Torbay and South Devon
NHS Foundation Trust

Social Media
Engagement Policy

Corporate Policy

If you require a copy of this policy in an alternative format (for example large print, easy read) or would like any assistance in relation to the content of this policy, please contact the Equality and Diversity team on: 01803 656676.

Date of Issue:	November 2020	**Next Review Date:**	November 2022
Version:	Version 3	**Last Review Date:**	November 2020
Author:	Laura Jenkins, Communications Manager		
Directorate:	Communications Department		
Approval Route			
Approved By:		**Date Approved:**	
Executive Team		September 2017	
IM&T Group		December 2020	
Links or overlaps with other policies:			
Disciplinary Policy			
Information Governance Policy.			
Feedback and Complaints Policy.			
Child Protection Policy G2075			

Amendment History

Issue	Status	Date	Reason for Change	Authorised
V1		**November 2014**	*Complete rewrite of original document due to developments in social media and its usage. Clearer advice on roles and responsibilities and appropriate uses.*	**Guy Boosey, Staff side, Anna Alexandra**
V0.66		**July 2017**	*Final proof*	**Claire Rowe**
V1.1		**Aug 2017**	*Changes to include safeguarding requirements for grooming. Plus addition of IG requirements around messaging patient data.*	**Claire Rowe**
V3		**November 2020**	*Review and update of policy. Includes amended contact details and update to available social media channels.*	**Laura Jenkins**

Table of Contents

Appendices

1 Policy statement

1.1 This policy is intended to help staff make appropriate decisions about the use of current and future social media channels, such as: blogs, wikis, podcasts, discussion forums, message boards, interactive news sites, as well as social networking sites including: Twitter, Facebook (including staff groups and pages), Instagram, Snapchat, TikTok, Tumblr, google+ and LinkedIn (this *list is not exhaustive)*.

1.2 This policy outlines the standards required of staff when using social media, the circumstances in which we monitor employees' use of social media and the action we will take following breaches of this policy.

1.3 This policy supplements the existing Trust policies around use of IT, websites and social networking.

2 Introduction

2.1 Torbay and South Devon NHS Foundation Trust (TSDFT) is increasingly using social media to engage with service users, staff and other stakeholders, as well as deliver key information. These online digital interactions are likely to be further extended as appropriate new channels become available.

2.2 Many employees enjoy sharing their knowledge and experience with others of similar roles and interests. The Trust understands these online activities and acknowledges that staff can improve their personal skills and experience through relevant interactions with others outside the organisation**.** However, the Trust has a responsibility to ensure the operational effectiveness of its business, including the public image, reputation and the protection of service users, staff and information. This involves ensuring confidentiality and maintaining security in accordance with the Information Governance Policy.

3 Scope

3.1 ***This policy applies to all staff employed by TSDFT, as well as those employed on temporary contracts (from here on referred to as contractors), which includes: bank staff, agency staff, staff employed by partners based at the Trust, students on placement, volunteers and other externally contracted staff.*** *If breached,* contract staff will be dealt with through the policies of their respective employers and may also be removed from their position on site if deemed necessary.

3.2 All staff and contractors are expected at all times to protect the privacy, confidentiality, and interests of: the Trust, service users, employees, contractors, partners and other stakeholders.

3.3 Breach of this policy by employees will be dealt with through the Disciplinary Policy and in serious cases may be treated as gross misconduct, leading to summary dismissal. Contract staff will be dealt with as stated in section 3.1.

4 Equality and diversity statement

4.1 The Trust is committed to preventing discrimination, valuing diversity and achieving equality of opportunity. No person (employee, service user or member of the public) will receive less favourable treatment on the grounds of the nine protected characteristics (as governed by the Equality Act 2010): sexual orientation, gender, age, gender re-assignment, pregnancy and maternity, disability, religion or belief, race, marriage and civil partnership. In addition to these nine, the Trust will not discriminate on the grounds of domestic circumstances, social-economic status, political affiliation or trade union membership.

4.2 The Trust is committed to ensuring all services, policies, projects and strategies undergo equality analysis. For more information about equality analysis and Equality Impact Assessments please refer to the Equality Analysis Procedure.

5 Managers' responsibilities

5.1 To ensure employees have a clear understanding of the use of social media inside and outside of the workplace and the current social media policies:

5.1.1 By directing all staff to read the policy carefully and feedback any questions they may have.

5.1.2 Through ensuring staff that need to develop a better understanding have access to appropriate training. For further advice please contact the Communications Team *(contact details included in section 16)*.

5.2 To take appropriate advice and action when abuse of social media in the workplace is brought to their attention, by contacting the Communications Team *(contact details included in section 16)* immediately to discuss the issue.

6 Employees' responsibilities

6.1 All employees and contractors are responsible for their own understanding and compliance with this policy and for ensuring that it is consistently applied. All staff and contractors should ensure that they take the time to read and understand it and if clarification is needed, then to discuss with their line manager in the first instance.

6.2 Staff and contractors are ultimately responsible for their own online behaviour and must take care to avoid online content or actions that are considered illegal such as: inaccurate, libelous, defamatory, harassing, threatening, or grooming (where someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse, sexual exploitation or trafficking).It is possible for staff to be subject to civil proceedings or criminal prosecution for their online content.

7 Definition

7.1 Social media is the collective of online communication channels dedicated to community-based input, interaction, content-sharing and collaboration. Websites and applications dedicated to: forums, microblogging, social networking, social bookmarking, social curation and wikis, are among the different types of social media, although not exhaustive.

8 Duties and responsibilities – Agreed corporate use of social media

8.1 The Trust currently has a corporate presence on: Facebook, Twitter, Vimeo and YouTube. In future, the number and type of corporate channels may increase with the development of new social media channels, depending on the stakeholders the Trust wishes to engage with. If staff want to convey news stories, events or messages through the corporate social media channels, please contact the Communications Team who will be able to advise and support publication *(contact details included in section 16).*

8.2 We recognise the importance of social media in shaping public thinking about, and engagement with, Trust services, employees and partners. We also recognise the importance of our staff being able to join in and help shape direction of our corporate engagement with these channels.

8.3 We encourage staff and contractors using social media channels in a professional capacity, to retweet or like messages sent out through the corporate account, helping to promote the content to their network and increasing the reach of the information. They are also encouraged to adapt the content in a professional manner to send out through their own channels, again spreading the message.

8.4 However, employees and contractors **are not authorised** to communicate by any means on behalf of the Trust via social media, **unless this has been agreed by their line**

manager and approved (in advance) by the Head of Communications. No social media sites or pages relating to the Trust should be set up by staff and/or contractors without prior approval from the Head of Communications.

8.4.1 Approval should be obtained by sending a request to the Communications Team *(contact details included in section 16),* who will be able to advise on the chosen channel and ensure that any risks have been discussed. A Social Media Planning form (attached in Appendix A) will be filled in during discussions with the Communications Team, before recommendations are sent to the Head of Communications for final approval. This approval requirement enables the Trust to ensure staff are properly prepared and trained for the proposed online engagement and any channels that are established are in line with the corporate objectives and comply with NHS branding and style guidelines.

8.5 All new professional social media channels should have one approved Account Manager who is responsible for the content published, even if there are several editors. The Communications Team *(contact details included in section 16)* can help set up the account and discuss the issues and requirements of the channels.

8.6 All approved professional social media channels will be reviewed within a year, and deleted if deemed to not be achieving the jointly agreed objectives set up in the Social Media Planning form.

8.7 Employees using social media in a professional capacity must not breach copyright laws when posting images. Taking images from Google images, Bing images or other photo libraries can incur a fee, or even prosecution for breaching copyright law. So knowledge of the copyright and usage licence is essential. For more information discuss with the Communications Team *(contact details included in section 16).*

8.7.1 Employees must also seek permission from colleagues or service users prior to publishing images of them on corporate social media channels, through the use of model release forms.

8.8 Social media training is available in-house to staff with a social media remit, to ensure that staff are aware of latest guidance and best practice and are able to use social media channels to their best effect. For more information, discuss with the Communications Team *(contact details included in section 16).*

9 Duties and responsibilities – Private use of social media

9.1 Any online activity by staff or contractors that brings **the organisation into disrepute or a breach of confidentiality rules,** regardless of whether it was posted in a personal or professional capacity, or on a third party site (for example Spotted Torquay on Facebook) will be treated as a breach of this policy**.** This includes any statement or comment that

could be seen to negatively affect the reputation or name of the Trust, or to breach the guidelines set out in sections 8-9.

9.2 Staff are personally responsible for the content they publish on social media channels. Staff should use the same principles and standards that would apply to communicating via other more traditional communication channels. For example, do not say anything that can't be said in a room full of friends, colleagues, service users, journalists or suppliers.

9.3 Staff and contractors in their personal use of social media may wish to retweet or like messages sent out through the Trust's corporate accounts, please do so as this again helps to promote the content more widely. They may also adapt the content (in a professional manner) to issue through their own channels to other networks if they wish.

9.4 Staff are able to reply to positive comments made on social channels by the general public, but are reminded to do so in a professional manner as you are representing the Trust (even from a personal account). This includes 'Liking' on Facebook, for example.

9.5 As well as being a disciplinary offence, misuse of social media can in certain circumstances constitute a criminal offence (for example cyber bullying, cyber stalking, grooming or trolling), or otherwise give rise to legal liability against the member of staff. Be aware the individual will be legally responsible for any comments made in a personal capacity within private social media accounts.

9.6 Staff and contractors using social media channels in a professional or personal capacity must adhere to the following guidelines. Breach of these guidelines may lead to disciplinary action and potentially be seen as gross misconduct:

9.6.1 Employees and contractors must not:

- Disclose confidential information about service users, staff, or the organisation. This includes posting any information that can be used to identify a service user's identity or health condition in any way.

- Disclose information relating to the Trust that is, or may be, sensitive or commercial in confidence, or that is subject to a non-disclosure contract or agreement. This applies to information about: service users, other staff and contractors, other organisations, commercial suppliers and other information about the Trust and their business activities.

- Make any detrimental comments about, or in any way use social media to criticise, attack or abuse colleagues.

- Publish or report conversations that are private, internal to the Trust or partner agencies.

- Share details of the Trust's implemented security or risk management arrangements. These details are confidential, may be misused and could lead to a serious breach of security occurring.

- Use personal insults, obscenities, inflammatory language or engage in any conduct that would not be acceptable as a staff member of the Trust.

- Reply to negative comments about the Trust or staff members, made by others on social media**.** If staff are concerned about a negative comment or complaint they see online, **do not reply**. This includes 'Liking' negative comments on Facebook, for example. Instead contact the Communications Team, who will consider a corporate response to the comment.

- Post photographs of their workplace or patients / service users from their own social media accounts. Any photographs that they feel need to be shared, should be through the corporate account with appropriate consent. (see point 8.7.1)

- Post comments or content which is likely to create any legal problems whether criminal or civil, for either the staff member or the Trust. These include comments that may be seen as: slanderous, libelous, defamatory, harassing, or offensive or threatening (trolling).

- Post any material which breaches copyright or other intellectual property rights, or invades the privacy of any person.

- Use messaging services such as WhatApp or iMessage to share identifiable or confidential patient data with colleagues in other Trusts, as they may not be secure. When discussing diagnosis or patient information use NHS email only (as suggested by NHS England).

9.6.2 Employees should:

- Respect copyright, fair use, data protection, defamation, libel and financial disclosure laws.

- Only use corporate logos or other visible markings or identifications associated with the Trust on professional accounts where prior permission has been obtained from the Communications Team.

- Contact the Communications Team (contact details included in section 16) immediately if approached for comment by a journalist or media representative, including via social media.

9.7 Staff may use designated facilities provided by the Trust for their private social media purposes during work breaks only. However, the Trust reserves the right to withdraw permission at any time if these facilities are abused.

10 Monitoring use of social media sites

10.1 Staff should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored and where breaches of this policy are found, action may be taken under the Disciplinary Policy.

10.2 The Trust reserves the right to restrict or prevent access to certain social media websites if personal use is considered to be excessive. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

11 Reporting inappropriate behaviour on social media

11.1 If a member of staff comes across information contained in social media sites that contravenes this policy they should report the issue immediately to the Communications Team, who will ensure appropriate action is taken by the relevant Trust department.

11.2 Incidents may be investigated by the Information Governance Team and/or through the Disciplinary Policy.

12 Breach of guidelines

12.1 The Trust may also take disciplinary action against any employee who brings the organisation into disrepute by inappropriate disclosure e.g. comments and or photographs on social networking sites or personal internet sites. Bank workers, agency staff and other externally contracted staff will be dealt with through the policies of their respective employers and may also be removed from their position on site.

12.2 If any material posted by staff in a professional or personal capacity breaches the guidelines discussed in sections 8 and 9, then this will be addressed under the Disciplinary Policy and, depending on the severity, may result in summary dismissal.

12.3 Where the social media guidelines mentioned in sections 8 and 9 have been breached the following procedures will be used:

12.3.1 The employee's line manager (or contracted organisation) will be contacted and they will carry out a preliminary investigation to find out what happened. The staff member will be asked to remove the problematic statement or message and given an explanation as to why it should be removed. This may involve a brief discussion with a complainant, a witness, or the employee concerned; whenever possible an initial written account of the events should be obtained. If it is necessary to discuss the incident with the employee, they should be advised that it is not a formal disciplinary meeting and is solely to establish the facts. There is no right to representation at this meeting. The employee must also be advised that an outcome

of the preliminary investigation will identify if there is a need for them to attend a further formal meeting.

12.3.2 Where the matter appears to be of a minor nature, the manager should deal with the issue informally, as in accordance with (section 10.3) 'Informal Action' of the Disciplinary Policy. However, if following the preliminary investigation further investigation is needed, or the matter is a potential disciplinary incident, a formal investigation will then be conducted.

12.4 If an employee finds their account details have been obtained by another person without permission (hacked) and these guidelines are broken as a result, they must rectify the problem as soon as possible by deleting any problematic messages and reporting the incident immediately to the Communications Team. The Communications Team can then give further advice to ensure the relevant social media account is more secure in the future. If a professional account is involved, the South Devon Health Informatics Service will also be informed.

13 Complaints about staff via social media channels

13.1 Any member of staff or contract staff that sees a negative comment about another employee should contact the Communications Team as soon as possible *(contact details included in section 16)* and where possible take a copy of the offending message *(as we may not have access to it if on a private account).* The message can then be sent to the correct department depending on the nature of the comment.

13.2 If the comment concerns a complaint about the staff member's work, rather than a complaint about them personally, then a copy of the complaint message will be sent to the Patient Advice and Liaison Service (PALS) to investigate the complaint further with the complainant, abiding by the Feedback and Complaints Policy.

13.3 Where staff members are mentioned in social media in a manner that is perceived to be threatening or abusive, or where the safety of the staff member is of concern, the comment will also be passed to the HR team to discuss with the member of staff's line manager (where a decision will be made on how to proceed). Other teams such as Legal, Safeguarding or Security teams may be copied into correspondence, based on the information in the comment and the language used.

14 Training and awareness

14.1 Advice and support will be provided by the HR, Information Governance and Communications Teams, as appropriate to support staff and managers in complying with this policy and following best practice when dealing with social media issues.

14.2 The Communications Team will raise awareness of this policy (which will be placed on the public facing site) through the publication of information on the Trust's intranet. Staff will be made aware of any changes that are made to the policy through information in the staff bulletin and through the policy approval process.

15 References

- ACAS – Social media & how to develop a policy
- LRA – Advice on Social Media & the Employment Relationship
- NHS England – Social media and attributed digital content policy
- NHS Branding Guidelines- Foundation Trusts

16 Contact details

16.1 Any queries regarding this policy should be directed in the first instance to the Communications Team via:

01803 217398 or communications.tsdft@nhs.net

17 Monitoring, audit and review procedures

17.1 A full review of this policy will take place every two years by the Head of Communications, unless legislative changes determine otherwise.

Appendix A - **Social Media Request Form**

Who is requesting a social media channel?

What channel would you like and why?

Why THAT specific channel?

Aim/purpose of the channel?

Profile description ~ when the channel will be staffed (in case they want to contact you), who it's aimed at? (Remember there is limited space so think less than 140 characters)

Risks and processes of using a social media ~ for example what happens if you're contacted by someone upset out of hours, how will you deal with complaints or sensitive data?

Account name:

Handle/name of user:

Do you wish to add any images to your profile, please attach to your email with this document?

Special instructions (Comms to complete):

Date set up:

Date to review channel/stream:

NHS
Torbay and South Devon
NHS Foundation Trust

Avoiding the risk of Social Media for staff

It's so easy after a hard day at work to go home and share with your friends on social media, the problems and issues you have faced throughout the day. However, few of us realise that some of the information we share could land us in hot water.

We are not trying to prevent you from using social media, but we do want to help you navigate through the murky waters, so you can enjoy the many benefits of social networking.

You may believe that what you write on your personal Facebook page (or other channel) is your personal opinion and has no effect on your work life. However, what you may not be aware of is that some content can breach your contract of employment, or even the law. To help you navigate social media, here are some quick tips on what you should avoid.

Don't

- Make critical, untrue or harmful comments about the Trust, its patients, or your work colleagues.
- Discuss patients past or present, or post information on their condition or illness which could help identify them.
- Take films or photos of patients or colleagues and publish them on your, or anyone else's, social media account.
- Comment or discuss any private or confidential work information.
- Use personal insults, swear or use unprofessional language that could be seen as sexist, homophobic, racist or generally offensive.
- Post comments or content that could be seen as libelous (a comment that is untrue and harmful to a person's reputation), harassing (publishing comments that are annoying or upsetting) or send messages that are seen as offensive or threatening (known as trolling).
- Sending or sharing explicit photographs of yourself to children or young people is a criminal offence and will be treated as such.
- Sending or sharing explicit photographs of children and young people is also a criminal offence.
- Online grooming behaviour of vulnerable adults or children will be investigated by the Trust and relevant agencies. Further information can be found on NSPCC website.
- Reply to negative comments made by the public about the Trust on any social media channels. If you are concerned about a comment or complaint you see online about the Trust or a fellow member of staff, **do not reply,** contact the Digital Content Manager who will discuss it with the right department and reply through the corporate channels.

Remember you are responsible for what you write on social media and anything you post will stay in the public domain for a #VERYLONGTIME, so be careful.

Taking part in social networks and online communities can offer many benefits to you as an individual, and for us as an organisation, so we don't want to put you off using them. The best advice is to approach social media with **common sense.**

Think before you tweet! Would you say it to your: boss, colleagues, friends and family? If not, then don't say it on social media!

Tips on how you can enjoy the benefits of social media:

- It's is a great way to keep up to date with your friends and colleagues, as well as the latest professional health information.
- If you wish to ***reply to positive feedback*** about the Trust or ward on social media, please do so in a professional manner as you are representing the Trust (even from a personal account).
- Share or retweet positive comments about your team or the Trust. This will help ensure our positive feedback reaches more accounts, helping to share in our good news.
- Follow/ like the Trust's corporate accounts, it will help to keep you up to date with other parts of the Trust.
- If you have any work related success stories, or other information you want to share with the public on the corporate channels, please send them to the Digital Content Manager (contact details at end).
- If a journalist or someone from the media contacts you through social media for a comment or to discuss an issue, contact the Communications team. Do not reply by yourself.
- Remember ***only use*** social media in work time if it's an agreed part of your job. If not, only use it during your work breaks.
- **Ensure you read the new Social Media Policy thoroughly.**

Security tips to keep you safe:

- Keep your password safe and avoid using obvious ones that others might easily guess.
- Be careful about the personal details you post online such as: address, phone number, email and date of birth; don't make stalking or identity fraud easy.
- When you set up an account make sure you look at the security settings. Ensure you have the right settings that only allow your friends to see your details.
- Make sure you know how to block or report any users that say anything offensive or upsetting.
- Be suspicious of any contacts that you don't know asking for any personal details or information about the Trust or patients.
- Think before you send nude or sensitive pictures through social media even to a loved one. Remember everything you send, even if deleted, can be found if someone looks hard enough.
- Remember many employers and potential employers now look at social media channels to find out more about you as a person. So watch what content you publish and the pictures you're tagged in.

For advice contact the Trust Communications Team
01803 217398
communications.tsdft@nhs.net