The Newcastle Upon Tyne Hospitals NHS Trust

Internet Security Policy

Version No.:	5.0
Effective From:	23 January 2019
Expiry Date:	23 January 2022
Date Ratified:	26 February 2019
Ratified By:	Clinical Policy Group

1. Introduction

1.1 The Trust acknowledges the importance of making the Internet available for use by employees and other relevant (authorised) individuals for purposes connected to Trust business.

1.2 It also recognises that the resources, services and interconnectivity available via the Internet require appropriate arrangements to be in place concerning Internet security. This policy sets out what these arrangements are.

2. Scope

2.1 This policy applies to all individuals who use the Internet with Trust computing or networking resources, as well as individuals who present themselves as being connected - in one way or another - with the Trust.

2.2 This includes employees, agency staff, students, Observer and Clinical Access placements, Work Experience placements, University staff, contractors users affiliated with third parties who access Trust computer networks.

2.3 Throughout this policy, the word "user" will be used to collectively refer to all such individuals. The policy applies to all computer and data communication systems owned by and/or administered by the Trust.

3. Specific policy

3.1 All information travelling over Trust computer networks that has not been specifically identified as the property of other parties will be treated as though it is a Trust corporate asset.

3.2 It is Trust policy to prohibit unauthorised access, disclosure, duplication, modification, diversion, destruction, loss, misuse or theft of this

information.

3.3 In addition, it is Trust policy to protect information belonging to third parties that has been entrusted to the Trust in confidence as well as in accordance with applicable contracts and industry standards.

4. Information movement

4.1 All software downloaded from non-Trust sources via the Internet must be screened with virus detection software prior to being opened or run.

4.2 All information taken off the Internet should be considered suspect and where possible be confirmed by separate information from another source. There is no quality control process on the Internet and a considerable amount of its information is outdated or inaccurate.

4.3 Contacts made over the Internet should not be trusted with Trust information unless a due diligence process has been performed beforehand. This due diligence process applies to the release of any internal Trust information (see the following section).

4.4 Users must not place Trust material (software, internal memos, etc.) on any publicly accessible Internet site, unless previously approved.

4.5 In more general terms, Trust internal information should not be placed in any location, on machines connected to Trust internal networks, or on the Internet unless the person(s) who have access to that location have a legitimate need to know.

4.6 Internet access will be monitored for any exchange of information inconsistent with the Trust's business. Examples include: pirated software; and inappropriate written or graphic material. Users are prohibited from being involved in any way with the receipt, viewing, production, storage or sending of any such information and material.

4.7 Exchanges of software and/or data between the Trust and any third party may not proceed unless a prior written agreement has been signed. Such an agreement must specify the terms of the exchange as well as the ways in which the software and/or data is to be handled and protected.

4.8 The Trust requires strict adherence to software vendors' license agreements. When at work, or when Trust computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Furthermore, off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with Trust work and are therefore prohibited. Similarly, reproduction of words posted or otherwise available over the Internet must be done only with the permission of the author/owner.

4.9 Staff using Trust information systems and/or the Internet should be aware that their communications are not automatically protected from viewing by third parties. There is no automatic encryption of data on the Internet, staff

should not send information over the Internet in connection with Trust business if they consider it to be private and/or confidential.

4.10 At any time and without prior notice, the Trust reserves the right to examine e-mail, personal file directories and any other information stored on Trust computers. This is to:

- ensure compliance by the user(s) with relevant Trust policy and procedure
- enable appropriate investigations to be conducted where there are grounds to suspect a breach of policy and/or procedure has occurred
- assist with the management of Trust information systems (see Trust E-mail Policy for further information).

5. Resource usage

5.1 The Trust encourages staff to explore the Internet, but if this exploration is for personal purposes it should be done in personal time, not during working time. Likewise, games, news groups and other non-business activities must be performed in personal time, not during working time. See Appendix A for site categories designated as inappropriate.

5.2 Use of Trust computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as it does not adversely affect business activity. Work related access to the Internet must always take priority.

5.3 Internet access from Trust computers is monitored and logged in real time. The Trust reserves the right to use this logged information in any investigation of suspected Internet abuse.

6. Public representations

6.1 Staff may indicate their affiliation with the Trust in work related online discussion boards, 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.

6.2 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.

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

6.4 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. **Reporting security problems**

7.1 If sensitive Trust information is lost, disclosed to unauthorised parties, or suspected of being lost or disclosed to unauthorised parties, the Information Governance office, or the Human Resources Department must be notified immediately.

7.2 If any unauthorised use of Trust information systems has taken place, or is suspected of taking place, the Information Governance office must be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen or disclosed the IT Service Desk Ext 21000 must be notified immediately.

7.3 Because it may indicate a computer virus infection or similar security problem, all unusual systems behaviour, such as missing files, frequent system crashes, misrouted messages and the like must also be reported immediately to the IT Service Desk Ext 21000. The specifics of security problems should not be discussed widely, but should be shared on a need-to-know basis.

7.4 Users must not attempt to "hack" (probe) security mechanisms at either the Trust, or other Internet sites.

8. **Responsibilities**

8.1 IT Department

The IT Department is responsible for:

a) establishing Internet security policies and standards
b) providing technical guidance on computer security
c) ensuring there is an appropriate policy and procedure in place to respond to virus infestations, hacker intrusions and similar events
d) monitoring compliance with Internet security requirements, including hardware, software and data safeguards
e) providing administrative support and technical guidance on matters related to Internet security
f) periodically conducting risk assessments on information systems to determine both risks and vulnerabilities
g) checking that appropriate security measures are implemented on systems in a manner consistent with the level of information sensitivity
h) checking user access controls are defined in a manner consistent with the need-to-know

8.2 Managers

Managers are responsible for:

a) ensuring staff are aware of this policy and that they understand they must comply with it all times

b) ensuring that the sensitivity of data on systems is defined and designated in a manner consistent with in-house sensitivity classifications
c) ensuring the implementation of security measures as defined in this document
d) ensuring that sensitive (confidential) data is deleted from disk files when the data is no longer needed or useful

8.3 Users

Individual users of Trust Internet connections are responsible for:

a) ensuring that they comply with this policy and other Trust policies and practices pertaining to Internet security at all times
b) not permitting any unauthorised individual to obtain access to Trust Internet connections
c) not using or permitting the use of any unauthorised device in connection with Trust computers
d) maintaining exclusive control over and use of their password, and protecting it from inadvertent disclosure to others
e) selecting a unique password that bears no obvious relation to themselves, their organisational group, or their work project and is not easy to guess
f) ensuring that data under their control and/or direction is properly safeguarded according to its level of sensitivity
g) reporting to the IT security office any incident that appears to compromise the security of Trust information resources. These include missing data, virus infestations and unexplained transactions
h) accessing only the data and automated functions for which they are authorised in the course of normal business activity
i) obtaining supervisor authorisation for any uploading or downloading of information to, or from Trust multi-user information systems if this activity is outside the scope of normal business activities

NB All users are required to sign an Acceptable Use Declaration.

9. **Contact point**

Any queries regarding this policy should be directed to the IT security office via the IT Department, RVI or IT Service Desk Ext 21000.

10. **Other Relevant Policies**

Users of Trust IT Systems and Intranet/Internet should also refer to the following policies:

• Network Security & Access Control Policy

- Email and Electronic Communications Policy
- Information Security Policy
- Social Media Policy

11. **Disciplinary Action**

11.1 An employee found in breach of this policy will be subject to disciplinary action that can include their dismissal.

11.2 Where any other user is found in breach, the Trust will take appropriate action to safeguard its interests and will notify the matter to the relevant third party pertaining to the individual(s) e.g. employer, school, college or educational establishment.

12. **Audit & Monitoring**

Standard / process / issue	*Monitoring and audit*			
	Method	*By*	*Committee*	*Frequency*
Sophos Web filter monitor	Internet audit logs reviewed. Any exceptional matters arisien from the reporting will be raised with IG committee.	IT Security	Information Governance committee	Periodic reporting by exception

13. **Review**

The Human Resources Manager, in conjunction with the Head of IM&T, is responsible for the review and amendment of this policy.

Appendix A

The following internationally recognised, categories of Internet sites have been designated inappropriate and are subject to automated blocking by the Trust.

- Adult and sexually explicit
- Criminal Activity
- Violence / Extreme
- Weapons
- Gambling
- Drugs, Alcohol & Tobacco
- Hacking, Spyware, Malware and Phishing
- Web-based email
- Social Networking
- Payday Loans
- Personal & Dating.
- Personal network storage
- Peer to Peer and Torrents
- Pro suicide and self-harm
- Online games / gaming
- File sharing
- Piracy / illegal downloads
- Terrorism
- Web Proxies / Anonymisers

The Trust reserves the right to add other individual sites and categories for automated blocking.

The Newcastle upon Tyne Hospitals NHS Foundation Trust

Equality Analysis Form A

This form must be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

PART 1

1. **Assessment Date:** _14/01/19_____

2. **Name of policy / guidance/ strategy / service development / Investment plan/Board Paper**:

Internet Security Policy

3. **Name and designation of author:**

Matt Carney – Head of Information Governance

4. **Names & Designations of those involved in the impact analysis screening process:**

Matt Carney - Head of Information Governance, Julia Scott - Governance & Security Officer

5. **Is this a:** Policy x Strategy □ Service □ Board Paper □

   Is this: New Revised x

   Who is affected: Employees x Service Users Wider Community

6. **What are the main aims, objectives of the document you are reviewing and what are the intended outcomes?**
(These can be cut and pasted from your policy)

The policy promotes the Trust stance on the use of Internet as a tool for work and personal use.

7. Does this policy, strategy, or service have any equality implications? Yes □ No X

If No, state reasons and the information used to make this decision, please refer to paragraph 2.3 of the Equality Analysis Guidance before providing reasons:

The Policy has no equality issues as it outlines the processes and procedures. This policy is a reminder of the staff obligations for correct use of Internet.

8. Summary of evidence related to protected characteristics

Protected Characteristic	**Evidence** **What evidence do you have that the Trust is meeting the needs of people in all protected Groups related to the document you are reviewing–** please refer to the Equality Evidence within the resources section at the link below: http://nuth-vintranet1:8080/cms/SupportServices/EqualityDiversityHumanRights.aspx	**Does evidence/engagement highlight areas of direct or indirect discrimination?** For example differences in access or outcomes for people with protected characteristics	**Are there any opportunities to advance equality of opportunity or foster good relations**? If yes what steps will be taken? (by whom, completion date and review date)
Race / Ethnic origin (including gypsies and travellers)	**This policy relates to the legal requirements for managing personal data.**		
Sex (male/ female)	**This policy relates to the legal requirements for managing personal data regardless of sex**		
Religion and Belief	**This policy relates to the legal requirements for managing personal data regardless of religion.**		
Sexual orientation including lesbian, gay and bisexual people	**This policy relates to the legal requirements for managing personal data regardless of sexual orientation.**		
Age	**This policy relates to the legal requirements for managing personal data regardless of age.**		
Disability –	**This policy relates to the legal requirements**		

learning difficulties, physical disability, sensory impairment and mental health. Consider the needs of carers in this section	**for managing personal data regardless of and difficulties or disabilities.**		
Gender Re-assignment	**This policy relates to the legal requirements for managing personal data and has no impact on any Gender re-assignment.**		
Marriage and Civil Partnership	**This policy relates to the legal requirements for managing personal data and has no impact on marriage or Civil partnerships.**		
Maternity / Pregnancy	**This policy relates to the legal requirements for managing personal data.**		

9. Are there any gaps in the evidence outlined above? If 'yes' how will these be rectified?

Section 8 is not applicable to this policy.. see response in 7

10. Engagement has taken place with people who have protected characteristics and will continue through the Equality Delivery System and the Equality Diversity and Human Rights Group. Please note you may require further engagement in respect of any significant changes to policies, new developments and or changes to service delivery. In such circumstances please contact the Equality and Diversity Lead or the Involvement and Equalities Officer.

Do you require further engagement No

11. Could the policy, strategy or service have a negative impact on human rights? (E.g. the right to respect for private and family life, the right to a fair hearing and the right to education?)

No

PART 2

Name of author:

Matt Carney

Date of completion

14/01/19

(If any reader of this procedural document identifies a potential discriminatory impact that has not been identified, please refer to the Policy Author identified above, together with any suggestions for action required to avoid/reduce the impact.)