Social Media Policy

Author	Not Available
Responsible Director	Managing Director
Ratified By	Quality and Safety Committee
Ratified Date	
Review Date	December 2015
Version	1.0
Policy consultation period	21.01.2015 – 20.02.2015

Related Policies & Guidelines:

- Disciplinary Policy
- Incident Reporting Policy

Contents

Amendment History

Version	Status	Date	Reason for Change	Authorised
1.0		December 2014	Initial policy for consultation	

1. Introduction

The Health Community is now making increased use of Social Networks to engage with their patients, service users and other stakeholders, and to deliver key messages for good healthcare and services generally. These online digital interactions are encouraged and their use is likely to be further extended as new communications channels become available.

This policy is provided so that staff and contractors of Central London Healthcare (CLH) are aware of their personal responsibilities for appropriate use of social media facilities they may access.

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

However, CLH has a responsibility to ensure the operational effectiveness of its business, including its public image, 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.

Staff and contractors whose role for CLH includes establishing, contributing to and maintaining official blogs and websites are guided through their individual job descriptions and related work instructions.

The information contained in this policy is based on the Department of Health Informatics Directorate NHS Information Governance: Information Risk Management Guidance: Social Interaction – Good Practice dated February 2012.

2. Scope

The policy applies to all CLH employees, temporary workers, students on placement and volunteers.

3. Definition and Terms Used

Social Networking is the term commonly given to websites and online tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests. It involves building communities or networks, encouraging participation and engagement. Social networking is also known as “social software”, “social computing” and includes (but not exclusively) the definitions as at Appendix 3.

4. Duties and Responsibilities

4.1 Private use of social media

Staff and contractors of CLH may use designated facilities provided by the organisation for their private Social Media purposes during their work breaks.

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

Staff are encouraged not to divulge who their employers are within their personal profile page (e.g. in accordance with the Royal College of Nursing (RCN) guidelines "RCN Legal Advice on using the internet"). However, those that do divulge their employer should state that they are tweeting/blogging etc. in a personal capacity.

Staff and contractors 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.

Staff and contractors are not authorised to communicate by any means on behalf of the organisation unless this is an accepted normal part of their job, or through special arrangement that has been approved in advance by the Senior Management Team. No social media sites or pages relating to CLH should be set up by staff and/or contractors without prior approval from the Board.

Staff and contractors who use Social Media must not disclose information of CLH that is or may be sensitive or confidential, 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 organisation and its business activities.

Corporate logos or other visible markings or identifications associated with CLH may only be used where prior permission has been obtained from the Senior Management Team.

Staff and contractors must not share details of CLH's implemented security or risk management arrangements. These details are confidential, may be misused and could lead to a serious breach of security occurring.

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

Unauthorised disclosure of confidential information would constitute misconduct /gross misconduct in accordance with CLH's Disciplinary Policy.

When using social networking sites, staff should respect their audience. As a general rule, staff should be mindful of any detrimental comments made about colleagues whilst using Social Media sites, e.g. failing to show dignity at work (harassment), discriminatory language, personal insults and obscenity. These examples are not exhaustive and will be considered a disciplinary matter.

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

4.2 Central London Healthcare use of social media

If staff want to convey news stories, events or messages through CLH's online corporate presence, then this must be done via the Senior Management Team.

A corporate twitter account has been created for positive news stories and should be accessed via the Senior Management Team.

5. Reporting Inappropriate Behaviour on Social Media

If a member of staff or contractor comes across information contained in Social Media sites that contravenes this policy, they should report the issue through the CLH Incident Reporting process.

All incidents will be investigated by the Management Team and appropriate action will be taken.

Appendix 1 – Potential Risks to CLH of Staff Using Blogging and Social Networking

A range of potential risks and impact consequences exist that staff and contractors of CLH should be aware of:

1. Unauthorised disclosure of business information and potential confidentiality breach

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

2. Malicious attack associated with identity theft

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

3. Legal liabilities from defamatory postings etc by staff

When a person registers with a website they typically have to indicate their acceptance of the site's terms and conditions. These can be several pages long and contain difficult to read and understand legal jargon. Such terms and conditions may potentially give the site "ownership" and "third party disclosure" rights over content placed on the site, and could create possible liabilities for CLH that allows employees to use them.

For example, where a staff member is registering on a website from a computer/electronic device within the organisation, it may potentially be assumed that the user is acting on behalf of the Trust and any libellous, inflammatory or derogatory comments may result in civil litigation or criminal prosecution. In addition, information being hosted by the website may be subject to other legal jurisdiction overseas and may be very difficult to correct or remove.

4. Reputational damage

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

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

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

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

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

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

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

Appendix 2 – Staff Guidelines on the Use of Social Media Sites

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 and importantly 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 contact details, date of birth, your profession, your organisation. Such information could put you at risk of identity fraud.
3. Think about what you want to use your online profile for, applying appropriate security and preferences settings as necessary.
4. Keep your password safe and avoid obvious ones that others might easily guess.
5. 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.
6. Do not say anything online that you would not say personally or wish others to hear.
7. Avoid unattributable anonymous comments.
8. Be suspicious of all unsolicited contacts. This can include phone calls, visits, faxed messages, email, SMS (Short Message Service) messages etc. from anyone asking about information about other staff, contractors, patients, service users or other potentially confidential information.
9. 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.
10. 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.
11. 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.
12. Do not send personal or other sensitive information over the Internet unless you are completely confident in the website's level of security/legitimacy The URL (Uniform Resource Locator) or web address of a website may at first glance look convincing and legitimate but could contain spelling errors or other variations i.e. ".co.uk" / "org.uk". "Secure" sites often have an "https" prefix in their web address and a padlock icon in the browser (where the browser supports this). The presence of these items may provide additional confidence that the site in question is legitimate and not a "spoof" or cleverly designed copy, intended to fool those who may overlook such detail.
13. In the event that you think you may have been a social engineering or blagging victim ensure you immediately report this as an incident in accordance with the organisation Incident Reporting Policy. Additional advice can be provided by the Information Governance Team where necessary. It is possible that a notice may be issued to other staff within the Trust with appropriate guidance to be alert to any new, unusual or suspicious activity.

Appendix 3 – Definitions

Social Media

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 who often share the same community interests. Such technologies can include blackberry messaging, instant messaging and other similar services etc.

Social Networking

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, Bebo, Myspace, Twitter and Linkedin.

Social Engineering

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.

Blagging

Blagging is 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. 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. Guidance is provided below in order to help clarify these issues for NHS organisations and their staff.

Blogging or Tweeting (micro-blogging)

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

Appendix 4 – References

NHS Information Governance: Information Risk Management Guidance: Social Interaction – Good Practice
http://systems.hscic.gov.uk/infogov/links/socnetworking.pdf