Hull NHS
Teaching Primary Care Trust

Hull Teaching Primary Care Trust

INTERNET USE POLICY

06.02.08

CONTENTS

INTRODUCTION

The purpose of this policy is to ensure the appropriate use of the Trust's Internet system and make users aware of what the Trust deems as acceptable and unacceptable use of its Internet system. By following the guidelines in this policy, the Internet user can minimise the legal risks involved in the use of Internet.

This document defines the Internet Use Policy for Hull Teaching Primary Care Trust. The Internet use Policy applies to all users of the Internet and relevant people who support the Internet system. The Internet is a general term that covers access to numerous computers and computer systems worldwide that are accessed electronically. Such systems include the World Wide Web (WWW), email (See Email Policy), File Transfer Protocol (FTP), newsgroups, Gopher, Intranet etc.

This document:

- Sets out the Trust's policy for the protection of the confidentiality, integrity and availability of the Internet system.
- Establishes organisational and user responsibilities for the Internet system.
- Provides reference to documentation relevant to this policy.

1. OBJECTIVES

The objective of this policy is to ensure the security of Hull Teaching Primary Care Trust Internet system. To do this the Trust will aim to (via HMHTT IT services):

1.1. Ensure availability
Ensure that the Internet system is available for users.

1.2. Preserve integrity
Protect the Internet system from unauthorised or accidental modification ensuring the accuracy and completeness of the Trust's assets.

1.3. Preserve confidentiality
Protect assets against unauthorised disclosure.

1.4 Employees should be aware that inappropriate use of the Trust's Internet system whether under this policy or otherwise may lead to disciplinary action being taken against an employee under the Trust's disciplinary procedures which may include summary dismissal.

1.5 Any non employee user as described in point 2 found to be using the Internet inappropriately will have access withdrawn and usage will be investigated which may lead to the individual being asked to leave the Trust.

1.6 Patient and clinical care are paramount to the Trust and must take precedent over all non business internet traffic, therefore if it is found that non business use of the internet is having a detrimental impact on clinical care then internet access will be withdrawn were necessary on a site by site basis.

2. Scope

This procedure applies to all PCT employees and any other person on Trust business irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership. All employees will be treated in a fair and equitable manner and reasonable adjustments will be made where appropriate (e.g. interpreter or signing provision, access arrangements, induction loop, etc.).

This policy applies to:

- All employees of the Trust
- Board and Professional Executive Committee (PEC) members and locality boards
- Contracted Third Parties (including Agency staff)
- Students and trainees
- Staff on secondment and other staff on placement within the Trust
- Staff and partner organisations (including Trade Unions) with approved access
- GP's and all practice staff
- Any other individual on Trust business

3. Roles and Responsibilities

3.1. The Trust will take all reasonable steps to ensure that users of the Internet service are aware of policies, protocols, procedures and legal obligations relating to the use of Internet. This will be done through training and staff communications at departmental and Trust team brief sessions. For new starters the policy will be included in the pack received at induction training.

3.2. The overall responsibilities for Information Governance are as follows and if advice is required the following can be contacted:

- Line Manager
- Director of Governance, Performance and Informatics – Board Level and Information Governance Lead
- Medical Director – PCT Caldicott Guardian
- Head of IM&T – IT Lead and day to day issues

4. ACCESS TO THE INTERNET SYSTEM

4.1. Access to the Trust Internet is granted when the employee's line manager requests the user be set up, usually as a new starter or when moving from a different Trust. This access comes as part of a package and the user will also receive email and U drive access. Upon the line manager requesting access for this 'package' it is the line manager's responsibility to ensure the member of staff is aware of the policies that apply to usage.

5. ACCEPTABLE & UNACCEPTABLE USE OF INTERNET

5.1. Best practice Summary

The Trust considers the Internet as an important means of communication and recognises the importance of appropriate Internet content and speedy replies in conveying a professional image and delivering good customer service. Use of the Internet for personal use should be limited to approved break periods (if any) or conducted within your own time. Counter Fraud & Security Management Services (CFSMS) may be involved in any investigation that the PCT instigates and as such if anybody believes that a PC is being used inappropriately in any way they must not use that particular PC at all and seek immediate advice from Head of IM&T or Security Manager.

Users must adhere to the following guidelines:

5.2. Acceptable Internet Usage

5.2.1. To access research material and other information relevant to your work.

5.2.2. To access web sites for personal use as long as this does not interfere with work or degrade the network speed and is conducted within approved break periods (if you have any) or in your own time and does not incur any cost to the Trust.

5.2.3. Authorised ordering, procuring of goods for Trust business.

5.3. Unacceptable Internet Usage

5.3.1. Creating, downloading or transmitting (other than for appropriately properly authorised and lawful research) any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

5.3.2. Creating, downloading or transmitting (other than for appropriately authorised and lawful research) any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material.

5.3.3. Creating, downloading or transmitting material that is designed to annoy, harass, bully, inconvenience or cause needless anxiety to other people.

5.3.4. Creating or transmitting “junk-mail” or “spam”. This means unsolicited commercial web mail, chain letters, jokes or advertisements. If these types of mails are received they should be deleted and not forwarded to other users.

5.3.5. Using the Internet to conduct private or freelance business for the purpose of commercial gain.

5.3.6. Creating, downloading or transmitting data or material that is created for the purpose of corrupting or destroying other user’s data or hardware.

5.3.7. Downloading streaming video or audio for entertainment purposes.

5.3.8. Downloading and/or installing any software from the Internet without obtaining written authorisation from Head of IM&T or Service Desk Manager.

5.3.9. The use of sites that allow users to pick up personal emails (i.e. Hotmail etc) are not permitted and will be blocked via network software due to potential risks imposed on the NHS network.

5.3.10. The use of some sites have been blocked (i.e. ebay) and others may be blocked on an ongoing basis if deemed necessary by either Head of IM&T or under guidance from HMHTT Infrastructure team if they are deemed to be having a detrimental impact on the network usage. Requests for a site to be unblocked for legitimate work purposes must go to the IT Helpdesk via Line Managers.

5.3.11. Using the Internet for any kind of chat room, myspace etc.

5.4 Procuring on the Internet

The Trust does not accept any liability for anyone using the Internet for personal use to order, procure goods for personal use or internet banking.

6. SYSTEM MONITORING

6.1. All Internet traffic is logged automatically (each site a user visits is included in the log, with the time visited and pages viewed) on each PC The Trust also uses software that prevents users visiting sites that may contain illegal and/or pornographic material or would have a known detrimental effect on bandwidth.

6.2. The Trust also has portable equipment that can be located at any site and will monitor all users access to Internet. All Trust sites will be covered periodically and reports produced for relevant managers.

7. EMPLOYEES RESPONSIBILITIES

7.1. To abide by and ensure adherence to Trust Policies and not to abuse use of the Internet.

7.2. If you have any questions or comments about this Internet use Policy, please contact the Hull IT Servicedesk (by email) its.servicedesk@hullpct.nhs.uk If you do not have any questions the Trust presumes that you understand and are aware of the rules and guidelines in this Internet Use Policy and will adhere to them.

7.3. To report any information security breaches via the Trust's incident reporting system.

7.4. To attend mandatory training regarding Information Governance

7.5. To comply with the Trust's code of conduct for employees in respect of Confidentiality and Information Security and the Caldicott and Data Protection Policy when using the Internet, both documents are available on the Trust's Intranet.

8. DEFINITIONS

8.1. Defamation & libel

What is defamation & libel?

A published (spoken or written) statement or series or statements that affects the reputation of a person (a person can be a human being or an organisation) and exposes them to hatred, contempt, ridicule, being shunned or avoided, discredited in their trade, business, office or profession, or pecuniary loss. If the statement is not true then it is considered slanderous or libellous and the person towards whom it is made has redress in law.

What you must not do

Make statements about people or organisations on any web pages you are including on the website without verifying their basis in fact.

What are the consequences of not following this policy?

Individuals and the Trust may be subject to expensive legal action.

8.2. Harassment

What is harassment?

It is important to clarify the distinction between the terms bullying and harassment as this is an area which causes confusion.
The Trust has a policy on Bullying and Harassment that you should refer to and can be found on the Intranet
The Advisory, Conciliation and Arbitration Service (ACAS) definitions state:

- Harassment, in general terms, is unwanted conduct affecting the dignity of men and women in the workplace
- It may be related to age, sex, race, disability, religion, sexual orientation, nationality or any personal characteristic of the individual, and may be persistent or an isolated incident
- The key is that actions or comments are viewed as demeaning and unacceptable to the recipient
- Bullying may be characterised as offensive, intimidating, malicious or insulting behaviour, an abuse or misuse of power through means intended to undermine, humiliate, denigrate or injure the recipient
- Bullying or harassment may be by an individual or involve groups of people
- It may be obvious or it may be insidious

What you must not do

Use the internet to harass other members of staff by displaying particular web sites that they consider offensive or threatening.

What are the consequences of not following this policy?

The Trust deals with harassment by providing advice, support and mediation. Those perpetrating harassment can also be made subject to the Trust's Disciplinary procedure. Any proven case of harassment will result in

disciplinary action against the guilty party which could ultimately lead to their dismissal.

8.3. Pornography

What is pornography?

Pornography can take many forms, for example written descriptions, still and moving images, cartoons and sound files. Some pornography is illegal in the UK and some is legal. Pornography that is legal in the UK may be considered illegal elsewhere. Due to the global nature of Internet, these issues must be taken into consideration. Therefore, the Trust defines pornography as the description or depiction of sexual acts or naked people that are designed to be sexually exciting. The Trust will not tolerate its facilities being used for this type of material and considers such behaviour to constitute a serious disciplinary offence.

What you must not do

- Create, download or transmit (other than for properly authorised and lawful research) pornography.
- Send or knowingly forward web mails with attachments containing pornography. If you receive a web mail with an attachment containing pornography you should report it to the (IM&T) Security officer or your Line Manager.

What are the consequences of not following this policy?

- Users and/or the Trust can be prosecuted or held liable for transmitting or downloading pornographic material, in the UK and elsewhere.
- The reputation of the Trust will be seriously questioned if its systems have been used to access or transmit pornographic material and this becomes publicly known.
- Users found to be in possession of pornographic material, or to have transmitted pornographic material, will be subject to an investigation which may lead to disciplinary action and ultimately dismissal. Police action may also be taken

8.4. Copyright

What is copyright?

Copyright is a term used to describe the rights under law that people have to protect original work they have created. The original work can be a computer program, document, graphic, film or sound recording, for example. Copyright protects the work to ensure no one else can copy, alter or use the work without the express permission of the owner. Copyright is sometimes indicated in a piece of work by this symbol ©. However, it does not have to be displayed under British law. So a lack of the symbol does not indicate a lack of copyright. In the case of computer software, users purchase a licence to use the work. The organisation purchases licences on behalf of its users.

What you must not do

- Alter any software programs, graphics etc without the express permission of the owner.
- Claim someone else's work is your own
- Send copyrighted material by the Internet without the permission of the owner. This is considered copying.

What are the consequences of not following this policy?

- A user and/or the Trust can face fines and/or up to two years imprisonment for infringing copyright.

9. POLICY ACCEPTANCE

All staff contracts explicitly state that Trust policies will be adhered to therefore acceptance of this policy by Trust staff is mandatory.

10. ASSOCIATED DOCUMENTATION

10.1 Policies:

Bullying and Harassment policy and procedure
Email Policy
Confidentiality and Information Security
Caldicott and Data Protection

11. REVIEW

11.1 This policy will be reviewed every 2 years

Author: Tracy Meyer
Title: Head of IM&T
Date: January 2008

Approved by: Date:

Reviewed by: Date: