Maidstone and Tunbridge Wells NHS
NHS Trust

Ref: FOI/CAD/ID 4042

Please reply to:
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone
Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net

27 June 2017

Freedom of Information Act 2000

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to social media.

1. Please provide me with a copy of your Trust's Social Media Governance Policy (for employees), or equivalent, and the date it was adopted.
2. Please list the Social Media programmes used by your Trust (i.e. if you use Twitter, Facebook, and Instagram etc. ... I do not need individual account details).
3. Please detail training offered to staff on the use of social media.
4. Please state how many people in your Trust have been disciplined as a result of social media behaviour, for the calendar years 2012-2016
5. Please provide the approximate number of people (headcount) employed by your Trust.

1. The social media policy was first adopted (ratified) in August 2012. The policy was updated, revised and ratified in 2016 and will be reviewed again in 2019.

MAIDSTONE AND TUNBRIDGE WELLS NHS TRUST

Social Media Policy and Procedure

Requested/ Required by:	Information Governance Committee
Main author:	Head of Communications, ext 25859
Other contributors:	Department of Health Informatics Directorate
Document lead:	Deputy Chief Executive
Directorate:	Corporate
Specialty:	Trust Management
Supersedes:	Social Media Policy, Procedure and Guidance [Version 1.0: August 2012]
Approved by:	Senior HR Meeting, 14th April 2016
Ratified by:	Policy Ratification Committee, 29th April 2016
Review date:	April 2019

Disclaimer: Printed copies of this document may not be the most recent version.
The master copy is held on Q-Pulse Document Management System
This copy – REV2.0

Document history

Requirement for document:	Recommendation – Department of Health - Common Law of Confidentiality - NHS Confidentiality Code of Conduct
Cross references:	- British Medical Association *Using Social Media: Practical and ethical guidance for doctors and medical students* http://bma.org.uk/-/media/Files/PDFs/Practical%20advice%20at%20work/Ethics/socialmediaguidance.pdf - NMC (2015) *The code: standards of conduct, performance and ethics for nurses and midwives* http://www.nmc-uk.org/Nurses-and-midwives/Advice-by-topic/A/Advice/Social-networking-sites/ - RCN Code of Conduct - GMC Code of Conduct - Health Professionals Council Code of Conduct
Associated documents:	- Maidstone and Tunbridge Wells NHS Trust. *IT Acceptable Use Policy* [RWF-OPPCS-NC-TM8] - Maidstone and Tunbridge Wells NHS Trust. *Code of Confidentiality* [RWF-OPPCS-NC-TM3] - Maidstone and Tunbridge Wells NHS Trust. *Anti-Fraud Policy and Procedure* [RWF-OPPPCS-NC-WF48] - Maidstone and Tunbridge Wells NHS Trust. *Disciplinary Policy and Procedure* [RWF-OPPPCS-NC-WF10] - Maidstone and Tunbridge Wells NHS Trust. *Speak Out Safely (SOS) policy and procedure* [RWF-OPPPCS-NC-WF33] - Maidstone and Tunbridge Wells NHS Trust. *Bullying and Harassment Policy and Procedure* [RWF-OPPPCS-NC-WF24]

Version Control:		
Issue:	**Description of changes:**	**Date:**
1.0	Original document	August 2012
2.0	Corrected typing errors, added additional social media profiles, updated Setting up, managing and monitoring Trust social media profiles section	April 2016

Policy statement for

Social Media Policy

Maidstone and Tunbridge Wells NHS Trust (MTW / the Trust) recognises the vital benefits and importance of using social media to communicate and engage with patients, staff and stakeholders, promote the Trust and its services, help raise awareness of public health campaigns and support the Trust's emergency planning role.

This policy is not meant to deter Trust employees from using social media but to help employees understand their responsibilities and prevent them from bringing themselves, the Trust or the NHS into disrepute either inadvertently or intentionally and the potential consequences in doing so.

Staff should be aware of the information risks and good practices associated with the protection of sensitive information in social media and other social interaction scenarios.

Staff are reminded of confidentiality and data protection provisions inherent in contracts of employment. Staff must not disclose confidential information about the Trust or its services whilst using social media. These provisions do not affect staff's entitlement under the Speak Out Safely (SOS) Policy and Procedure (formerly Whistle Blowing).

Social Media Procedure

1.0 Introduction and scope

This policy and procedure applies to all staff, including bank, locum and temporary staff and contractors or agency workers working for, or on behalf of, the Trust.

The policy provides a general awareness of the associated risks of using both personal or MTW corporate social media profiles and how this may potentially affect the effectiveness of Trust services or damage the Trust's reputation.

2.0 Definitions

Social media is the term commonly used for websites that allow people to interact with each other in virtual communities, by sharing information, videos, images, opinions, knowledge and interests. As the name implies, social media involves the building of online communities or networks, encouraging participation and engagement.

Social networking websites (such as Facebook and Twitter*)* are perhaps the most well-known examples of social media, but the term covers other web-based services. Examples include:

- blogs (a contraction of the term web log - a regularly updated website or web page, typically run by an individual or small group, that is written in an informal or conversational style) and vlogs (a contraction of the term video log – a blog in which the postings are primarily in video form)
- audio and video podcasts
- 'wikis' (such as *Wikipedia*)
- message boards (forums)
- social bookmarking websites (such as *del.icio.us*)

- photo, document and video content sharing websites (such as Instagram, Flickr and YouTube)
- micro-blogging services (such as Twitter, Google+, LinkedIn, Facebook*)*
- Mobile messaging services (such as WhatsApp and video messaging application Snapchat

Blagging: the term commonly used to describe the deliberate, reckless and potentially criminal obtaining and/or disclosing of personal information about individuals without that person's knowledge or valid consent.

Trojan: a Trojan horse, or Trojan, is malware that appears to perform a desirable function for the user prior to run or install but instead facilitates unauthorized access of the user's computer system. *"It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems"*, as Cisco describes.

Malware: short for *malicious software*, is software designed to secretly access a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Phishing: is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by email or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to fool users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

Instant messaging (**IM**): is a form of real-time direct text-based communication between two or more people using personal computers or other devices, along with shared software clients. The user's text is conveyed over a network, such as the Internet. More advanced instant messaging software clients also allow enhanced modes of communication, such as live voice or video calling.

3.0 Duties (roles and responsibilities)

Staff should remember that all individuals are bound by the Common Law of Confidentiality and the NHS Confidentiality Code of Conduct. Failure to comply with this policy whilst blogging or using social media sites may result in disciplinary action being taken by the Trust that could, ultimately, depending on the seriousness of any breach, result in dismissal.

Staff and contractors should remember that they are ultimately responsible for their own online behaviour and must take care to avoid online content or actions that are inaccurate, libellous, defamatory, harassment, threatening or otherwise illegal. It is possible for staff or contractors to be subject to civil proceedings or criminal prosecution.

Staff and contractors must not disclose information that is or may be sensitive or confidential or that is subject to a non-disclosure contract or agreement. This applies to information about patients, other staff and contractors, other organisations, commercial suppliers and other information about the Trust and its business activities.

Employees should be mindful of the Trust's policies and procedures and Codes of Conduct that are part of their employment and professional requirements. These include:

- The confidentiality clauses in contracts of employment;
- The Trust's Disciplinary Policy and Procedure and Bullying and Harassment Policy and Procedure;
- Professional Codes of Conduct (e.g. Nursing and Midwifery Council, General Medical Council, Health Professions Council and the Royal College of Nursing).

Any breach of any of the above may be deemed gross misconduct and may result in disciplinary action being taken. Employees' actions may also have legal implications. They may be committing actionable defamation or breach of confidentiality. The latter could also have professional consequences.

Staff are also legally liable if they breach legislation relating to the gathering, storage or processing of data at all times. Therefore, everyone who manages or handles personal information within MTW must:

- understand that they are contractually responsible for following good data protection practice;
- be aware of their responsibilities and obligations to respect confidentiality
- be appropriately trained to do so; and
- be appropriately supervised

3.1 Communications Team

The Communications Team lead on all social media activity for the Trust, managing, updating and monitoring the Trust's corporate social media profiles and social media activity.

The Communications Team also help Directorates set up service social media accounts, train staff in managing and monitoring those profiles and provide basic reputation management, and tone and brand awareness training. In addition, they oversee the management of service-led social media profiles.

Through their role as social media lead, the Communications Team may, from time to time, identify comments or posts on social media from employees, which could potentially be inappropriate. In these circumstances the Communications Team will forward any relevant posts and associated information to the local / Directorate manager, and if appropriate HR, for them to follow up.

3.2 Managers

Where it has been identified a member of staff has potentially posted inappropriately, their line manager will handle any follow-up locally, and if relevant, seek advice from HR with regards to relevant HR policies.

3.3 Human Resources (HR)

HR will guide and advise local managers on HR matters in relation to any potentially inappropriate social media activity by a member of staff.

3.4 Information Governance

Information Governance provides a central point of information for all data protection matters. Information Governance provides training on the gathering, storage and processing of data to all staff.

4.0 Training / competency requirements

It is mandatory for all staff, including new starters, locum, temporary, students and contract staff members, to complete, on an annual basis, information governance training. The principles of confidentiality are covered in this training.

Staff wishing to set up and manage a corporate social on behalf of the Trust must receive training from the Communications Team.

5.0 The risks of social media and mitigations

5.1 Why are blogging and social networking an Information Governance issue?

The use of blogging and social networking websites by employees can expose the organisation to information risks, even where these sites are not accessed directly from work.

5.2 What are the potential dangers to the organisation of using blogging and social networking?

5.2.1 Unauthorised disclosure of business information and potential confidentiality breach

Blogging and social networking sites provide an easy means for information to leak from an organisation, either maliciously or otherwise. Once posted to a site, organisational information enters the public domain and may be processed and stored anywhere globally. In short, organisational control is lost and reputational damage can occur.

5.2.2 Malicious attack associated with identity theft

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

5.2.3 Legal liabilities from defamatory postings by employees

When a user registers with a site they typically have to indicate their acceptance of the site’s terms and conditions. These can be several pages long and contain difficult to read legal language. Such terms and conditions may 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 user is registering on a site from a PC within the Trust, it may be assumed that the user is acting on behalf of the Trust and any libellous or derogatory comments may result in legal action. 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.

5.2.4 Reputational damage

Ill-considered or unjustified comments or images left on sites may adversely affect public opinion toward an individual or the Trust. This can lead to a change in social or business status with a danger of consequential impact.

5.2.5 Malicious code targeting social networking users causing virus infections and consequential damage

Sites may encourage or require the download and installation of additional code in order to maximise the site’s functionality and potential value. Where sites have weak or ineffective security controls it may be possible for code to be changed to contain malicious content such as viruses and Trojans, or to trigger unintended actions such as phishing.

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

Sites can pose threats to the Trust’s information infrastructure. Particularly as the use of rich media (such as video and audio) becomes the norm in such sites, the bandwidth consumption generated by these sites can be significant and they have the potential to be the biggest bandwidth consumers within an organisation.

5.3 How has the Trust responded to these risks?

Whilst technical controls have been applied to block or control undesirable website usage the main defence against threats associated with using social media is user awareness.

Knowledge of the potential problems related to blogging and social networking will help employees in their safe use of such services and help protect the Trust.

5.4 Advice to help avoid problems when using social media

Appendix 4 aims to help employees use social media whilst maintaining a safe professional environment and protecting themselves and the Trust.

On registration, understand what you are signing up to and importantly what security and confidentially claims and undertakings exist. Watch for add-ons i.e. additional features or applications that change the terms and conditions of what you have signed up for, or that may require changes to the security settings of your devices.

Examine carefully any email coming from social networking sites or contacts as these may be unreliable containing malicious code or be spoofed to look as though they are authentic.

Please refer to Appendix 4 for a guide to the dos and don’ts on using social media.

5.5 Acceptable / inappropriate use

The Trust has a reasonable and lawful expectation that staff will not bring the Trust into disrepute. This is extended to the home environment as well.

Any grievance with the organisation or an individual who is employed directly by the Trust should be channelled through procedures and policies already in place and dealt with within the work environment.

If staff become aware of a breach in this policy, they have a duty to contact their line manager in the first instance, if it is appropriate to do so. It is possible such a matter may be resolved locally, although HR would act to support line managers if this was not the case and further action needed to be taken.

Work devices

Employees may access social networking sites, not blocked by the Trust, for personal purposes but should not do so during the working day. Staff should be mindful of the Trust Anti-Fraud Policy and Procedure in relation to using such sites for their own personal use, particularly in respect to abuse of Trust assets and property.

5.6 Personal devices

Employees accessing social media sites on their personal devices should not do so during working time.

Additional guidance for registered healthcare professionals

In addition to popular social networking sites such as Facebook and Twitter, there are a number of well-established sites aimed specifically at medical professionals, such as doctors, nurses, physiotherapists, medical students and occupational therapists.

Practical and ethical guidance is available from:

- British Medical Association (BMA) - http://bma.org.uk/-/media/Files/PDFs/Practical%20advice%20at%20work/Ethics/socialmediaguidance.pdf
- Nursing and Midwifery Council (NMC) – http://www.nmc-uk.org/Nurses-and-midwives/Advice-by-topic/A/Advice/Social-networking-sites/
- Health and Care Professions Council - http://www.hcpc-uk.org/Assets/documents/100035B7Social_media_guidance.pdf

Setting up, managing and posting to Trust corporate social media profiles

The Communications Team sets up, manages and runs all corporate Trust social media profiles.

The Communications Team is responsible for updating the main Trust profiles, which are:

Twitter: www.twitter.com/mtwnhs
Facebook: www.facebook.com/mymtwhealthcare
LinkedIN: www.linkedin.com/company/maidstone-and-tunbridge-wells-nhs-trust
NHS Choices:
www.nhs.uk/Services/Trusts/Overview/DefaultView.aspx?id=1178

The Communications Team also sets up Trust social media profiles for services and helps manage these alongside staff from that department. Examples of these profiles include:
www.facebook.com/pages/The_Wells_Suite
www.facebook.com/mtwmaternity
www.facebook.com/mtwchildrens
www.facebook.com/mtwpatientresearchambassador
www.twitter.com/mtwhealthphys

If your service or department is interested in managing a social media profile on behalf of the Trust, you must contact the Communications Team in the first instance. Under no circumstances should staff set up a corporate profile without prior approval from the Communications Team, or having received training from the Communications Team.

Information posted to Trust service or department social media profiles must have a corporate, professional tone and be relevant to patients, stakeholders and visitors using that service or department.

If you are aware of any Trust service or department that use social media, and they are not one of those listed above, please report these to the Communications Team.

You can contact the Communications Team at: mtw-tr.communications@nhs.net

01622 228658

Good practice tips to recognise and address potential problems associated with blagging

1. Be suspicious of all unsolicited contacts including phone calls, visits, faxed messages, email, SMS messages asking for information about other staff, contractors and patients.
2. Ensure you take steps to verify the identity of the caller/sender.
3. Do not provide information about the Trust, patients or other individuals unless you are certain of the recipient’s identity and authority to have the information requested.
4. Avoid disclosing personal or other sensitive information.
5. Don’t send personal or other sensitive information over the Internet unless you are completely confident in the website’s legitimacy and implemented security.

6. If you think you have been a victim of blagging ensure you immediately report this as an incident, in the first instance, to your line manager.

6.0 Monitoring and audit

This policy will be reviewed following ad-hoc incidents throughout the year.

APPENDIX ONE

Process requirements

1.0 Implementation and awareness

Communication plan

This policy needs to be communicated to all staff, this will be achieved by:

- Once ratified the PRC Chairman will email this policy/procedural document to the Clinical Governance Assistant (CGA) who will activate it on the Trust approved document management database on the intranet, under 'Policies & Q-Pulse'. Q-Pulse
- A monthly publications table is produced by the CGA which is published on the Trust intranet under 'Policies & Q-Pulse'; notification of the posting is included on the intranet "News Feed" and in the Chief Executive's newsletter.
- On reading of the news feed notification all managers should ensure that their staff members are aware of the new publications.
- Global communication and supporting documentation
- Making paper copies available
- Informing staff of the policy during Induction and IG training sessions

2.0 Review

The policy will be reviewed every three years. If substantive changes are required to the policy during this time it will be resubmitted to the review group.

3.0 Archiving

The Trust approved document management database retains all superseded files in an archive directory in order to maintain document history. Documents submitted as part of the Trust Information Governance Toolkit and similar audit returns will be retained for a minimum of three years.

APPENDIX TWO

CONSULTATION ON: Social Media Policy and Procedure

Please return comments to: Head of Communications

By date: 1 April 2016

Name:	Date sent	Date reply received	Modification suggested? Y/N	Modification made? Y/N
Local Counter Fraud Specialist	18/03/16			
Senior Information Risk Owner (SIRO)	18/03/16			
Caldicott Guardian	18/03/16			
Director of Health Informatics	18/03/16			
Information Asset Owners	18/03/16	18/03/16	Y	Y
Head of Legal Services	18/03/16			
Director of Human Resources	18/03/16	18/03/16	Y	Y
Head of Information Governance	18/03/16			
HR committee	18/03/16	19/04/16	Y	Y
Head of Emergency Planning & Response	06/07/16			
The role of those staff being consulted upon as above is to ensure that they have shared the policy for comments with all staff within their sphere of responsibility who would be able to contribute to the development of the policy.				

APPENDIX THREE

Equality Impact Assessment

In line with race, disability and gender equalities legislation, public bodies like MTW are required to assess and consult on how their policies and practices affect different groups, and to monitor any possible negative impact on equality. The completion of the following Equality Impact Assessment grid is therefore mandatory and should be undertaken as part of the policy development and approval process. **Please note that completion is mandatory for all policy development exercises. A copy of each Equality Impact Assessment must also be placed on the Trust's intranet.**

Title of Policy or Practice	Social Media Policy and procedure
What are the aims of the policy or practice?	To ensure all staff are aware of the responsibilities in respect to data protection
Identify the data and research used to assist the analysis and assessment	
Analyse and assess the likely impact on equality or potential discrimination with each of the following groups.	**Is there an adverse impact or potential discrimination (yes/no).**
Males or Females	No
People of different ages	No
People of different ethnic groups	No
People of different religious beliefs	No
People who do not speak English as a first language	No
People who have a physical disability	No
People who have a mental disability	No
Women who are pregnant or on maternity leave	No
Single parent families	No
People with different sexual orientations	No
People with different work patterns (part time, full time, job share, short term contractors, employed, unemployed)	No
People in deprived areas and people from different socio-economic groups	No
Asylum seekers and refugees	No
Prisoners and people confined to closed institutions, community offenders	No
Carers	No
If you identified potential discrimination is it minimal and justifiable and therefore does not require a stage 2 assessment?	
When will you monitor and review your EqIA?	At the time of review of the policy/procedure
Where do you plan to publish the results of your Equality Impact Assessment?	As Appendix Three of this policy/procedure on the Trust approved document management database

FURTHER APPENDICES

The following appendices are published as related links to the main policy /procedure on the Trust approved document management database:

No.	Title	Unique ID
4	Dos and don’ts regarding social media	RWF-OPG-CORP44

2. The Trust has corporate social media accounts on Twitter, Facebook, LinkedIn, YouTube and Google+.
3. All staff can access the policy online. Social media is covered in the face to face IG update training sessions. Where a member of staff has been designated an editor of a corporate Maidstone and Tunbridge Wells NHS Trust social media page, the communications team will meet with them to explain the necessary protocols and guidelines. The member of staff is advised to read the social media policy online.
4. 12 cases during the calendar years of 2012-2016.
5. This information can be found on the Trust website www.mtw.nhs.uk