Heart of England NHS
NHS Foundation Trust

POLICY ON THE USE OF THE INTERNET

META DATA

Policy Title:	**POLICY ON THE USE OF THE INTERNET**
Date:	**JUNE 2006**
Review Date:	**JUNE 2008**
Created by:	**Head of ICT**
Source:	**ICT Director**
Stored Centrally:	**Trust Intranet**
Linked Trust Policies:	**Disciplinary Policy** **Grievance Policy** **Data Protection Policy** **Induction Policy** **ICT Policy and Procedures**

TABLE OF CONTENTS **PAGE**

1. Circulation

This Policy and associated procedures apply to all persons working within the Heart of England NHS Foundation Trust that access the Internet using Trust systems.

This includes (but not exclusive to):

- Permanent staff
- Temporary (including students, locums, contract staff)
- Honorary staff
- Visiting staff
- Non Executive Directors

2. Introduction

This policy identifies the formal position of the Trust and standards for use in connection with access to the Internet/Intranet.

All use of the Trust's Internet facilities is governed by the terms of this policy.

It is designed to protect users and to limit risks to the Trust associated with corporate and personal liability under relevant legislation e.g. Data Protection Act 1998, Freedom of Information Act 2000, Computer Misuse Act 1990.

Internet facilities are made available to users for the following purposes:

- Trust corporate and business processes
- To support patient care
- Management
- Research
- Education and Training

A certain amount of personal use by staff is allowed but must be kept to a minimum and usage will be monitored.

3. Policy Objectives

The objectives of this policy are to:

- Ensure all Users are informed of what constitutes "acceptable use" and their legal and ethical responsibilities

- Establish and maintain standards and procedures for the use of the Service

- Reduce the potential liabilities arising form misuse. As an employer, the Trust may be liable for employees actions if committed "in the course of employment" and the employee may also be personally liable

- Maintain the confidentiality, integrity and availability of information stored, processed and communicated

- Provide a technically secure environment for all information that is accessed or made available via the Internet.

4. Scope of the Policy

This policy relates to access to the Internet using Microsoft Internet Explorer.

No other type of Internet software is to be installed or used on Trust PC's.

Under certain circumstances some areas may have direct control of local systems for which they retain responsibility for maintenance, configuration and security. ICT Directorate Policies and Procedures will provide the template to enable local responsibilities and adherence to Trust and National requirements.

5. Legislative Framework

All Users must recognise that there is a clear legislative framework affecting the use of the Internet by the Trust.

The key legislation is the Computer Misuse Act 1990. Breach of its provisions (outlined in the Inappropriate Use section) may also amount to the commission of an offence.

Users should be aware that any access personal access to the Internet will be subject to the provisions of these Acts.

6. Responsibilities

All Users must comply with this Policy at all times (including use of the Intranet/Internet whilst off duty).

Any failure to comply is likely to lead to investigation which may lead to disciplinary proceedings.

Any breaches relating to this Policy must be reported using the published ICT Incident Reporting Policy.

7. Risks

7.1 Unauthorised Access

Access to the Internet is routed via NHSnet.

Trust systems are protected against unauthorised public access by the use of a Firewall.

7.2 Malicious Software

There is a risk of infection from computer viruses or damage from other software when files are transferred or downloaded and pose a substantial risk to the integrity of Trust systems.

The Trust's systems are designed to protect against these dangers with virus checking but this does not mean that Users should not take sensible precautions when using the Internet.

8. Inappropriate Use

Under no circumstances may Users access Internet sites that are clearly inappropriate.

Examples include, but are not limited to:

- Obscene or pornographic material
- Discriminatory material (on grounds of sex, race, disability, sexual orientation, age, religion or otherwise)
- Material considered pertinent to the commission of crime, terrorist acts and illegal drugs
- Use of the Internet for the sale or purchase of items via auction sites
- Posting material on the Internet or sending messages that could bring the Trust into disrepute

As a guideline, “inappropriate sites” are those that could cause offence to colleagues or which could bring the Trust into disrepute.

The Trust will be the final arbiter of what is or is not offensive material, except where a criminal investigation is involved.

9. Conditions of Use

Users should regard Internet access as a privilege and Heart of England NHS Foundation Trust places trust in its staff to exercise this privilege in their own time, without detriment to their job and in accordance with the conditions outlined in this policy.

Users are informed that Internet access is routinely monitored and that action may be taken if used inappropriately.

10. Obtaining Internet Access

To gain access to Trust systems, the following form must be completed which can be found at:

http://clininfodbs/formtracking/FullApplication.asp.

.

11. Constraints

Once Internet access has been approved, Users will be required to abide by the following guidelines:

- Internet facilities should be limited to Trust business

- Limited use is allowed for personal use but this is subject to the demands of the organisation and working requirements

- It must be emphasised that personal use of the Internet is at the discretion of the Trust and may be withdrawn if widespread abuse of the system is found

- Staff will not make use of the Internet (or their access to the Internet) for any purposes which might be considered to contravene legislation or any stated policy of the Trust or which might be considered offensive to any other member of the Trust

12. File Formats

The following generic file formats are indicative of the types that may be downloaded:

- 12.1.1 Microsoft Word (.doc)
- 12.1.2 Microsoft Excel (.xls)
- 12.1.3 Microsoft Access (.mdb)
- 12.1.4 Microsoft PowerPoint (.ppt)
- 12.1.5 Microsoft Publisher (.pub)

- 12.1.6 Adobe Acrobat (.pdf)
- 12.1.7 Text Files (.txt)
- 12.1.8 Rich Text Format (.rtf)

This is not an exhaustive list. For further guidance, refer to the ICT Department.

13. Trust Email Addresses

Trust staff are discouraged from providing their Trust Email address when using public Internet sites for activity not associated with Trust business.

14. Blocked Internet Sites

Access to certain Internet sites is automatically blocked.

A User who attempts to access a blocked site will have a message displayed on their PC to that effect.

The access attempt will be logged and reported to the Information Security Manager/appropriate personnel as a breach of the Trust Internet policy.

If a User or group of Users has a business requirement to access sites that they consider should not be blocked, they should contact the Information Security Officer for a final decision.

15. Security

Users must not seek to gain unauthorised access to confidential data or to restricted areas of the Trust's network.

All Users are responsible for their own passwords.

Allowing another User to use the Internet using your User Name or Password is considered to be misuse of the Internet and may be subject to disciplinary action by the Trust.

16. Monitoring

The Trust reserves the right to monitor Internet usage.

There may be occasions when there is evidence that inappropriate Internet use is taking place. In such cases, the Trust may monitor Internet usage, without giving notice to the individual concerned.

17. Copyright and Intellectual Property Rights

Material on the Internet is subject to the same restrictions as written material in books, magazines or other paper materials with respect to copyright and intellectual property rights.

Users must seek permission from the relevant parties to use any material not owned by Heart of England NHS Foundation Trust.

Users have a responsibility to ensure that copyright and licensing laws are not breached when downloading, copying or transmitting to third parties works of others without their consent.

Any breach of these laws may result in both the user and the Trust being liable to prosecution.

18. Personal Use

The Trust Internet Access system is intended primarily for business use.

Facilities are made available to users for the following purposes:

- Trust corporate and business processes
- To support patient care
- Management
- Research
- Education and Training

Personal use must not be to the detriment of normal work or contractual requirements

The amount of personal use must not be such that it causes disruption to legitimate business use by other Users of the system

Accessing non Trust Email accounts e.g. Yahoo, Hotmail, AOL is strictly prohibited

19. Password Control

Users must not disclose their password to anyone else.

Disclosure of passwords is a disciplinary offence. Where a User is discovered to be disclosing their password a report will be sent their Manager and copied to the Information Governance Manager and Human Resources.

Users must not attempt to use another Users user profile and password. Offenders may be subject to the Trust's disciplinary procedure.

Users must not permit any other person to access and use the Internet or their Email address.

20. Viruses

The intentional introduction/sending or downloading of files or attachments which contain viruses or which are mean to compromise the Trust's systems is a serious breach of Trust policy.

This will result in disciplinary action which could result in dismissal and prosecution under the Computer Misuse Act.

21. Monitoring

The Trust will actively monitor Internet Access usage.

Staff who may have concerns about this may contact the Information Security Officer or Information Governance Manager at any stage to discuss their concerns.

22. Performance Review

The Trusts Internet Access Policy will be reviewed in line with Information Governance reporting requirements.