NHS
Ashford and St. Peter's Hospitals
NHS Foundation Trust

Internet Usage and Security Policy

Author: **Head of IT**

Executive Lead: **Simon Marshall Director of Finance and Information**

Status: Approval date: Jan 2019

Ratified by: Information Governance Steering Group

Review date: Jan 2022

Patients first • Personal responsibility • Passion for excellence • Pride in our team

History

Issue	Date Issued	Brief Summary of Change	Author
1	Mar 2002	Various cosmetic changes Reference to Cyber Patrol added. Reference to “Chatrooms, newsgroups and e-mail” changed to “Chatrooms, newsgroups and similar fora, together with e-mail and instant messaging” DiskNet changed to Norton antivirus Definition of Virus added	
2	July 2005	Change to author and changes in anti-virus and internet monitoring software.	
3	March 2007	Glossary of terms updated	
4	June 2008	Updated: Policy Overview Updated: Management of Internet Use Updated: Security Updated: Glossary of Terms	
5	Sept 2010	Amendments to Job Titles and Departments Updated Glossary of Terms Updated Bibliography Addition of sections for monitoring and reviewing, Sections 5-9	
6	June 2012	Amendments to author and job title	Head of IT
7	Dec 2012	Added scope and policy objectives Amended Glossary of Terms	Head of IT
8	Dec 2015	Updated name of who did the EIA Modified to new format	Head of IT
9	Jan 2019	Updated: Author Amended: Sections 3, 4, 6, 14 Amended: Glossary of Terms Updated: Section 13	Head of IT

For more information on the status of this document, please contact:	
Policy Author	Malcolm Flier - Head of IT
Department/Directorate	Health Informatics / Finance
Date of issue	Jan 2012
Review due	Jan 2022
Ratified by	Information Governance Steering Group
Audience	All Staff

Executive summary

This document explains the policy governing the use of the Internet 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.

This policy also supports Trust compliance with NHS security regulations relating to controlled connections to national computer networks. For example, NHS Digital for access to the NHS National Network (currently N3).

Contents

SECTION **Page**

See also: Any relevant trust policies/guidelines or procedures

1. Introduction

- Access to the Internet will be provided automatically to networked Trust devices and is subject to the terms of this policy
- The Trust reserves the right to refuse or remove access
- Employees may use their Internet facilities for non-work research or browsing, outside of work hours, provided that all other usage policies are adhered to
- Internet access must be conducted honestly, lawfully and appropriately
- All existing Trust policies apply to conduct on the Internet
- An Internet user can be held accountable for any breaches of security or confidentiality

2. Scope

This policy is relevant to all staff groups. Use of the Internet is encouraged in the execution of day-to-day business to the extent that it supports the Trust's business objectives. Users must respect the Trust's standards of business conduct whenever the Internet is used.

This policy applies to all authorised users of the Trust's computer network (including all permanent and temporary employees of the trust, agency staff, agents, subcontractors, consultants, and third-party vendors).

A valid user account is required to access the computer network (subject to an individual completing the Trust's prerequisite network training, either at Induction or separately through the IT Training Team based in the Minerva Centre).

Access to the Internet via the Trust's corporate network is only possible using computers issued by the Trust. Personal devices are out of scope but may access the Internet via the Trust's public Wi-Fi network, which is subject to separate controls, as described in the public Wi-Fi Terms & Conditions.

3. Purpose

It is the intention of Ashford and St. Peter's NHS FT to provide access to the resources of the Internet. The facilities to provide such access commit a considerable amount of organisational resource for telecommunications, networking, software, storage, etc. and this policy describes the Trust's expectations for the use of those resources efficiently and effectively in the particular conditions of the Internet.

Access to the Internet will be provided automatically to networked devices. The Trust reserves the right to refuse or remove access subject to the terms of this policy. Employees may use their Internet facilities for non-work research or browsing during meal times or other breaks, or outside of work hours, provided that all other usage policies are adhered to.

In order to restrict access to certain sites, the Trust subscribes to a service which maintains a database of forbidden sites. This is updated regularly and exists to protect staff from visiting sites, which may pose a threat to the organisation.

While explicit requirements for Internet usage are set out below, it is worth summarising the overall intent:

First and foremost, access to the Internet is provided as a business tool to be used primarily for Healthcare business related purposes. Conduct must be honest and appropriate, and respectful of the law (e.g. copyright, software licensing rules, property rights, privacy and prerogatives of others). All existing Trust policies apply to conduct on the Internet, especially (but not exclusively) those that deal with intellectual property rights, privacy, misuse of organisation resources, harassment, information and data security, confidentiality and discipline. Breaches of this policy will be subject to the Trust's Disciplinary Policy.

Unnecessary or unauthorised Internet usage can cause network and server congestion. It can delay other users, take away from work time, consume supplies, and tie up printers and other shared resources. Unlawful Internet usage may also result in negative publicity and reputational damage to the Trust, exposing both it and the individual concerned to significant legal liabilities.

Computer-mediated communication, which can be synchronous (such as instant messaging, online chat, web and video conferencing), asynchronous (e-mail, blogs, wikis, newsgroups) or a mixture of both (social networking sites) is increasing in variety and scope. This offers unprecedented opportunity for the individual user to communicate widely and to promote the Trust. Because of this, special care must be taken to maintain the clarity, consistency and integrity of the Trust's corporate image. Anything that one employee writes or says on the Internet can be taken as representing the Trust as a whole. For this reason, it may be necessary to forgo a measure of individual freedom when participating in such communication for and on behalf of the organisation, as outlined below.

While direct connection to the Internet offers a plethora of potential benefits, it can also open the door to some significant risks to Trust data and systems if appropriate security guidelines are not followed. This may mean preventing systems with sensitive data or applications from connecting to the Internet entirely, or it may mean that certain users must be prevented from using certain Internet features such as file transfers. The overriding principle is that security is to be the first priority. An Internet user can be held accountable for any breaches of security or confidentiality.

4. Explanation of Terms Used

- Organisation or Trust refers to Ashford & St. Peter's Hospitals NHS Foundation Trust.

- The term Document covers any kind of file that can be read on a computer screen as if it were a printed page, including HTML files read in an Internet browser, any file meant to be accessed using an Office application or its viewer, including PDF files.

- Graphics includes photographs, pictures, animations, movies, or drawings.

- Display includes monitors, flat-panel active or passive matrix displays, projectors, televisions and virtual-reality tools, tablet computers, hand held devices (iOS, Android), etc.

5. Duties and responsibilities

5.1 New staff are referred to this policy at Induction. Staff who require training are encouraged to undertake the appropriate training courses available in the Minerva IT Training Centre.

5.2 The Network Manager undertakes regular audits of internet traffic, and in addition, there is a Proxy Server URL filter in place to regulate access to internet and web sites.

6. Policy

6.1 The Trust reserves the right to inspect (or in the case of encrypted confidential data files, verify with the user of) any and all files stored on the network or on local storage, such as hard drives, in order to assure compliance with policy.

6.2 The display of any kind of "offensive" material (including pornographic images or documents) on any Trust system is a disciplinary offence and will be dealt with in accordance with the relevant procedure. In addition, "offensive" material (including pornographic material) may not be archived, stored, distributed, edited or recorded using the Trust's network or computing resources.

6.3 For the purposes of this Policy, "offensive" material is defined as that which would contravene the Trust's relevant policies. Such examples will include hostile or derogatory material (including images) relating to colleagues, gender, ethnicity, race, sex/sexual orientation, religious or political convictions and disability, although these categories are not exhaustive.

6.4 Users who accidentally connect to a site that contains sexually explicit or otherwise "offensive" material must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program. Users must advise the IT Department immediately.

6.5 The Trust's Internet facilities and computing resources must not be used knowingly to violate the laws and regulations of the United Kingdom or any other nation, or the laws and regulations of any country, state, city, province or other local jurisdiction in any material way. Use of the Trust's resources for illegal activity is also deemed a disciplinary offence and will be dealt with under the Trust's disciplinary procedure, and the Trust will co-operate with any legitimate law enforcement activity.

6.6 Any software or files downloaded via the Internet onto the Trust network or local storage become property of the Trust. Any such files or software may be used only in ways that are consistent with their licences or copyrights. Large files, such as .mpg files, “music on demand” or any other “entertainment media” files should not be downloaded. Where there is a legitimate business reason to download such files, a request can be made to the IT Help Desk for assistance.

6.7 Media streaming (e.g. YouTube) is discouraged and may be blocked due to the negative impact it creates on the performance of the network. Should access to streaming media be a work related requirement, a request can be made to the IT Help Desk with approval from the department line manager.
If there is a requirement to upload a video for work related purposes (e.g. training) and shared with colleagues, approval must be obtained from the Media & Communications team.

6.8 You should not use Trust systems to access the Internet, or use your NHS e-mail address, for private business activities to download software, images, video and music for private social media and discussion forums (such as Facebook, Twitter, eBay or other auction sites, etc.).

6.9 No employee may use Trust facilities knowingly to download or distribute pirated software or data.

6.10 No employee may use the Trust's Internet facilities to propagate deliberately any malicious code (e.g. virus, worm, Trojan Horse or trap-door program) that is designed to interfere with the normal running of other users' machines or applications.

6.11 No employee may use the Trust's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

6.12 Each member of staff using the Trust's Internet facilities shall identify himself or herself honestly, accurately and completely (including his/her organisation affiliation and function where requested) when participating in online discussion groups or similar fora, or when setting up accounts on outside computer systems.

6.13 Only those employees who are duly authorised to speak to the media, or to analysts or in public meetings on behalf of the Trust may speak/write in the name of the Trust on online discussion fora. Other employees may participate in such fora in the course of work activities when relevant to their duties, but they do so as individuals speaking only for themselves. Where an individual participant is identified as an employee or agent of the Trust, he/she must refrain from any unauthorised political advocacy or from the unauthorised endorsement or appearance of endorsement by the organisation of any (commercial) product or service not sold or provided by the Trust, its subsidiaries or its affiliates.

6.14 The Trust retains as normal the copyright to any material posted to any online discussion site (or similar computer-mediated communication forum) or World Wide Web page by any employee in the course of his or her duties.

6.15 Employees are reminded that online discussion fora are public areas where it is inappropriate to reveal confidential Trust information of any sort, including patient or employee data, professional secrets, financial data or any other material covered by existing Trust policies and procedures on confidentiality. Employees releasing any such protected information via such fora - whether or not the release is inadvertent - will be subject to the Trust's Information Security Policy, the Trust’s Disciplinary Policy and any other relevant Trust policies and procedures.

6.16 Use of the Trust's Internet access facilities to commit breaches of conduct or offences which contravene Trust policies and procedures will be dealt with in accordance with the relevant procedures.

6.17 Access to the Internet will not be allowed from devices connected to medical equipment – e.g. analysers in the Pathology laboratories.

Technical

6.18 User IDs and passwords help maintain individual accountability for Internet resource usage. Any employee who obtains a password or ID for an Internet resource must keep that password confidential. Trust policy prohibits the sharing of user IDs or passwords obtained for access to Internet sites.

6.19 Any file that is downloaded must be scanned for viruses before it is run or accessed and the Trust has provided Anti-Malware (Antivirus) software to enable this to happen.

Security

6.20 The Trust has installed a variety of network security mechanisms to assure the safety and security of the organisation's network. Any employee who attempts to disable, defeat or circumvent any Trust security system will be subject to the Trust’s disciplinary procedure.

6.21 Files containing sensitive Trust data that are transferred in any way across the Internet must be encrypted. Further guidance on the practical use of encryption tools can be requested from the IT Department. Guidance is also available for the use of email in such circumstances and this is published on the NHSmail portal.

6.22 Computers that have data connections independent of the Trust network circumvent the Trust's network security mechanisms and contravene the Information Governance Statement of Compliance (IGSoC). The IGSoC is the agreement between NHS Digital and the Trust that sets out the information governance policy and terms and conditions for use of NHS Digital (NHSD) services. It contains a number of obligations to enable use of NHSD services, which aim to preserve the integrity of these services.

6.23 A computer with a private connection to another outside computer or network can be used by an attacker to compromise any internal network to which that computer is attached. That is why computers used for independent broadband or leased-line connections to any outside computer or network must be physically isolated from the Trust's network. Further guidance on such requirements can be requested from the IT Department.

7. Training

7.1 No training is required

8. Stakeholder Engagement and Communication

8.1 The policy has been written by the Health Informatics Team and is reviewed and approved by the Information Governance Steering Group. The policy is available to all staff on TrustNet.

8.2 All new staff are referred to this policy at Induction.

9. Approval and Ratification

9.1 Ratification of this policy will be sourced from the Information Governance Steering Group.

10. Dissemination and Implementation

10.1 The policy will be disseminated through the Aspire global email.

10.2 This policy will be published on the Trust intranet and internet sites.

11. Review and Revision Arrangements

11.1 This policy will be reviewed by the author every 3 years, or before if necessary.

12. Document Control and Archiving

12.1 This is a Trust-wide document and archiving arrangements are managed by the Head of Regulation & Accreditation and the Information Content Manager (Quality and Communications Teams) who can be contacted to request master/archived copies.

12.2 On the internet site, the document will be highlighted as green, when in date, amber 3 months prior to review date, and red if expired

.

13. Monitoring compliance with Policies

This document will be monitored regularly to ensure it is effective and to assure compliance

Requirement to be monitored	Leads	Tool	Frequency of monitoring	Reporting Arrangements	Lead(s) for acting on recommendations
This policy will be regularly reviewed and updated	IT Department and Information Governance lead(s)	Report to Information Governance Steering Group	At least every 3 years or more frequently if required	HIS policy audit report to: Information Governance Steering Group	Assigned by Information Governance Steering Group
Access management and web filtering in place in accordance with this policy	IT Department nominated responsible (Network manager)	Report to Information Governance Steering Group	At least every 3 years or more frequently if required	HIS policy audit report to: Information Governance Steering Group	n/a

14. Supporting References / Evidence Base

14.1 NHS Digital Acceptable Use: User guide
14.2 NHS England Social media and attributed digital content policy
14.3 Information Governance Statement of Compliance (IGSoC)
14.4 Data Protection Act 1998 - www.legislation.gov.uk
14.5 Computer Misuse Act 1990 - www.legislation.gov.uk

Glossary of Terms

Browser: (AKA Web Browser, e.g. IE, Chrome, Firefox, Edge, etc.): a software application that facilitates searching and accessing of the World Wide Web

Email: Electronic mail; a means of exchanging messages with other connected users across a network or the Internet.

Extranet: similar to an intranet but used by organisations to provide communications for external groups such as suppliers and customers.

Firewall: a specialised network device that protects an organisation's LAN and/or intranet from unauthorised external access.

HTML: Short for Hypertext Markup Language, is the predominant mark-up language for the creation of web pages. It provides a means to describe the structure of text-based information in a document - by denoting certain text as headings, paragraphs, lists and so on – and to supplement that text with interactive forms, embedded images or objects and links to other documents.

Hypertext: Text which contains links to other text that can be accessed by a mouse click.

Internet: global network for exchanging information held on computers as Web sites and pages. Nobody owns or manages it; it has grown by adopting common standards.

Internet servers: hardware that runs the Internet. These are computers that store Web site information, route calls and handle email and data traffic.

Intranet: a private version of the Internet, used by organisations as the basis of their own networks. They use the same technology as the Internet (servers, Web sites, etc.) but are usually made secure from outsiders by use of firewall techniques.

LAN: Local Area Network, typically used to connect members of a workgroup, department or single-sited organisation.

Malware: Short for Malicious Software, a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. It includes computer viruses, worms, trojan horses, spyware, dishonest adware, ransomware, rootkits, and other malicious and unwanted software.

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 behaviour to constitute a serious disciplinary offence.

Server (AKA File Server or Network Server): a computer connected 'centrally' and accessible from terminals and other computing devices such as PCs.

Virus Any malevolent program intended to harm files on a computer device or to pirate any information available on a PC or network.

Web site: a "place" on the Web made up of a collection of web pages, images or other digital resources.

Web browser: see Browser above.

World Wide Web (www): a system of interlinked hypertext documents accessed via the internet, made up of web sites.

APPENDIX 1: EQUALITY IMPACT ASSESSMENT

Equality Impact Assessment Summary

Name and title: Morné Beck – Head of IT
Policy: Internet Usage and Security Policy

Background • Who was involved in the Equality Impact Assessment
The EIA was performed by the Head of IT
Methodology • A brief account of how the likely effects of the policy was assessed (to include race and ethnic origin, disability, gender, culture, religion or belief, sexual orientation, age) • The data sources and any other information used • The consultation that was carried out (who, why and how?)
The policies were examined and reviewed to ensure that no negative impact on equality would result from the policies.

Key Findings

- Describe the results of the assessment
- Identify if there is adverse or a potentially adverse impact for any equalities groups

There is no impact on equality.

Conclusion

- Provide a summary of the overall conclusions

The policies apply to all staff regardless of race, ethnic origin, gender, culture, religion or belief, sexual orientation and age.

Recommendations

- State recommended changes to the proposed policy as a result of the impact assessment
- Where it has not been possible to amend the policy, provide the detail of any actions that have been identified
- Describe the plans for reviewing the assessment

The policy should be approved.

APPENDIX 2: CHECKLIST FOR THE REVIEW AND APPROVAL OF DOCUMENTS

To be completed (electronically) and attached to any document which guides practice when submitted to the appropriate committee for approval or ratification.

Title of the document:
Policy (document) Author: Malcolm Flier, Head of IT
Executive Director: Simon Marshall, Director of Finance and Information

		Yes/No/ Unsure/ NA	Comments
1.	**Title**		
	Is the title clear and unambiguous?	**Yes**	
	Is it clear whether the document is a guideline, policy, protocol or standard?	**Yes**	
2.	**Scope/Purpose**		
	Is the target population clear and unambiguous?	**Yes**	
	Is the purpose of the document clear?	**Yes**	
	Are the intended outcomes described?	**Yes**	
	Are the statements clear and unambiguous?	**Yes**	
3.	**Development Process**		
	Is there evidence of engagement with stakeholders and users?	**Yes**	
	Who was engaged in a review of the document (list committees/ individuals)?		
	Has the policy template been followed (i.e. is the format correct)?	**Yes**	
4.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	**Yes**	
	Are local/organisational supporting documents referenced?	**Yes**	
5.	**Approval**		
	Does the document identify which committee/group will approve/ratify it?	**Yes**	
	If appropriate, have the joint human resources/staff side committee (or equivalent) approved the document?		
6.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	**Yes**	
	Does the plan include the necessary training/support to ensure compliance?		
7.	**Process for Monitoring Compliance**		

		Yes/No/ Unsure/ NA	Comments
	Are there measurable standards or KPIs to support monitoring compliance of the document?		
8.	**Review Date**		
	Is the review date identified and is this acceptable?	**Yes**	
9.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?	**Yes**	
10.	**Equality Impact Assessment (EIA)**		
	Has a suitable EIA been completed?	Yes	

Committee Approval (insert name of Committee) Information Governance Steering Group			
If the committee is happy to approve this document, please complete the section below, date it and return it to the Policy (document) Owner			
Name of Chair		**Date**	
Ratification by Management Executive (if appropriate)			
If the Management Executive is happy to ratify this document, please complete the date of ratification below and advise the Policy (document) Owner			
Date: n/a			