

The Newcastle Upon Tyne Hospitals NHS Trust

Personnel Policies & Procedures

Internet Security Policy

Effective from: December 2010

Review Date: December 2013

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 There is no quality control process on the Internet and a considerable amount of its information is outdated or inaccurate.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 Access to permissible non-work-related Internet sites is subject to a user quota of up to one hour per working day. Individual exceptions may apply. Requests for exemptions must be made to the IT Security team via the IT Service Desk Ext 21000.

5.4 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 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.

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.

6.5 Social Networking. (e.g. blogs, wikis, Facebook) and media sharing (e.g YouTube)
Whilst the Trust recognises the individual's right to a private life, during any use of social networking sites or maintenance of personal blogs, employees are required to refrain from making any reference to the Trust that could bring it into disrepute, or interacting or writing on sites in a way that could constitute harassment of a third party. Any information posted on social networking sites which may bring the Trust into disrepute, breach confidentiality or damage working relationships between colleagues will be treated as a disciplinary offence.

Internet libel is the publication of a defamatory statement in permanent form, which includes publication on the internet. The Trust will undertake swift action if it becomes aware of statements posted on websites which may be considered defamatory.

Any form of harassment, including defamatory statements or other unacceptable content will be given serious consideration by the Trust and appropriate action will be taken.

If an employee becomes aware of a statement on a website which could be considered defamatory they should contact IT Services Desk with the following information:

- Their name and contact details
- The location of the statement
- The nature of the complaint – ie why they object to the statement.

The Trust reserves the right to secure the removal of any such statement, and will carry out an investigation into how such a statement was posted.

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 IT security 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 IT security 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

IT Department

- 8.1 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

Managers

- 8.2 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

Users

8.3 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 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:

- [Access Control Policy](#)
- [Trust E-mail Policy](#)
- [Information Security 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. 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 Skills
- Violence
- Weapons
- Gambling
- Drugs, Alcohol & Tobacco
- Hacking, Malware and Phishing
- Web-based email
- Chat rooms, instant messaging and related activities
- Social Networking
- Personal & Dating.
- Online games / gaming
- File sharing
- Piracy / illegal downloads
- Terrorism
- Web Proxies

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

THE NEWCASTLE UPON TYNE HOSPITALS NHS FOUNDATION TRUST
IMPACT ASSESSMENT – SCREENING FORM A

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

Policy Title:	Internet Policy	Policy Author:	Richard Oliver
		Yes/No?	You must provide evidence to support your response:
1.	Does the policy/guidance affect one group less or more favourably than another on the basis of:	No	Minor changes to existing policy. Policy is effective Trustwide.
	• Race		
	• Ethnic origins (including gypsies and travellers)		
	• Nationality		
	• Gender		
	• Culture		
	• Religion or belief		
	• Sexual orientation including lesbian, gay and bisexual people		
	• Age		
	• Disability – learning difficulties, physical disability, sensory impairment and mental health problems.		
2.	Is there any evidence that some groups are affected differently?	No	
3.	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?		
4(a).	Is the impact of the policy/guidance likely to be negative? <i>(If “yes”, please answer sections 4(b) to 4(d)).</i>		
4(b).	If so can the impact be avoided?		
4(c).	What alternatives are there to achieving the policy/guidance without the impact?		
4(d)	Can we reduce the impact by taking different action?		

Comments:	Action Plan due (or Not Applicable):

Name and Designation of Person responsible for completion of this form: Richard Oliver Head of Information Security & governance..... Date: 30/12/10.....

Names & Designations of those involved in the impact assessment screening process:..... ISSB (Trust Information standards board) Andy Jardine Director of IT.....

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

For advice on answering the above questions please contact Helen Lamont, Director of Nursing, or, Christine Holland, Senior HR Manager. On completion this form must be forwarded electronically to Steven Stoker, Clinical Effectiveness Manager, (Ext. 24963) steven.stoker@nuth.nhs.uk together with the procedural document. If you have identified a potential discriminatory impact of this procedural document, please ensure that you arrange for a full consultation, with relevant stakeholders, to complete a Full Impact Assessment (Form B) and to develop an Action Plan to avoid/reduce this impact; both Form B and the Action Plan should also be sent electronically to Steven Stoker within six weeks of the completion of this form.