Tees, Esk and Wear Valleys NHS
NHS Foundation Trust

Internet Policy

Ref IT-0007-v6

Status: Ratified
Document type: Policy

Contents

1 Why we need this policy

1.1 Purpose

This policy also helps the Trust comply with legislation and NHS security regulations relating to controlled connections to national computer networks:

- HSCIC Statement of Compliance (this will change to HSCN with effect from 1/4/17)
- Computer Misuse Act 1990
- Sexual Offences Act 2003
- EU Privacy and Monitoring Directive 2000
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- Private and Electronic Communications (EC Directive) Regulations 2003
- Crime and Disorder Act 1998

1.2 Objectives

- This document explains the policy and procedure that governs use of the *Internet* and *World Wide Web* within the Trust.
- Compliance with this policy will ensure that access to the Internet will be available and responsive to the business needs of the Trust.

2 Scope

2.1 Who/what this policy applies to

- This policy applies to all authorised users of the Trust's computer network (including all permanent and temporary employees of the Trust, volunteers, agency staff, agents, subcontractors, consultants, and third party vendors).
- There are a number of ways to access the Internet via the Trust's network including the Guest Wi-Fi, guest access should only be used by partner agencies, professional service providers and other official business users. It is not to be used by staff, patients or their friends and families. More details on the Guest network can be found in the Access to Information Systems Policy
- A valid user account is required to access the Trust's computer network (subject to an individual completing the Trust's prerequisite network training unless using the Guest Network).

- Trust Smart Phones can also be used to access the Internet, but can access the internet directly via the mobile providers network and therefore have different filtering rules applied, so it may be possible to access a site via a smart phone that is blocked on the Trust network. Trust staff who are issued with smart phones are still expected to abide by this policy and the acceptable use set out within it.
- This Policy does not apply to the Patient Access to the Internet system, that has its own procedure, but like the Guest Wi-Fi, the PATTI network is not intended for staff use.

2.2 Roles and responsibilities

Role	Responsibility
All users of the Trust's computer network and smart phones	• Adhering to this policy
The Trust	• Legal responsibility for Internet access control and monitoring.

- No deviation whatsoever can be sanctioned from the statutory and legal obligations of the Trust.
- Any breach of this policy by users will be regarded as misconduct, and will be subject to the Trust's disciplinary policy.

3 Policy

3.1 Acceptable Use

- The Trust provides access to the Internet as a tool to support its business activities. Users may access the internet for reasons related to Trust business, this includes streaming video and audio.
- Users may access the Internet for limited personal use. Such use should preferably be restricted to outside of normal working hours and during breaks.

⚠ Business use of the Internet takes precedence over personal use at all times.

⚠ Personal use of the internet must not:

- Consume a significant amount of resources, including staff time;
- Interfere with staff productivity or performance;
- Involve significant costs to the Trust;
- Detrimentally affect the Trust's business interests, reputation, or cause loss of goodwill to the Trust;
- Pose any risks to the integrity, security and confidentiality of the Trust's corporate and clinical systems.

3.2 Unacceptable Use

ⓘ Users cannot:

- Visit *websites* that contain indecent, obscene, pornographic or offensive materials;
- Make or post indecent remarks, proposals or materials on the Internet;
- Upload, download, or otherwise transmit:
    - any defamatory, sexist, racist, offensive or unlawful material;
    - material that is designed to annoy, harass, bully, inconvenience, intimidate or cause needless anxiety to other people;
    - material with malicious intent;
    - unlicensed commercial software or copyright materials;
- Download unauthorised software—including MP3 and other types of music files, games, videos, freeware, shareware or evaluation software;
- Download streaming video or audio media for entertainment purposes, including listening to Internet-based radio stations; Please note that streaming is allowable for business use or professional interest.
- Access the Internet for any illegal purposes;
- Reveal or publicise in any way sensitive corporate and confidential patient information;
- Visit websites associated with gambling, online auctioning, peer-to-peer file sharing, and online gaming;

- Use the Internet to conduct private or freelance business, or for personal gain;
- Represent personal opinions as those of the Trust;
- Intentionally interfere with the normal operation of the computer network, including the propagation of computer viruses and sustained high volume network traffic (for example, large file downloads) that substantially hinders others in their use of the network;
- Engage in any activity not explicitly authorised by the Trust;
- Otherwise, waste time using the Internet for non-Trust business.
- Use web-based email services other than NHS Mail for sending PII or business information. (Web-based mail services such as Gmail, Yahoo etc. may be used for limited personal use)

3.3 Internet Monitoring

The Trust is responsible for the security of the Internet access provided through its computer network. The Trust's computer network and associated information assets will be:-

- available for all authorised users;
- protected from unauthorised or malicious use; and
- protected from unauthorised disclosure.

To help enforce this policy, the Trust has invested in technology to filter and monitor the usage of its Internet connection. The Internet filtering and monitoring system is used to:

- Monitor, analyse, and track all access to the Internet within the Trust;
- Categorise websites based on content;
- Allow or block access to websites by category, keyword, bandwidth, and file type;
- Reduce legal liability associated with Internet misuse;
- Produce logs and reports (for example, to list website names and time spent on them by each user, track attempts to visit blocked sites, track usage trends etc.).

3.3.1 Access to blocked websites

- Contact the Information Service Desk if there is a perceived need to access a website blocked by the Internet monitoring system.
- Access to the specified website may be allowed if it directly relates to Trust business and there are no risks to the security and confidentiality of the Trust's corporate and clinical systems.
- Users must read the terms and conditions of any sites requiring membership.

3.4 Maintenance and Availability

3.4.1 Availability

- Access to the Internet will normally be available 24/7. However, support will be available during normal information service desk operating hours.

- Every effort will be made to maintain the availability and optimal performance of the Trust's connection to the Internet.

3.4.2 Planned maintenance

- Planned maintenance work is sometimes needed on the systems that provide access to the Internet.
- Information department will try to keep service disruption to a minimum.
- When downtime is planned, this information will be communicated via inTouch and e-bulletin.

3.4.3 Emergency maintenance

- Emergency maintenance of the systems that provide access to the Internet may also be required.
- However, due to the nature of the emergency, it may not be possible to provide five working days' notice.

3.4.4 Recovery

- The information department will maintain a log of the system configuration.
- In the event of a failure in the systems that provide access to the Internet, this information will be used to restore service as promptly as possible.

3.4.5 Reconfiguration

- The information department will keep a change control log, which will record all changes made to the configuration of the systems that provide access to the Internet.

4 Definitions

Term	Definition
Internet	A system of computer networks located all over the world that are linked together to allow computers on these networks to communicate and exchange information. The Internet is not the same as the *World Wide Web*.
Pornography	Pornography can take many forms. For example, textual descriptions, still and moving images, cartoons, and sound files. Some pornography is illegal in the UK and some is legal. Pornography considered legal in the UK may be illegal elsewhere. Because of the global nature of the Internet and email, 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 behavior to constitute a serious disciplinary offence.
Smartphone	Similar to a mobile phone but with the added functionality including the ability to connect to the internet.
Web browser	A software application programme that provides a way to look at and interact with all the information on the *World Wide Web*.
Website, web site or site	A set of interconnected web pages, usually including a homepage, and prepared and maintained as a collection of information by a person, group, or organisation.
World wide web, www or the web	A way of exchanging information between computers on the *Internet*, tying them together into a vast collection of interactive multimedia resources. The World Wide Web is not synonymous with the *Internet*.

5 Related documents

Information Security and Risk Policy
Email Policy
Access to Information Systems Policy

6 How this policy will be implemented

Line managers must ensure their staff access and use the Internet in accordance with this policy. Upon request, the Information Service Desk can provide usage reports from the Internet monitoring system to help managers deal with any suspected misuse of the Internet.

⚠ Users who misuse the trust’s Internet access facilities risk having their Internet access privileges removed.

- Users who fail to follow this policy risk disciplinary action and termination of employment.
- The trust acknowledges its obligation to report any illegal activities to the appropriate authorities.

- The trust permits users to access the Internet in accordance with this policy and will not accept any liability whatsoever for any personal loss or expense incurred.
- The trust could be liable for actions performed by users if they misuse the Internet. Internet access logs are valid forms of legal evidence.
- Unless informed otherwise, the trust assumes that all users understand this policy and accept personal responsibility for adhering to its requirements.

7 How this policy will be audited

The information department will conduct checks of the network to ensure compliance with the policy. The trust's audit department will also review this policy and associated procedures annually.

8 References

- Information Security and Risk Policy
- Network Security Policy
- Email Policy and Procedure
- Access to Information Systems Policy
- Telephone Usage Policy
- HSCIC Statement of Compliance

9 Document control

Date of approval:	11 January 2017	
Next review date:	31 December 2024	
This document replaces:	IT-0007-v5 Internet Policy	
Lead:	Name	Title
	Keith I'Anson	Desktop Product Manager
Members of working party:	Name	Title
This document has been agreed and accepted by: (Director)	Name	Title
	Drew Kendall	Director of Finance and Information
This document was approved by:	Name of committee/group	Date
	Information Strategy and Governance Group	December 2016
This document was ratified by:	Name of committee/group	Date
	Executive Management Team	11 January 2017
An equality analysis was completed on this document on:	December 2016	

Change record

Version	Date	Amendment details	Status
1	23 Sep 2009	Review date extended to 31 March 2010	Withdrawn
2	7 Apr 2010	Minor amendments	Withdrawn
	3 Jul 2013	Review date extended to 1 October 2013	
	6 Nov 2013	Review date extended to 31 March 2014 while being rewritten	
3	26 Mar 2014	Sections 2.5 and 4 amended to refer to Smartphones.	Withdrawn
	24 Jul 2015	Use of web mail removed	
4	24 Jul 2014	Sections 2.5 and 4 amended to refer to Smartphones.	Withdrawn
5	13 Jan 2016	Minor updates on streaming for business use	Withdrawn
6	11 Jan 2017	Section 2.1 amended to reflect multiple ways to access the Internet from the Trust network, specifically the Guest Wi-Fi. Also made reference to PATTI access being separate. Some minor grammatically and spelling	Published

		amendments. 3.4, method of communicating down time changed.	
6	10 Jan 2020	Review date extended from 11 Jan 2020 to 30 March 2020	Published
6	2021	Trustwide policy portfolio review extension	Published
6	12 April 2022	Review date extended 16 Sept 2022 to allow completion policy review, consultation and approval processes	Published
6	Oct 2022	Review date extended to 30 April 2023	Published
6	May 2023	Review date extended to 31 October 2023	Published
6	May 2024	Review date extended to 31 Dec 2024	Published