TRUST-WIDE POLICY

SOCIAL MEDIA POLICY

DOCUMENT REF: PTWDSOCIA
(Version No. 3.0)

Name and designation of policy author(s)	Alexa Traynor – Associate Director of Strategic Communications & Marketing
Approved by (committee, group, manager)	Sarah Barr- Associate Director of IM&T (Chief Information Officer)
Approving signature	Electronic approval received
Date approved	8th March 2018
Review date	March 2021
Review type (annual, three yearly)	Three yearly
Target audience	All Staff
Links to other strategies, policies, procedures	Bullying and Harassment Policy Email and Internet Acceptable Usage Policy Disciplinary Policy & Procedure Incident Reporting Policy Information Security Policy Safeguarding Adults & Children Policy Raising Concerns Policy
Protective Marking Classification	Public

Consultation:

	Authorised by	Date Authorised	Comments
Impact Assessment	Dee-Anne Bentley – Document Control Manager & FOI Lead	20th February 2014	No requirement for full assessment.
Fraud Assessment	N/A	N/A	N/A

Circulation/Dissemination:

Date added into Q-Pulse	13th March 2018
Date notice posted in the Team Brief	13th March 2018
Date document posted on the intranet	13th March 2018

Version History:

Date	Version	Author name and designation	Summary of main changes
May 2013	1.0	Alexa Traynor - Associate Director of Strategic Communications & Marketing.	First version. Approved by Integrated Governance Committee on 29th May 2013
December 2014	2.0	Emer Scott - Associate Director of Strategic Communications & Marketing (Interim)	Social media examples updated. Additional information about benefits of using social media. Policy extended with new section covering social media use by patients/visitors. New section clarifying process and approvals required to set up Trust social media accounts. Clarification of duties regarding confidentiality and information governance. Clarification of guidance on copyright including use of images. Clarification of processes around any inappropriate use of social media. Guidance for staff extended to reflect requests for more “do / don’t” examples. Shared with trade union representatives, HR and Information Governance for comment. Submitted for document control 13th May 2015.
March 2018	3.0	Alexa Traynor - Associate Director of Strategic Communications & Marketing.	Reviewed. No updates required, removal of reference to blackberry messenger.

CONTENTS

1.0 Introduction

Social media refers to websites and apps which allow people to interact online with each other– e.g. by sharing information, opinions, knowledge and interests. As the name implies, social media involves online communities or networks, encouraging participation and engagement.

The best-known examples include: social networking sites like Facebook, LinkedIn and Google Plus; photo/video-sharing sites such as Instagram, YouTube and Vine; micro-blogging sites such as Twitter; blogs, audio and video podcasts; 'wikis' (such as Wikipedia); message boards; and social bookmarking websites such as Pinterest.

It enhances our ability to engage and communicate with our key audiences; however there are some risks. It is important that appropriate professional boundaries with patients are not jeopardised (e.g. by staff becoming Facebook 'friends' with their patients).

This policy explains our approach to social media and the process for creating and managing accounts linked to the Trust, including those where staff post about their work or professional expertise. It also provides guidance on our expectations about staff use of social media, both in a professional and a personal capacity.

Where someone's association with the Trust can be identified and/or they are discussing work-related issues on social media, they are expected to behave appropriately and in ways that are consistent with the Trust's values and policies, their individual responsibility as a Trust employee, and with the relevant professional codes of conduct for healthcare professionals. Employees who are found to breach the Trust's policy on Social Media may be managed in line with the Trust's Disciplinary Policy, Bullying and Harassment Policy or any other appropriate policy.

All employees are reminded of the need to maintain both patient and colleague confidentiality when using social media as outlined in this policy.

The intention of this policy is not to stop or dissuade Trust staff from using social media personally or professionally; it is to minimise any risks for individual staff members and the Trust. it is worth noting that there have been several cases elsewhere of staff being dismissed by their employer for inappropriate use of social media.

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

2.0 Scope

This policy applies to all staff who are directly employed by the Trust. This policy also applies to any non-contracted, temporary, secondments, bank, agency, students, volunteers or locums whilst on placement at the Trust. It also outlines our policy on use of social media by patients/visitors.

3.0 Responsibilities

Managers

It is every manager's responsibility to:

- Ensure that staff are aware of this policy and the parameters that are outlined.
- Thoroughly investigate any instances where behaviour is not in accordance with the procedure that is set out within the policy.

Staff

Staff must ensure that they:

- Are complying with the expectations of this policy to support the reputation of the Trust and, where relevant, of their profession.

- Conduct themselves online in the same manner that would be expected of them in any other situation.

4.0 Definitions

This policy applies to all forms of social media. They can be sub-divided as below.

Social Media is the term commonly used for online and mobile communication technologies that enable messages and opinions to be shared with others. It includes text messaging, instant messaging and other similar services.

Social Networking uses online sites and tools that allow people to interact and/or connect with others. Popular examples include Facebook, Twitter and LinkedIn. LinkedIn and Twitter can be particularly useful for connecting with key influencers in your field.

Blogging allows people to share thoughts, news and opinions with others e.g. in an online diary or personal opinion column. Tweeting (micro-blogging) allows people to do this in very short messages. Many blogs/tweets are interactive allowing visitors to respond with comments or share the messages with others. It is increasingly common for blogs to feature advertisements to financially benefit the blogger or to promote a blogger's favourite cause. The word blog is derived from the phrase weB LOG.

5.0 Policy Objectives

The objectives of this policy are:

- To outline to staff what is acceptable usage of social media both at work and in their personal lives.

- To set out the process for creating official Trust social media accounts / pages. To encourage staff to be mindful of what content they share on the internet.
- To ensure appropriate standards of confidentiality are maintained.
- To ensure that professional boundaries with patients are maintained and protected.
- To understand the implications of using social media inappropriately.
- To set out our expectations of patients/visitors using social media on our sites or involving our staff or other patients/visitors.

The intent of this policy is not to stop staff from conducting legitimate activities on the internet but to minimise the risk of any problems arising, both for individual staff and the Trust.

6.0 Adherence to Other Trust Policies & Procedures

Staff using social media should always adhere to codes of conduct and policies which are part of their professional and employment requirements. These include:

- Professional code of conduct (e.g. Health Professions Council)
- Other codes of conduct (e.g. confidentiality clause in your contract)
- Relevant Trust policies, including:
    - Bullying and Harassment Policy
    - Email and Internet Acceptable Usage Policy
    - Disciplinary Policy & Procedure
    - Incident Reporting Policy
    - Information Security Policy
    - Safeguarding Adults Policy
    - Safeguarding Children Policy
    - Raising Concerns Policy

7.0 Social Media Principles

7.1 Use at Work

Staff are able to access the main social media sites from the Trust's PCs but must comply with all aspects of this policy when doing so. If staff wish to access social media sites such as Facebook, Twitter and blogs while they are at work they must follow the principles below:

- Any member of Trust staff or of any other organisation which uses the Trust network is only entitled to access appropriate websites from the Trust's computers as outlined in the Email and Internet Acceptable Usage Policy.
- Staff may access social media for work purposes or the benefit of the Trust (e.g. professional development or to promote a service) during working hours at their manager's discretion.
- When at work, staff must only access social media accounts for personal use during allocated break times. This applies regardless of whether they are using a Trust device or a personal device. Use of the guest Wi-Fi network on personal devices should be limited to allocated break times only.
- Social media must only be used in an ethical and lawful manner – subject to the principles as below.

7.2 Personal Use

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

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

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

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

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

When using social media, Trust employees have a responsibility to refrain from any action which brings them, their work colleagues, the Trust or the NHS into disrepute. The following list in section 7.3 is not exhaustive, but gives some examples of the minimum standard of behaviour required.

7.3 Standards for Staff Using Social Media

Trust employees must not maintain a site, update a status or a page, or engage in instant messaging that brings the Trust into disrepute. As already stated, this applies even when doing so in a non-work capacity – for example, a website for an outside group. The following paragraphs set out the minimum standards expected of staff when using social media:

7.3.1 Make clear opinions are your own

If a member of staff discloses that they work for the Trust or can be identified as an employee through association with other people, they should ensure their profile and related content is consistent with how the Trust would expect them to present themselves to colleagues and business contacts.

Staff should also make it clear that their views are their own, not those of their employer. The use of a disclaimer which states this, however, does not override the need to follow the other standards outlined in this policy.

7.3.2 Do not set up official Trust/departmental sites

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

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

7.3.3 Communicating as yourself

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

If an employee posts under a pseudonym and at a later stage these posts are associated with their real name, all previous posts will be admissible in a disciplinary investigation or hearing.

7.3.4 Respect others

The Clatterbridge Cancer Centre is committed to providing an organisation free from bullying and harassment in all its forms and will take all steps, in partnership with recognised Trade Unions, to achieve this objective including, where necessary, appropriate action in accordance with the agreed disciplinary policy.

Therefore anything which could be seen as racist, sexist, homophobic, sexually explicit, threatening, abusive, disrespectful or unlawful (for example images, references and/or comments) must not be published online.

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

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

7.3.5 Be aware of how online posts are, or can become, public

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

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

Staff should carefully consider what they want to say before they publish anything, and work on the basis that anything they write or post could be shared

more widely without their knowledge or permission. Staff should configure their privacy settings and review them regularly because social media sites cannot guarantee confidentiality, and do sometimes change their settings. This means the public, employers or any organisation that staff have a relationship with may be able to access a staff member's personal information - and once information is online, it can be difficult to remove it.

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

7.3.6 Get your facts right

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

7.3.7 Ensure comments are legal

All comments must be legal and must not incite people to commit a crime. There are legal requirements around privacy and confidentiality that staff must not breach – for example, the Data Protection Act 1998. Any confidentiality breaches of the Data Protection Act 1998 are a breach of contract of employment. All staff must complete their annual Information Governance Training and ensure that all Trust policies are adhered to.

7.3.8 Understand the implications of defamation

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

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

7.3.9 Respect copyrights

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

7.3.10 Be careful when talking about work-related issues

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

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

You should state that any opinions expressed are your own, not your employer's. Staff must also respect patient confidentiality, and must never disclose information that could identify a patient.

7.3.11 Be careful about the use of photos

If staff post any photos of themselves or colleagues in uniform or in an identifiable work setting, they must ensure that these represent a professional

image of the Trust. Staff should not use a photo of themselves in uniform as their profile picture; this could give the impression that their site is an official site.

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

7.3.12 Protect patient confidentiality

Confidentiality must be respected by anyone who posts anything about their work on the internet, and under no circumstances should anything be posted that identifies a patient (including their relatives, visitors or carers).

Staff must ensure they know the Trust policy on patient confidentiality and follow it at all times.

7.3.13 Respect safeguarding issues

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

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

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

7.4 Business Use

The Communications Team has responsibility for external communications at the Trust and are the only people authorised to set up social media accounts and campaigns for the Trust. Anyone who wants to launch a social media account or campaign for the Trust must contact the Communications Team. They will need to provide details of: the social media platform they plan to use, the aim of the account, the audience, how it will be resourced and managed (e.g. who will produce content, who will have access to upload content), a risk analysis, and how information on it will be stored (e.g. for FOI). The Communications Team will consider the request. Where appropriate, the Communications Team will liaise with Information Governance before deciding whether to approve the request.

In certain cases, permission may also be required from the Information Governance Board before developing a Trust project/presence in any form of social media. If this is the case, the Communications Team will inform the requestor of this after discussion with the Information Governance team. A 'business case' which provides more detail on the areas outlined in the previous paragraph, will need to be provided – including an exit strategy. The Communications Team and Information Governance Manager can advise on this. A copy of the business case must be submitted to the Communications Department for comment before it goes to the Information Governance Board.

Staff must respect copyright, fair use and financial disclosure rules. It is also advisable to have methods (e.g. Excel, CSV, XML, HTML or PDF format) or a plan in place to capture the content of any external social site you use so that it can be held on Trust systems as part of an information governance audit trail.

7.5 Social media use by patients/visitors

Patients/visitors are welcome to use social media sites while on our premises or in relation to our services and care, as long as they are not breaching another

patient/visitor's confidentiality or posting comments that are offensive, illegal or defamatory.

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

8.0 Queries & Complaints

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

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

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

9.0 Reporting Inappropriate Behaviour on Social Media

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

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

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

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

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

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

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

10.0 Training

There is no specific training required although workshops may be arranged for staff who would find it helpful. The policy will be cascaded to all staff who must direct their enquiries to the Communications Team.

11.0 Audit

The Communications Team and/or HR will record instances where a potential cause for concern is known and will act in accordance with this policy.

The policy will be audited on an ongoing basis by the Communications Team.

12.0 References

There are no references relevant to this policy.

13.0 Appendix

Appendix 1 –Staff Guidance on the Use of Social Media Sites

We care about our staff and the following guidance aims to protect you. Please don't leave yourself open to using social media in a way that may harm you professionally or personally, or to having your account hacked. This Guidance should be read in conjunction with the Social Media Policy.

How to avoid problems with blogging and social networking sites

1. When registering with a website, understand what you are signing up to by reading the terms and conditions carefully. It's important to determine what security, confidentiality and liability claims, undertakings and exclusions exist. If in any doubt seek the advice of your Information Governance Team.

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

3. Think about what you want to use your online profile for (e.g. sharing personal news / photos with friends or to network with others in your profession), applying appropriate security and preferences settings as necessary.

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

5. Never leave your social media browser open and unlocked (e.g. on a device that is not protected by a pin code or password) when you are not using it; this may enable someone else to tweet or post from your account. Log out of the account and, if you have your own computer, lock your screen when you leave the machine.

6. Don't 'save passwords' for social media sites when using a shared computer.

7. Be aware that social media can blur the boundary between your personal, public and professional lives. Be conscious of your online image and how it may impact on your professional standing – patients and employers (current and future) may not be amused by the photos from your best friend's stag do if they see them on Facebook or Twitter.

8. Never feel pressurised to accept a 'friend' request from another member of staff. All staff have the right to refuse friend requests without causing offence.

9. 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.

10. Do not say anything online that you would not say personally or wish others to hear.

11. Avoid unattributable anonymous comments.

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

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

14. 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 authority to have that information. Check that the intended recipient has appropriate information governance arrangements in place to handle any information disclosed to them. Always check with your line manager or Information Governance Manager before sharing information as you could breach the Data Protection Act 1998 resulting in a fine for the Trust, disciplinary action against you or even prosecution by the Information Commissioner's Office. For more information about online safety, please visit the Information Commissioner's Office website on the link below http://ico.org.uk/for_the_public/topic_specific_guides/online/social_networking

15. Avoid disclosing personal or other sensitive information in 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.

16. Do not send personal or other sensitive information over the Internet unless you are completely confident in the websites level of security/legitimacy.

17. Staff who post online have an ethical obligation to declare any conflicts of interest.

18. Maintain professional boundaries with current or former patients. The BMA advises doctors and medical students not to accept Facebook friend* requests from their current or former patients, and this is good advice for all NHS staff. (Where a member of staff is already friends with a patient,

they should exercise judgment to ensure professional boundaries are maintained and they do not breach confidentiality, including on social media.)

19. Defamation and contempt of court laws can apply to any comments posted on social media/the internet in either a personal or professional capacity.

Adapted from BMA guidance document: 'Using social media: practical and ethical guidance for doctors and medical students'

*Trust Facebook accounts are set up as pages that people can 'like', rather than 'friending'.