Use of Social Networking Websites Policy

START DATE:	March, 2013	**NEXT REVIEW:**	March 2015
COMMITTEE APPROVAL:	Joint Management Trade Union Committee		**CHAIR'S SIGNATURE:**  **STAFF SIDE CHAIR'S SIGNATURE:** 
	DATE: 14th February, 2013		
	ENDORSED BY: Consultative Committee		**DATE: 14 February 2013**
DISTRIBUTION:	Trust Wide		
LOCATION:	Intranet: Human Resources – Policies Folder		
RELATED DOCUMENTS:	IT Acceptable Use Policy Information Security Policy Web Communications Policy Media Policy		
AUTHOR / FURTHER INFORMATION:	Mary Sampson, Corporate HR Manager		
STAKEHOLDERS INVOLVED:	HUMAN RESOURCES, STAFF SIDE, GENERAL MANAGERS & DIRECTORS		

DOCUMENT REVIEW HISTORY:

Date	Version	Responsibility	Comments
Feb 2013	2	Mary Sampson	Section 4; Responsibilities of employees and personal conduct ; includes a comment on Trust values and bullying and harassment, Section 4.1 Security and identity theft: advice re: internet friends.
Jan 2011	1	Mary Sampson	

Chelsea and Westminster Hospital NHS Foundation Trust

Use of Social Networking Websites Policy

1.0 Introduction

This policy on social networking websites is in addition to the Chelsea and Westminster's Hospital NHS Foundation Trust's IT Acceptable Use Policy and Information Security Policy. The Information Technology Acceptable Use Policy categorises acceptable and unacceptable usage of the Trust's email and internet systems.

As employees are aware, the internet at work is intended solely for use in conducting Trust business. However, the Trust recognises that many employees use the internet for personal purposes and that many employees participate in social networking on websites such as Facebook, Twitter, MySpace, Bebo and Friendster. The Trust does not permit access to social networking sites at work, however, it is recognised that many staff access these sites outside of work in their private lives.

The purpose of this policy is to outline the responsibilities of employees using the internet to access social networking websites at any time to ensure that their personal conduct and behaviour using these forums does not raise concerns for the Trust, its patients or staff

2.0 Scope

This policy will apply to all employees of the Trust, staff with honorary contracts, students, voluntary workers, contractors, seconded staff, bank and agency staff.

This policy does not cover any exceptional use of these sites for service purposes which must be authorised by the relevant Divisional Director of Operations, IMT Director and Head of Communications.

3.0 Definitions

The term Social Networking is used to cover such internet sites as Facebook, MySpace and Bebo. It also includes blog sites, internet homepages and other interactive services.

The term Blogging is used to describe a public website that is used to write an online diary e.g. Twitter.

4.0 Responsibilities of employees and personal conduct

According to the Trust values launched in May, 2012 all staff are required to treat all hospital related information safely and with respect. At the same time the hospital must also ensure that confidentiality and its reputation are protected. The Trust respects an employee's right to a private life. However, Trust employees will not use or maintain a social networking site that contains:

- Person identifiable information of Trust patients and /or their relatives. This does not preclude staff having pictures of patients on their site if they are a relative; however this should not be a photograph taken of them whilst they are a patient at the Trust..
- Photographs of Trust patients and/or their relative's person identifiable information of another Trust employee in relation to their employment including judgements of their performance and character.
- Photographs of another Trust employee taken in the work situation or in their working uniform.
- Statements that brings the Trust, its services, it's staff or contractors into disrepute. This includes any statements, pictures or comments which could be construed or interpreted as abusive or derogatory or which could be understood as constituting the harassment and bullying of a work colleague.
- When registering with a website from a Trust Device, employees must read the site's terms and conditions. No employee can sign up to terms and conditions of a website unless they have authorisation from the Information Governance Team. NB. Social networking sites are not permitted to be accessed whilst at work and have an IT block.
- Trust confidential or business information must not be loaded onto a personal social networking site.
- Examine carefully any email or message coming from social networking sites or contacts as these may be unreliable containing malicious codes, be spoofed to look authentic or a phishing email.
- Ensure that they do not conduct themselves in a way that is detrimental to the employer; and
- Take care not to allow their interaction on these websites to damage working relationships between members of staff and patients at the hospital.

4.1 Security and identity theft

Employees should be aware that social networking websites are a public forum, particularly if the employee is part of a "network". Employees should not assume that their entries on any website will remain private even if carried out outside of the Trust IT environment.

Employees should be careful about what they write about online and should give careful consideration to their online privacy settings and their choice of internet "friends"

Employees must be security conscious and take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, employees should:

- Ensure that no information is made available that could provide a person with unauthorised access to the Trust and/or any confidential information; and
- Refrain from recording any confidential information regarding the Trust on any social networking website.

5.0 Trust Policies and Codes

The Trusts Information Technology Acceptable Use policy outlines clearly what is regarded as unacceptable use of the internet at work. This policy states that any inappropriate personal conduct or behaviour using internet sites will lead to disciplinary action if it brings the Trust's reputation into disrepute or exposes it to potential liabilities.

There are a number of other Trust policies detailed in Appendix 1 which staff need to be mindful of when participating on social networking sites.

6.0 Monitoring of internet access at work

- C&W NHS FT will ensure that the network is monitored for potential security breaches. All monitoring will comply with current legislation.

The Trust considers that valid reasons for checking an employee's internet usage include suspicions that the employee has:

- been spending an excessive amount of time viewing websites that are not work-related; or
- acted in a way that damages the reputation of the Trust and/or breaches confidentiality.
- The Trust will ensure IT engineers constantly review all devices and application logs on a daily basis.

7.0 Monitoring of sites

The Trust monitors employees' internet use to ensure that it is in accordance with IT Acceptable Use policy and this policy. Access to the web may be withdrawn in any case of misuse of this facility.

Disciplinary action will be taken against employees who bring either the Trust and/ or its staff into disrepute and in accordance with the Trust's disciplinary policy leading to potential dismissal for gross misconduct.

Appendix 1

1.0 Other Trust Policies and Codes

Under the Trust's Confidentiality Code of Conduct for Staff, employees have a duty to ensure that all patient and staff information is processed fairly, lawfully and as transparently as possible and have a right to access any information held about them. In common law, there is an implied duty of trust and confidence between an employer and an employee. Employees who have access to confidential information should be aware that any misuse of this information and that inadvertent disclosure could result in disciplinary action, bringing into question professional registration and possibly result in legal proceedings.

The Trust 's Harassment & Bullying in the Workplace sets out the right of all employees to be treated with dignity and respect at work and advises on employee behaviour that could cause distress and anxiety to others in the workplace, including activity taking place on social networking websites. Harassment at work is unlawful under a number of Acts and these are referred to in the Equality and Diversity Policy.

If an employee is subjected to harassment because of protected characteristics (with the exceptions of marriage and civil partnership, and pregnancy and maternity), he or she may have grounds to bring a complaint to an employment tribunal under the relevant anti-discrimination legislation. It should be noted that the potential for harassment can take place in online environments such as social networking websites and as such employees must refrain from mentioning members of staff personal information on such sites. Any breaches will be considered as gross misconduct under the Trust's Disciplinary Policy.

This Web Communications Policy sets out the Trust's processes for maintaining the accuracy and quality of information on the Trust website, information about the Trust on other websites such as NHS Choices, and our social media profile on websites such as Twitter and is managed by PR and Communications Department.

This Media Policy sets out the Trust's processes for handling media enquiries, both in and out of hours, and what staff should do when they are contacted by the media in their capacity as a Trust employee, as an expert in their field (for example in a particular medical or surgical specialty), or as a representative of another body (for example a professional organisation, a trade union, or a charity).

It also sets out the process for Foundation Trust Governors speaking to the media and introduces the Trust's process for VIP visits and other events.

2.0 A summary of the laws relating to this document

Leading statutory authority

Equality Act 2010
Defamation Act 1996
Data Protection Act 1998
Human Rights Act 1998
Regulation of Investigatory Powers Act 2000
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)

Employment Practices Data Protection Code (PDF format, 5.5MB) (on Information Commissioner's website)

The Regulation of Investigatory Powers Act 2000 and Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 allow employers to investigate or detect the unauthorised use of its telecommunication system, including internet use.

The Data Protection Act 1998 will also apply if the monitoring of internet use involves the processing of information from which an individual can be identified. The Employment Practices Data Protection Code (PDF format, 5.5MB) (on the Information Commissioner's Office website) provides guidance on how employers can meet the Act's requirements.

Employers should also take into account art.8 of the European Convention on Human Rights (listed in sch.1 of the Human Rights Act 1998), which covers the right to respect for private and family life.

An employee who makes a defamatory statement that is published on the internet may be legally liable for any damage to the reputation of the individual concerned. An employer may be vicariously liable for the acts of an employee done in the course of employment, even if performed without the consent or approval of the employer. A company can sue if a defamatory statement is made in connection with its business or trading reputation.