North East Ambulance Service NHS
NHS Foundation Trust

Internet Policy

Document Control Sheet

Q Pulse Reference Number	POL-F-IMT-9
Version Number	V03
Document Author	Information Governance Manager
Lead Executive Director Sponsor	Director of Finance and Resources
Ratifying Committee	Finance Committee
Date Ratified	19 September 2017
Date Policy Effective From	17 November 2017
Next Review Date	19 September 2020
Keywords	Acceptable, access, account, anti-virus, browser, control, copyright, data, email, encryption, ISP, legal, malware, media, monitoring, network, peer to peer, personal, phishing, prohibited, proxy, reports, server, sites, social, streaming, virus, web, webmail, www.

Unless this copy has been taken directly from the Trust Quality Management site (Q-Pulse) there is no assurance that this is the most up to date version.

This policy supersedes all previous issues.

Version Control - Table of Revisions

All changes to the document must be recorded within the 'Table of Revisions'.

Version number	Document section/ page number	Description of change and reason (e.g. initial review by author/ requested at approval group	Author/ Reviewer	Date revised
0.1	All	No changes post initial review period	IG Manager	Oct 2011
0.2	All	Following comments from IGWG	IG Manager	Nov 2011
0.3	All	Following comments from Policy Review Group: • Formatting changed from 1.5 line spacing to 1. • Trust logo updated. • Section 5.1 – change "have agreed" to "will agree" • 8.1 Definition of "excessive paid work time" • Section 14 – Condense this section and specify what will be reported, to which committee. • Colour coding added to Appendix A table. Added to enable staff to report inappropriate access to content.	IG Manager	Nov 2011
01	All	Following ratification by Governance and Risk Committee. Document owner changed to Director of Finance and Resources.	IG Manager	April 2012
02	All	• Sections re-ordered with new monitoring table. • 3.2 Policy applies to all domain users (Trust staff and 3rd party users e.g. NDUC, Physiotherapists). • 7 Routine monitoring undertaken by Information Security Working Group. • 7.2 Line manager can request ad-hoc usage reports is breach in policy is suspected. Appendix B Social media, streaming media and web based email now allowed.	IG Manager	March 2014
02	All	Reformatted into new Trust template	IG Manager	October 2016
03	Section 6.2	Added: *Whilst the Trust, through software, will attempt to restrict access to inappropriate content, this is not infallible. Therefore all staff also have the responsibility to decide if the content of websites they are viewing is appropriate and/or related to their role.* *Just because you can access a website does not mean you should!*	Assistant Director IM&T	07/08/2017
03	Section 4.4 Section 6.1 Section 6.2 Section 6.3 Section 6.4 Section 6.5 Section 6.6	Addition of IAO. Clarification of what is permissible access. Clarification of inappropriate access. New: Monitoring software. New: Viruses. New: Copyright. New: Internet Service Providers.	IG Manager	26/08/2017

Version number	Document section/ page number	Description of change and reason (e.g. initial review by author/ requested at approval group	Author/ Reviewer	Date revised
	Section 6.7	New: Public representations.		
03	All	Change of 'Internet' to 'internet'. Change of 'Policy' to 'policy' Other minor grammar corrections.	Director of Strategy, Transformation and Workforce	04/09/2017
03	1 2 4	Changes to Introduction. Clarification of purpose. Removal of IGWG and ISWG responsibilities and allocated to IG Manager,	Director of Quality and Safety	04/09/2017
03	 6.2 8	Reference to discrimination law replaced with Equality Act 2010. Expanded to include all characteristics in Equality Act 2010. Updated.	Engagement Manager	11/09/2017
03	6.7	Wording amended and reference to 6.4 removed.	Finance Committee	19/09/2017

This page should not be longer than one single page.

Contents

1. Introduction

Internet access is provided in accordance with the Domain Account Policy which governs access to the Trust's information technology infrastructure. The internet is a valuable business tool and is provided by the Trust to support staff in undertaking their duties.

When used correctly, the internet provides an efficient way of accessing and sharing information. Correspondingly, incorrect or improper use will have the opposite result. Unfortunately the largely uncontrolled nature of the Internet means that users can inadvertently access sites containing offensive, obscene, defamatory, abusive or otherwise unlawful material. In these instances users must exit such sites immediately. Prolonged or regular access to such sites is considered as intentional misuse of the facility. Any serious misuse of the systems may be regarded as a disciplinary offence.

This policy respects and complies with the applicable laws including (but not limited to):

- UK Data Protection Legislation
- EU General Data Protection Regulation 2016
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Copyright Design and Patents Act 1988
- Human Rights Act 1998
- Obscene Publications Act 1959, Protection of Children Act 1999, Criminal Justice Act 1988
- Protection from Harassment Act 1997, Defamation Act 1996, Equality Act 2010
- Regulation of Investigatory Powers Act 2000
- Terrorism Act 2006
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

2. Purpose

This policy governs the acceptable use of the internet. The system must not be used to exchange any information, data, software, which could bring the Trust into disrepute or result in exposure to litigation or prosecution, by regulatory bodies.

The Trust reserves the right to monitor and record all communications and internet activity sent or received via the service's network or computer equipment for violations of this policy.

The Trust reserves the right to filter access to internet sites containing material or services deemed inappropriate.

3. Scope

This policy covers all sites and systems operating and utilised by the Trust.

The policy applies to any individual employed, in any capacity, by the Trust, and any volunteer or contractor who holds a Trust domain account.

4. Duties - Roles & Responsibilities

4.1 Trust Board

The Trust Board is collectively responsible for ensuring that the information risk management processes are providing them with adequate and appropriate information and assurances relating to risks against the Trust's objectives.

4.2 Chief Executive

The Chief Executive is ultimately responsible for the proper use and security of Trust systems. Implementation of, and compliance with the policy is delegated to the Director of Finance and Resources.

4.3 Director of Finance and Resources

The Director of Finance and Resources, who is also the Senior Information Risk Owner (SIRO) is the sponsor of this policy and has overall responsibility for the development and regular review of policies within their areas of responsibility.

The SIRO is also responsible for making sure the trust meets all legislative requirements in relation to information security.

4.4 Information Asset Owner

The Information Asset Owner (IAO) is responsible for Risk Management of the internet and intranet. The Information Asset Owner is the Assistant Director of IM&T.

4.5 Information Governance Manager

Has responsibility for:

- Developing, maintaining and implementing this policy.
- Monitor internet usage and report to managers where breaches in security are identified.

- Investigate requests for sites that are blocked which staff feel should be available.
- Work with line managers and risk management leads in the investigation of potential breaches of this policy.
- Implement secure processes to protect personal information transferred electronically.
- Report any risks related to internet use to the SIRO and IAO.

4.6 Line Managers

Have a responsibility to ensure all current, new and temporary staff/users are instructed in their responsibilities in relation to the use the internet and work in a manner consistent with this policy.

4.7 All users

All users are personally responsible for ensuring that they are aware of and compliant with this policy. By signing up to a Domain Account, users will agree to this policy and its guidelines and should be aware that a breach of this policy may be regarded as serious misconduct which would lead to disciplinary action or dismissal in accordance with disciplinary procedures. Users should also be aware that internet usage will be monitored and any unacceptable usage will be acted upon.

5. Glossary of Terms

This policy uses the following terms:

Term	Description
Access Control	Refers to mechanisms and policies that restrict access to computer resources.
Adult and sexually explicit sites	Including, images, and descriptions of an adult nature that are classed as inappropriate and could cause offence.
Anti-virus	A software program which helps protect a computer against being infected by a virus.
Browser	Provides an easy to use interface for accessing the information on the internet. Internet Explorer and Firefox are versions of browser software.
Encryption	The process of converting information into a form unintelligible to anyone except holders of a specific key or password.
Internet	A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols.

Term	Description
Malware	A form of computer program designed with malicious intent. The intent may be to cause annoying pop-up ads with the hope you click on one and generate revenue, or forms of spyware and viruses that can be used to steal your identity or track your activities.
Network	A group of computers and associated devices that are connected by a communications line or wireless link.
Peer to Peer network	A connection between two or more computers not on the same network allowing files on an individual's hard drive (C drive) to be shared with other individuals in the peer to peer network. These networks can consume large amounts of network capacity and bypass security measures.
Personal data	Information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[1]
Phishing	An attempt to fraudulently acquire sensitive financial or personal information, such as credit card information or National Insurance number, by impersonating a business representative or trustworthy person. Phishing attempts are usually initiated through the internet using a fake website purporting to be the real site such as a bank, email, phone calls, or Instant Messaging.
Proxy Server/Setting	A software agent that performs a function or operation on behalf of another application or system while hiding the details involved.
Social Media	Websites and applications that enable users to create and share content or to participate in social networking.
Streaming Media	Any kind of internet content that is continuously transmitted such as radio broadcasts, video e.g. YouTube, Google Video, internet radio.

6. Policy Content

6.1 Permissible access

For ease of reference the term internet will be used for all forms of web based access

[1] EU General Data Protection Regulation 2016

i.e. intranet, extranets and NHS and World Wide Web pages.

The internet is an important source of information in supporting us in the provision of high quality health and social care. Access to the internet is primarily for healthcare related purposes. That is for NHS work or for professional development and training. Reasonable personal use is permitted provided this does not interfere with the performance of your duties. Personal access to the internet can be limited or denied by your manager. Staff must act in accordance with their manager's local guidelines. The Trust has the final decision on deciding what constitutes excessive use.

The use of the internet for personal transactions only, such as booking reservations or tickets or the purchase of any goods or services for personal use, is permitted. Employees should regard this facility as a privilege that should not be abused and should normally be exercised in their own time and without detriment to the job. Inappropriate or excessive use may result in disciplinary action and/or removal of facilities. Staff should be aware that internet access will be subject to monitoring.

6.2 Inappropriate use

Certain use of the internet is prohibited and includes the following:

- Accessing and/or downloading or publishing any offensive or inappropriate content relating to gender identity, marriage, civil partnership, maternity/paternity, age, sex, race, religion or belief, disability, sexual orientation, political convictions, pornographic, violent, criminal, gambling, defamatory, or other offensive or illegal content or images.
- Intentional downloading of viruses or related security threats.
- Downloading, sending or copying any copyright material without licence or permission of the copyright owner.
- Any attempt to access the internet anonymously e.g. remote proxies.

The above list is not exhaustive and is considered a serious breach of policy which will be managed in line with Trust Disciplinary Policy and/or criminal proceedings. Suspected attempts to access certain categories of site, specifically those which display any material likely to be illegal such as child abuse or obscene images which seek to deprave will result in immediate notification to the Police for investigation.

The Trust notes that access to subjects and sites of a potentially contentious nature may be appropriate in some areas of normal operation and/or in specific circumstances, e.g. education, advice, counselling on gambling, approved research, etc. The Trust therefore places special responsibilities of care on staff operating in such areas to ensure that such access is necessary and that other users, staff and members of the community are not exposed to any such material without good cause.

Staff should not use the internet to conduct personal transactions in pursuit of their own commercial or business interests nor in such a way as to implicate the Trust in those transactions.

Whilst the Trust, through software, will attempt to restrict access to inappropriate content, this is not infallible. Therefore all staff also have the responsibility to decide if the content of websites they are viewing is appropriate and/or related to their role.

Just because you can access a website does not mean you should!

Employees should operate the 'back' button immediately should they inadvertently access unsuitable material and report this immediately to the IM&T Service desk (this may be done online if out of hours). Purposeful access or downloading of such material shall be deemed an act of gross misconduct.

6.3 Monitoring software

To support the Trust in meeting its legal obligations, the Trust has implemented monitoring software which prevents users visiting websites that may be unsuitable. Further information on the monitoring software is provided in the monitoring section of this policy.

There may be circumstances where staff, for the purpose of their work, need access to sites which may be blocked. If that is the case, staff should complete and submit their request within the application. Sites will not be unblocked for personal use.

If staff find that they can access a site which they feel should be blocked, they can report this via the IM&T Service Desk.

6.4 Viruses

Viruses can damage computer systems, destroy data, cause disruption and incur considerable expense for the Trust. The IM&T Department will ensure that Trust equipment connecting to the domain has appropriate virus scanning software installed that this is regularly updated. Users must not independently load software onto Trust devices and any software installations must be arranged with the IM&T Department.

6.5 Copyright

Files must not be downloaded from the internet and used in such a way as to violate copyright laws. Even if downloading is permissible under copyright law, there may be restrictions with regard to copying, forwarding, or otherwise distributing files. Staff should be aware that copyright law includes music. Therefore music tracks such as MP3's videos must not be downloaded or streamed. Software license agreements should be read and adhered to. Staff must not transmit copyright software from their computer via the internet.

Only authorised members of staff have the ability to publish content on Trust intranet/internet page. Training is provided to these staff to ensure that they are aware of what should and should not be published and all documents are governed by the Freedom of Information Act and as such may have to be disclosed when a request for such information is received.

6.6 Internet Service Providers

Internet access must be via the Trust's network provided equipment in all instances. the use of modems is strictly prohibited on the Trust domain. The internet provides the ability to transmit messages and documents globally. E-mail being transmitted across the internet is completely insecure without encryption. No person identifiable / confidential information must be sent over the internet without the use of an approved encryption certificate.

Many employees of the Trust will have private external e-mail accounts (webmail) that are provided by Internet Service Providers (ISP's), which may be accessible via the Web, e.g. Hotmail accounts etc. These accounts must under no circumstances be used to transfer confidential organisational information or for the transfer of confidential person identifiable information. No e-mails containing such information are to be sent to or from these accounts. No confidential person identifiable information should be stored on the internet via cloud file storage.

6.7 Public representations

Staff may indicate their affiliation with the Trust in work related bulletin board discussions, chat sessions and other offerings on the internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an e-mail address.

In either case, whenever staff provide an affiliation they must also clearly indicate that the opinions expressed are their own, and not those of the Trust.

All external representations on behalf of the Trust must first be cleared with the Chief Executive. Additionally, to avoid libel problems, any affiliation with the Trust included with an internet message, defamatory posting, or similar written attacks are strictly prohibited.

Staff must not publicly disclose internal Trust information via the internet that may adversely affect the Trust's public image. Care must be taken to properly structure comments and questions posted to public news groups and related public postings on the internet.

7. Training Required for Compliance with this Policy

All staff to receive mandatory Information Governance training on an annual basis.

8. Equality and Diversity

The Trust is committed to providing equality of opportunity. We aim to give people the freedom to flourish and develop in an environment free from discrimination, harassment, bullying and prejudice where their contributions, skills and knowledge are recognised and embraced.

We want to ensure that we provide services and employment opportunities that consider and are tailored to peoples' specific needs. Further details or our aims and objectives are outlined in our Equality Strategy – One Service for All.

We use the NHS England's Equality Delivery System 2 as our framework to monitor and improve our performance on equality and inclusion. We have also made a commitment to the Job Centre Two Ticks about Disability scheme, the Stonewall Work Place Equality Index meet our mandated requirements in relation to the Workforce Race Equality Standard and support a range of other initiatives.

This policy has been assessed to identify any potential for adverse or positive impact on specific groups of people protected by the Equality Act 2010 and does not discriminate either directly or indirectly.

The Trust values and respects the diversity of its employees and the communities it serves. In applying this policy we have considered eliminating unlawful discrimination, promoting equality of opportunity and, promoting good relations between people from diverse groups. Any issues highlighted in the assessment have been considered and incorporated into the policy and approved by the Head of Service/Director and relevant committee.

9. Monitoring Compliance with and Effectiveness of this Policy

9.1 Compliance and Effectiveness Monitoring

Arrangements for the monitoring of compliance with this policy and of the effectiveness of the policy are detailed below.

Monitoring Criterion	Response
Who will perform the monitoring?	Information Governance Manager
What are you monitoring?	• Names and numbers of staff attempting to access inappropriate web content (adult /sexually explicit sites; hacking sites; to obtain peer to peer software and proxy). • Names and numbers of staff trying to access the internet anonymously e.g. through attempting to bypass existing security settings and remote proxies. **Ad hoc reporting** • In addition to regular reports, specific issues on Internet usage may be highlighted by other means for example, a user's line manager or investigating officer. Requests should be made through the IM&T Service Desk. In such a case, no information would be provided to the line manager, unless a clear breach of policy had been identified and then in line with the investigation process.

	• The line manager will be informed if the reports indicate that no specific issue is highlighted by the monitoring system. • It may be advised that the individual is informed if any further monitoring of usage is to take place as per the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
When will the monitoring be performed?	Bi-monthly
How are you going to monitor?	Sophos Internet Monitoring tool
What will happen if any shortfalls are identified?	Where unusual activity is detected the Information Governance Team will notify relevant line managers to investigate further. These reports are specifically aimed at identifying users who may be repeatedly trying to access blocked sites or inappropriate content. Line managers will feedback to the Information Governance Team the outcome of any investigations and these will be summarised and reported to the Information Security Working Group.
Where will the results of the monitoring be reported?	Anonymised reports to the Information Governance Working Group.
How will the resulting action plan be progressed and monitored?	The action plan will be progressed by the Information Security Working Group and monitored by the Information Governance Working Group.
How will learning take place	Learning will be via the action plans and monitored by Information Governance Working Group.

9.2 Compliance and Effectiveness Monitoring Table for this policy

Process in the policy	Monitoring and audit					
	Key Performance Indicators (KPI)/ Criteria	**Method**	**Who By**	**Committee**	**Frequency**	**Learning/ Action Plan**
Compliance with Trust policy template, format and ratification process	• Style, format and template • Explanation of terms used • Consultation process • Ratification process • Review arrangements • Control, including archiving arrangements • Associated documents • Supporting references • Monitoring section in policy	Assessing all new and reviewed policies against the guidance through presentation to relevant approval groups	Author and approval groups	Finance Committee	Ongoing	To be developed as necessary
Monitoring and reporting on policy compliance	Number of incidents involving internet use	Via Sophos Internet Monitoring Tool and Alerts	IG Manager	ISWG and IGWG	Bi-monthly	Monitor via Action Plans

10. Consultation and Review of this Policy

This policy has been reviewed in consultation with:

- Information Security Working Group
- Information Governance Working Group

The policy will be reviewed every three years unless there are significant revisions to be made.

11. Implementation of this Policy

This policy is to be implemented Trust wide through staff briefings, newsletters, team brief, divisional meetings.

12. References

This document refers to the following guidance, including national and international standards:

- Data Protection Act 1998 http://www.legislation.gov.uk/ukpga/1998/29/contents
- EU General Data Protection Regulation 2016 http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
- Freedom of Information Act 2000 http://www.legislation.gov.uk/ukpga/2000/36/contents
- Computer Misuse Act 1990 http://www.legislation.gov.uk/ukpga/1990/18/contents
- Copyright Design and Patents Act 1988 http://www.legislation.gov.uk/ukpga/1988/48/contents
- Human Rights Act 1998 http://www.legislation.gov.uk/ukpga/1998/42/contents
- Obscene Publications Act 1959 http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents
- Protection of Children Act 1999 http://www.legislation.gov.uk/ukpga/1999/14/contents
- Criminal Justice Act 1988 http://www.legislation.gov.uk/ukpga/1988/33/contents
- Protection from Harassment Act 1997 http://www.legislation.gov.uk/ukpga/1997/40/contents
- Defamation Act 1996 http://www.legislation.gov.uk/ukpga/1996/31/contents
- Equality Act 2010 http://www.legislation.gov.uk/ukpga/2010/15/contents
- Regulation of Investigatory Powers Act 2000 http://www.legislation.gov.uk/ukpga/2000/23/contents
- Terrorism Act 2006 http://www.legislation.gov.uk/ukpga/2006/11/contents

- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
  http://www.legislation.gov.uk/uksi/2000/2699/contents/made

13. Associated Documentation

This policy refers to the following Trust documents:

Domain Account Policy POL- F- IMT- 5
Disciplinary Policy POL-WOD-HR-7

14. Appendices

14.1 Appendix A: Allow / block site list by category

Allow	Block
Arts	Adult/Sexually Explicit
Blogs & Forums	Alcohol & Tobacco
Business Advertisements & Pop-Ups	Chat
Computing & Internet	Criminal Activity
Custom	Downloads
Education	Gambling
Entertainment	Games
Fashion & Beauty	Hacking
Finance & Investment	Hosting Sites
Food & Dining	Illegal Drugs
Government	Intimate Apparel & Swimwear
Health & Medicine	Intolerance & Hate
Hobbies & Recreation	Peer-to-Peer
Infrastructure	Phishing & Fraud
Job Search & Career Development	Photo Searches
Kid's Sites	Proxies & Translators
Motor Vehicles	Real Estate
News	Spam URLs
Personals and Dating	Spyware
Philanthropic & Professional Orgs.	Tasteless & Offensive
Politics	Ringtones/Mobile Phone Downloads
Reference	Violence
Religion	Weapons
Search Engines	
Sex Education	
Shopping	
Society & Culture	
Sports	
Streaming Media	
Travel	
Uncategorised	
Web-based email	

14.2 Appendix B: Risk assessment of access to streaming media/social media/web based email

Risks of streaming media use

- Excessive use may lead to lost productivity (Statistics could be deceptive because apparent usage can be pushed up by web pages that auto refresh every few minutes, and users may be doing their daily work while running a browser in the background).
- In competition for bandwidth for legitimate business use.
- Risk malware entering the domain.
- Users could be scammed into clicking on a link in an email to an interesting video, and then told to download a plugin or update the video player software, which is actually malware.

Risks of social media use

- Excessive use may lead to lost productivity.
- Particularly disruptive because it requires the users' immediate and ongoing attention.
- Information leakage.
- Piracy and Infringement.
- A medium for personal attacks such as blackmailing, extortion, cyber bullying & cyber stalking.
- Applications – whether provide the exposure of information leakage, and may also provide an attack vector for introducing malware.

Web based email

- Personal email downloaded by direct connection to ISPs and web-based mail systems (e.g. Hotmail) may also bypass attachment and content monitoring systems that are in place on official internet connections. This is another route by which Trojans and viruses can enter the domain even when it virus checks its official email.
- Unauthorised exposure to confidential or sensitive information (could allow webmail access but blocked from attaching files).

Mitigation

- Ultimately the effective supervision of staff, to prevent excessive internet use, is a local management responsibility.
- Widespread blocking will also penalise responsible internet users who wish to visit a non-work-related site in their own time.

It can be difficult for line management to track the extent to which their staff are using the internet. It maybe that weekly reports are generated listing the total internet use for each employee, without giving details of what they are looking at. The return on investment of developing such a reporting system is high, given the infrastructure capacity and productivity recovered by deterring excessive personal use.