can be significant and they have the potential to be the biggest bandwidth consumers within an organisation. In an aggregated sense widespread use of blogging and social networking sites may introduce new capacity issues for local and national NHS infrastructure and services.

3.4 Staff intimidation or harassment with the possibility of personal threat or attack against the blogger, sometimes without apparent reason

Other online bloggers can hold strong views and may potentially be offended at what they read, however unlikely or unintended that might seem. In extreme cases this negative reaction could lead to a targeted attack or assault against the original blogger with potential to cause them anxiety, distress and personal safety issues.

APPENDIX B - STAFF GUIDANCE ON THE USE OF SOCIAL MEDIA SITES

This guidance should be read in conjunction with the Trust's Acceptable Use of the Internet and Email Policy.

How to avoid problems with blogging and social networking sites

1. If uploading multimedia content to an external social media site, be sure it represents the values and behaviours of the organisation. Everyone in the multimedia content must give their consent for the content to be used within a social media environment.

2. As the voice of the Trust, employees are responsible for ensuring that any multimedia content posted is appropriate and is in keeping with Trust's values and behaviours. Ensure that content:

   - Does not breach an individual's privacy, dignity and confidentiality.
   - Is in keeping with your role in the organisation and does not compromise your own reputation or that of the Trust.
   - Is not likely to provoke, attack or offend others.
   - Is not racist, sexist, homophobic, sexually explicit, abusive, offensive or otherwise objectionable.
   - Does not break the law or otherwise condone or encourage unlawful activity.
   - Does not appear to impersonate someone else.
   - Does not describe or encourage activities which could endanger the safety or well-being of others.
   - Is not seen to support any political party, cause or religious view.

3. Some social media sites allow people to be tagged, or flagged for ease of identification. This should be used with caution. While it is generally ok to tag in other organisations, when tagging in individuals bear in mind that it may lead to the blurring of boundaries between professional and personal use or the unintentional exposure of an individual's personal information to a wider audience.

4. When registering with a website, understand what you are signing up to by reading the terms and conditions carefully and determine what security, confidentiality and liability claims, undertakings and exclusions exist. If in any doubt seek the advice from the information governance and/or communications team.

5. Be careful about the personal details you post online such as contact details, date of birth, your profession, your organisation. Such information could put you at risk of identity fraud.

6. Think about what you want to use your online profile for, applying appropriate security and preference settings as necessary.

7. Keep your password safe and avoid obvious ones that others might easily guess.

8. Be aware of your personal responsibility for the words you post and also for the comments of others you allow on your blog or webpage.

9. Avoid un-attributable, anonymous comments.

10. Be suspicious of all unsolicited contacts. This can include phone calls, visits, , email, SMS (Short Message Service) text messages, WhatsApp messages etc., from anyone asking for information about other staff, contractors, patients, service users or other potentially confidential information.

11. Where a new contact claims to be a legitimate member of staff or a business partner organisation, ensure you take steps to verify their identity and business needs directly with their department head or other organisation.

12. Do not provide information about your organisation, its service users or other individuals including structures and networks unless you are certain of the recipient's identity and their authority to have access to that information. Check that the intended recipient has appropriate information governance arrangements in place to handle any information disclosed to them.

13. Avoid disclosing personal or sensitive information by email. Where this is necessary ensure the recipient's email address is verified and legitimate, and that appropriate data encryption standards are used for patient/client and other sensitive information. If in doubt please contact the NHIS Service Desk for further advice.

14. Do not send personal or other sensitive information over the internet unless this has been approved by your line manager and the information governance department.

15. In the event that you think you may have been a social engineering victim ensure you immediately report this as an incident in accordance with the Trust Incident Reporting Policy. Additional advice can be provided by the information governance team and/or human resources department where necessary. It is possible that a notice may be issued to other staff within the Trust with appropriate guidance to be alert to any new, unusual or suspicious activity.

APPENDIX C - COMMUNICATIONS BY EMPLOYEES

- The Communications Team must be involved in all trust-produced campaigns on social media, as it has responsibility for external communications.
- Written permission must be requested from the Communications Team before developing a Trust project presence in any form of social media. This includes the setting up of any social media accounts associated with the Trust. Requests to use additional social media channels other than the Trust's corporate accounts must be made to the Communications Team by filling in the Social Media Request form (appendix E)
- You must respect copyright, fair use and financial disclosure rules.
- You must observe professional codes of conduct whilst representing the Trust online.

SOCIAL MEDIA DOs AND DON'Ts

Sherwood Forest Hospitals recognises the value social media platforms such as Facebook, LinkedIn, Instagram and Twitter can bring to its employees. We are aware many staff use social media networks in their own time, using their own computers and smartphones.

Every staff member has permission to use social media at work for work purposes. Social media offers some great ways to really grow your professional network, discover new ideas, share learning and best practice, and take your career to the next level.

However, it is the responsibility of everyone within the Trust to use social media responsibly. Although members of staff are not acting on behalf of the organisation when using social media they must be mindful that their online posts could potentially be damaging to the Trust if they are inaccurate or flippant.

Please remember that when you use these sites, as Trust employees, you are encouraged to maintain standards of professionalism and may be held to account for any inflammatory, derogatory, slanderous or abusive statements. Just as we do not tolerate bullying in real life, we will not tolerate it online. Such activity can amount to misconduct and employers will need to take disciplinary action for inappropriate behaviour exposed by social media or inappropriate comments made on social media.

Please consider what you do, who you work for and who this affects before you post anything online and check these handy dos and don'ts.

DO

- Think! Would I be happy saying this to my mother/boss/local police officer or a journalist?
- Be safe – Never give personal information to others via the internet.
- Celebrate success and good practice - if you and your team have done something great then let people know. Make sure posts are doing something positive, providing worthwhile information or engaging key stakeholders in worthwhile dialogue.
- Keep your comments light and positive. If you cannot, then it is probably best not to comment at all.
- Take responsibility for anything you publish, be that in a personal or Trust-endorsed capacity.
- Ensure it is good use of your time – remember your day job. Ensure your social media activities do not interfere with your main clinical or corporate commitments.
- Use social media responsibly and read the Trust social media policy.
- Be open about who you are and be clear that your views are your own, and not those of the Trust.
- Respect copyright laws and credit the work of others. Always seek permission if citing or referencing someone else's work or website. Where a reference is made, link back to the original source material.
- Think "does this reflect badly on the Trust, the hospitals or our staff?" If it could, don't post. If you have any doubts, don't post.

DON'T

- Post anything that could damage the Trust, its brand or its reputation.
- Post photographs of patients, their families and carers, visitors or staff without making sure they are happy to be involved (gain appropriate consent).
- Publish fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise unlawful or inappropriate information or footage that would be offensive to readers of the submission or would otherwise breach any Trust Policy or break the law.
- Publish confidential information (business or personal) about or acquired from the Trust.
- Criticise or cause embarrassment to the Trust, its patients, healthcare partners, other stakeholders or staff in a public post (including any website).
- Use social media to share training materials or footage unless they have been correctly signed off by clinical governance and meet all the necessary legal requirements.
- Retweet or repost information which you would consider libellous or a breach of our social media policy – even if you did not write the original content you are still liable if you share or repost/retweet.
- Set up any Trust group or account without the express permission of the Communications Team. If in doubt, ask a member of the communications team or email sfh-tr.communications@nhs.net.
- Respond directly to media if they approach you via social media.
- Do not enter into a debate or conversation in social media sites with individuals criticising the Trust policy, treatment or individuals. You should instead alert the Communications Team who can handle the comments appropriately on behalf of the Trust
- In the event of a major incident involving the Trust and/or its partners, do not comment directly but re-tweet official statements from the organisation's main social media accounts. This will avoid misinformation being inadvertently shared at critical times.

APPENDIX D – CONSENT FORM FOR NON-CLINICAL RECORDINGS

The current consent form can downloaded here.

APPENDIX E – SOCIAL MEDIA ACCOUNT REQUEST FORM

Please complete the below form if you would like access to a SFH social media account, wish to submit posts on one of the official SFH social media accounts or want to apply to formally contribute to an existing online social media channel on work-related subjects.

Requests should clearly illustrate the potential benefit to patients and/or colleagues both within SFH NHS Foundation Trust and the wider healthcare community and/or the organisation as a whole. It must also be able to illustrate team and departmental commitment to the project. Managing or contributing to a blog, Twitter, Facebook, Instagram

or other social media account without regularly updating it, or failing to respond to comments from patients, the public or other users in a timely manner can negatively affect the Trust's reputation, and may lead to approval being rescinded and the site being closed down.

Permission to set up or contribute to an account will only be granted once the staff or team have provided the detail below, and successfully completed both training and a short competency test.

Name
Department
Extension
Line Manager
(NB: Approving line manager(s) are expected to conduct a monthly review of any social networking account overseen by them. This review is to check that posts are regular and relevant, and add value to the Trust)
Social media channels requested to connect with
e.g. Twitter, Facebook, Instagram, etc.
Have you already tried supplying the Communications team with content for the main Trust accounts?
If you would like to set up a new account, what do you feel the advantages would be to the Trust of having this as a separate account rather than providing content for the official Trust channels?
Details of the audiences you wish to reach

Please state what you intend to achieve with the posts
What benefits do you see from connecting with the above networks?
Who will manage enquiries out of hours?
What process will you have for dealing with negative comments?
Please provide some sample posts
Detail how you will maintain a schedule of social media posts over a sustained period.
Provide an outline plan should the account be hacked.

APPENDIX F - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Social Media Policy			
New or existing service/policy/procedure: Social Media and Recordings for Non-Clinical Purposes Policy			
Date of Assessment: April 2022			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	**a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?**	**b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?**	**c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality**
The area of policy or its implementation being assessed:			
Race and Ethnicity	N/A	N/A	N/A
Gender	N/A	N/A	N/A
Age	N/A	N/A	N/A
Religion	N/A	N/A	N/A
Disability	N/A	N/A	N/A
Sexuality	N/A	N/A	N/A
Pregnancy and Maternity	N/A	N/A	N/A
Gender Reassignment	N/A	N/A	N/A
Marriage and Civil Partnership	N/A	N/A	N/A
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	N/A	N/A	N/A

What consultation with protected characteristic groups including patient groups have you carried out? N/A
What data or information did you use in support of this EqIA? N/A
As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments? N/A
Level of impact From the information provided above and following EQIA guidance document Guidance on how to complete an EIA (click here), please indicate the perceived level of impact: **Low Level of Impact** For high or medium levels of impact, please forward a copy of this form to the HR Secretaries for inclusion at the next Diversity and Inclusivity meeting.
Name of Responsible Person undertaking this assessment: Richard Brown
Signature: *Richard Brown*
Date: 21.04.22