Social Media – A Guide for Staff

This guidance is provided so that users and contractors of Central Manchester University Hospitals NHS Foundation Trust are aware of the organisational position and their personal responsibilities for the appropriate use of social media facilities they may access. Within the guidance are the uses of both NHS and other external websites and online blogging facilities.

This guidance is necessary since many employees and contractors enjoy sharing their knowledge and experience with others of similar roles and interests.

We encourage these online activities and acknowledge that staff and contractors 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 its public image and reputation and for the protection of its information assets of all kinds. This involves ensuring confidentiality and maintaining security in accordance with NHS Information Governance Policy and good practice.

This guidance applies to those members of staff that are employed by organisations accountable to Central Manchester University Hospitals NHS Foundation Trust. This guidance applies to all employees and workers including contracted, non-contracted, temporary staff, honorary contracts, secondments, bank staff, agency staff, students, volunteers and locums.

Terms used:

Social Media is the term commonly used for web-based and other mobile communications technologies that enable messages and opinions to be shared in dialogue with others.

Social Networking is the use of interactive web based sites or social media sites, allowing individuals on-line interactions that mimic some of the interactions between people with similar interests that occur in life. Popular examples include Facebook.com and Linkedin.com.

Social Engineering is 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's staff or maintenance contractor etc.

Blogging or Tweeting is using a public website to write an on-line 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, photographs or videos. Many blogs and tweets are interactive allowing visitors to respond leaving comments or to potentially send messages to 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. Examples of these websites include Twitter.com and Blogging.com.

Twitter is a 'microblogging' platform which allows users to post short messages (up to 140 characters in length) and converse with other users via their phones or web browsers. Unlike e-mail or text messaging on mobile phones, these conversations take place in the open.

The platform is experiencing a phenomenal adoption curve in the UK and being used increasingly by government departments, Members of Parliament, a number of our stakeholders, as well as millions of businesses, non government organisations and individuals. It is free to use with a relatively low impact on resources and has the potential to deliver many benefits in support of our communications objectives.

Blagging is the term commonly used for the deliberate, reckless and potentially criminal obtaining and/or disclosing of personal information about individuals without that person's knowledge or valid consent. Recent media reports allege that blagging is an issue that may particularly affect individuals who are of media interest but may potentially affect anyone.

The terms Social Engineering and Blagging are sometimes used interchangeably to describe methods of hacking into systems including phone services or where trickery is used to fool people into disclosing confidential information.

Troll/Trolling - Associated with internet discourse, trolls submit a deliberately provocative posting to an online message board with the aim of inciting an angry response. Any tweets, posts or replies which appear to be hostile or offensive should be reported to twitter/facebook etc immediately, then deleted.

YouTube is a video-sharing website on which users can upload, view and share videos. Most of the content on YouTube has been uploaded by individuals, although media corporations including CBS, BBC and other organisations offer some of their material via the site, as part of the YouTube partnership programme. Unregistered users may watch videos, and registered users may upload an unlimited number of videos. Videos that are considered to contain potentially offensive content are available only to registered users 18 years old and older.

Private use of Social Media:

Never update your status telling people you are on holiday or not at home. For reason of personal security and also insurance companies view this as not taking 'all precautions necessary to prevent a theft' and as such your home insurance could be void should your property be broken into.
Remember: The internet is a public resource. Once you put something on a social networking site the site owns all the rights to the information including the copy rights to all photographs.

Users and contractors of the Trust are ultimately responsible for their own online behaviour. Staff and contractors must take care to avoid online content or actions that are inaccurate, libellous, defamatory, harassing, threatening or may otherwise be illegal. It is possible for staff or contractors to be subject to civil proceedings or criminal prosecution.

It is important to remember that all Trust policies apply equally inside and outside of work hours when work related.

Users and contractors are not authorised on any social network to communicate by any means on behalf of Central Manchester University Hospitals NHS Foundation Trust unless this is an accepted normal part of their job, or through special arrangements that have been approved in advance with permission from your line manager and The Communications Department.

Sensitive and Confidential Information:

Users and contractors who use Social Media must not disclose information relating to Central Manchester University Hospitals NHS Foundation Trust which may be:

- Sensitive
- Confidential
- Third party personal data (information which identifies an individual). This could include comments about a person, photographs etc.
- That is subject to a non-disclosure contract or agreement. This applies to information about patients, other staff and contractors, other member organisations, commercial suppliers and other information about the Trust and our business activities.

Information Security:

Users and contractors must not share details of the member organisation's implemented security or risk management arrangements. These details are confidential and may lead to a serious breach of security occurring.

Departments considering using Social Media

If individual departments choose to set up their own social networking sites this must be agreed within their directorate/division. Provision must be put in place in advance to ensure that each site is managed appropriately. It is the responsibility of the individual department to ensure that queries/criticisms are dealt with in line with usual procedures and that the site(s) is maintained to a professional standard. The Communications Department must be alerted in advance if departments are considering setting up their own social media sites after consultation with Divisional Director.

Managers may choose that using Social Media as a means of communication as a benefit, however certain considerations must be made when scoping the use of Social Media.

Moderating the site must be done on the five working days of each week (Monday-Friday), in order that any malicious comments are removed as soon as possible. This must be undertaken within the department. Where possible it is advisable that departments check their account at the weekends/Bank Holidays too.

Disclaimers on a social media sites does not remove the member organisation's obligations to accuracy and implications.

Comments made to a social network site belong to the member organisation and therefore could be disclosed under the Freedom of Information Act 2000.

A plan must be in place to identify how the former issues are going to be addressed.

The plan should be sent to the directorate manager and Communications Department for their comments before finally being signed off by a director.

Freedom of Information Requests

When a member organisation (or department within a member organisation) creates a social network site such as Twitter or Facebook, the Information Commissioner has dictated that the organisation must be in a position to receive a Freedom of Information/Environmental Information Request via that medium and site.

To be valid, a request does not have to mention the FOI Act, but it does need to include a name and a means of contact. This could be just a name and an email address.

Any department who wish to run or are running such a site must undertake training in their ability to identify an FOI or EIR request. Any requests received should be forwarded as soon as possible to foi@cmft.nhs.uk

Additional Guidance for Staff at Work and Home

Staff may be aware of numerous cases reported in the media about inappropriate comments posted online by staff of various organisations. There has also been an increase of such incidents within the Trust. In order to protect staff from many of the common pitfalls, we have provided some guidance below:

- When registering with a website, understand what you are signing up to by reading the terms and conditions carefully and importantly determine what security, confidentially and liability claims, undertakings and exclusions exist.

- 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.

- Ensure 'Privacy' settings are set appropriately.

- Do not reply to messages or accept friend requests from people you don't know and especially patients.

- Never state your address, telephone number or date of birth.

- Respect others when using Social Networking sites.

- Social networking sites allow photographs, videos and comments to be shared with thousands of other users. However, it may not be appropriate to share work-related information in this way. For example, there may be an expectation that photographs taken at a private organisation event will not appear publicly on the Internet, both from those present and perhaps those not at the event.

- The use of photographs on websites, Facebook sites etc require written permission from the subject photographed or their parent/guardian. A consent form is available from your Communications Team.

- Staff should be considerate to their colleagues in such circumstances and should not post information when they have been asked not to. They should also remove information about a colleague if that colleague asks them to do so.

- Under no circumstance should inappropriate/derogatory comments be made about the organisation, the services provided, other staff, or any patients. This may amount to cyber-bullying.

- Staff must refrain from identifying Trust colleagues and patients by name.

- Do not post materials that could be considered discriminatory e.g. re gender, marriage or civil partnership, gender reassignment, pregnancy and maternity leave, sexual orientation, disability, race, colour, ethnic background, nationality, religion or belief and age.

- Don't say anything on-line that you would not say personally or wish others to hear.

- Remember: Once something is put on a social networking site, even if you delete it, there may be a record of it kept indefinitely.

In serious cases, disciplinary action may be taken against individuals who use social networking sites inappropriately.

Health professionals must also ensure that their use of social networking does not bring them into conflict with standards and codes of conduct published by their professional bodies. The NMC have produced guidance on how the code can be applied to the use of social networking sites. This can be accessed via the following link:
http://www.nmc-uk.org/Nurses-and-midwives/Advice-by-topic/A/Advice/Social-networking-sites/

Staff Side Organisations may also have useful guidance on the use of social networking sites, such as:

- www.rcn.org.uk/__data/assets/pdf_file/0008/272195/003557.pdf
- www.csp.org.uk/publications/social-media-guidance

Related Documents:

Standards of Business Conduct & Hospitality Policy
http://staffnet.cmft.nhs.uk/Policies/Corporate/Standards%20of%20business%20Conduct%20%20Hospitality%20PolicyOct%202011.pdf

Freedom of Information Procedure
http://staffnet.cmft.nhs.uk/Policies/Informatics/FOI%20Procedure.pdf

Internet and E-mail Use Policy
http://staffnet.cmft.nhs.uk/Policies/Informatics/Internet%20and%20E-mail%20Use%20Policy%20Version%202.3.1a.pdf

Mobile Phone Policy
http://staffnet.cmft.nhs.uk/Policies/Governance/ON9-3603-22-10-2013-10-18-20.pdf

Produced by: Communications Department (in partnership with Human Resources and Staff Side)
November 2013