

The Newcastle Upon Tyne Hospitals NHS Foundation Trust
Laptop and Portable Computing and Data Storage Policy

Effective: March 2010

Review: March 2013

1 Introduction

- 1.1 This policy combines and replaces the Trust Laptop Policy and Offsite & Data Transfer.
- 1.2 The effective and efficient use of computerised data processing is a vital part of the operation of the Trust. This policy sets out to clarify how computer facilities should be operated to ensure data is secure and to identify prohibited actions which could put the security of data in jeopardy or adversely affect the integrity of the Trust or which would be in breach of national legislation.

2 Scope

- 2.1 Authorised Trust staff will be given access to portable computer systems and equipment to facilitate the execution of their duties. This policy defines the terms and conditions under which systems and equipment must be used and gives notice of improper or prohibited uses of portable computer systems and data.
- 2.2 For the purposes of this document portable computers are defined as Laptop and Notebook computers, and digital storage devices such as PDAs (Personal Digital Assistants), Palmtops, USB memory sticks Writable CDs and Advanced Mobile Phones.
- 2.3 Only authorised staff shall have access to portable computers and systems provided by the Trust. This policy applies to all Trust staff and contractors.
- 2.5 All Trust staff must abide by the conditions of this policy.

3 Specific policy

- 3.1 Authorised Trust staff will be given access to portable computer systems and equipment (e.g. Laptop and Notebook computers, PDAs, Palmtops, Advanced Mobile Phones) if required to facilitate the execution of their duties.
- 3.2 Only legally acquired software and licensed programs must be used and staff may not install any software products without authorisation. All

software and data files are the property of the Trust and the approved Anti-Virus software package must be installed and updated regularly.

- 3.3 Portable data storage media shall not be used to carry personal identifiable information outside Trust premises without authorisation and must be password protected and encrypted. Disposal of any portable media should comply with the Trust disposal procedure.
- 3.4 The security of portable computing devices is the individual's responsibility at all times and must be locked securely away when unattended in any public place. When using a vehicle, staff must lock equipment in the luggage compartment and remove it if the vehicle is to be left unattended.
- 3.5 Back-ups must be made to the Trust network on a regular basis. Incidents that constitute a loss of hardware or data should be reported through the Trust Incident Reporting Procedure and to the IT Helpdesk.
- 3.6 The Trust will maintain a register of devices and will use software to manage the type of data transferred between Trust systems and portable devices.
- 3.7 Software and programs used on any Trust system or computer shall be legally acquired and in the case of licensed software, each copy shall be licensed and the Trust will adhere to the relevant licensing agreement.
- 3.8 Staff may not install any software products onto Trust computers nor connect any device to Trust computers or networks without authorisation from the IT Helpdesk
- 3.9 Software and data files created by staff on Trust equipment are the property of the Trust.

4 Authorised Usage

- 4.1 Staff will be issued with system access passwords. In line with the Trust [Access Control Policy](#).
- 4.2 Portable data storage media such as CDs, diskettes or tapes shall not be used to carry personal identifiable information outside Trust premises without authorisation from the Caldicott Guardian and data files so authorised must be encrypted.
- 4.3 The Trust uses Pointsec protector as the standard device encryption tool for portable data media. Portable data storage media; USB memory sticks, pda's, advanced mobile phones, digital music players that are connected to the Trust network will be registered on initial connection.
- 4.4 After registration the software will monitor any data transferred between the Trust network and the device.

- 4.5 Data held on a personal device will be accessible without encryption however if any data is subsequently copied from the Trust network into that device then enforced encryption of the whole device will take place.
- 4.6 Any data transferred from Trust systems to either a USB memory stick or writable CD should be automatically encrypted. The user will be prompted to select a decrypt key of their own choosing. If the data is then accessed from a Trust device the data will be decrypted automatically. If the data is accessed from a non Trust device the encryption key will be required before data can be accessed. Users are responsible for ensuring that the device has been encrypted in line with this policy. Help and guidance is available through the IT Service desk Ext 21000
- 4.7 Data transferred from the Trust via a portable media device to a non Trust PC will be autoencrypted if the data remains on the PC when the portable data device is removed.
- 4.8 Certain file types will not be transferrable between Trust PC and storage device. These would include executable files, software and program files, music and video files.

5 Laptops

- 5.1 Portable computer equipment may only be used outside Trust premises with appropriate authorisation and must be protected at all times against loss or theft. The security of portable computing devices is the individual's responsibility at all times, and staff should check their home and car insurance policies.
- 5.2 Trust laptops will have their hard drives fully encrypted. It is the responsibility of staff to ensure that the laptop they are using is fully encrypted in line with this policy. Any laptop not encrypted should be reported to the IT service desk and must not be taken off Trust premises until encryption is complete.
- 5.3 Encryption will be automatic and will run as a background process when the laptop is attached to the Trust Network.
- 5.4 The hard drive itself will be encrypted so any data transferred to the drive after the encryption process will be protected.
- 5.5 Portable equipment that is carried in a vehicle should be locked in the luggage compartment and must be removed if the vehicle is to be left unattended.
- 5.6 The Portable Computer must be placed in a securely locked location when not in use.
- 5.7 Staff should not leave the Portable Computer unattended in any public place
- 5.8 Staff should not leave the Strong Authentication token in the same location as the Portable Computer.

- 5.9 Staff should not keep password details in the same location as the Portable Computer.
- 5.10 Portable data storage devices should be kept secure at all times.
- 5.11 Faulty portable data storage devices should not be returned to the manufacturer or supplier for repair without having all data removed or destroyed.
- 5.12 Lost or stolen equipment must be reported immediately via the Trust Incident Reporting Procedure and to the IT Helpdesk.

6 User Accountability

- 6.1 Only equipment supplied or authorized by the Trust should be used to process or store identifiable personal information for Trust business.
- 6.2 **The Trust does not automatically sanction the use of personal mobile devices. Users who do use personal devices, PDA's, smartphones, etc. must ensure that Trust data transferred to those devices is fully protected in line with this policy. Any patient identifiable data held on these devices must be encrypted to the recommended 256 bit standard. It is the responsibility of the user to ensure the appropriate level of security and access control is in place.**
- 6.3 Staff may not access personal information from Trust files for their own use, to do so would be viewed as a serious breach of privilege incurring disciplinary action which may include dismissal.
- 6.4 Staff are bound by the Trust Information Security Policy and by the common law duty of confidentiality concerning the information that they use as part of their work for the Trust.
- 6.5 Backup of the system software and configuration must be made on a regular basis. The portable computer should be connected to the local network and booted from the user domain on the local server as regularly as possible (at least weekly), to maintain the currency of operating systems and virus protection software.
- 6.6 Disposal or maintenance of portable computer equipment that may hold personal identifiable information must be referred to the IT Helpdesk.
- 6.7 Staff may not use Trust portable computers or systems to access or attempt to access any systems or networks that they are not authorised to use or are not permissible for Trust business use. Such unauthorized attempts or access will be viewed as serious breach and will result in disciplinary action which may include dismissal.

- 6.8 Portable computers supplied by the Trust for use on Trust business outside Trust premises may only be connected to NHSnet at a location for which NHSIA code of connection approval exists. Portable computers must not be connected to the Internet through a non NHS Internet Service Provider. Remote access via Dial up to the NUTH network will be possible where permission has been granted.
- 6.9 **Staff are responsible for ensuring that any portable storage device taken off site is fully encrypted in line with this policy.**
- 6.10 Staff must comply with the [Trust Email](#) and [Internet](#) policies.

7 System and data integrity

- 7.1 Staff must not introduce computer viruses or related malignant code into Trust information systems. To do so deliberately will incur disciplinary action that may include summary dismissal and prosecution. The Trust will install virus protection software and will make staff aware of procedures designed to minimise the risk of infection. Disregard of procedure resulting in virus infection of Trust systems will be considered a serious breach of Trust policy.
- 7.2 The Portable Computer Systems must have an Anti-Virus software package installed. Users are not to alter the configuration of this package. The anti-virus system's database of virus definitions must be updated on a regular basis, each day if possible, but at least weekly.
- 7.3 All serious virus infections which have not been automatically eradicated by the system's anti virus software must be reported to the IT Helpdesk who will in turn report the incident to the NHS Information Authority.

8 Responsibilities

- 8.1 Staff shall be familiar with all Trust policies covering data processing and shall not perform any action in breach of those policies that could render the Trust liable at law nor shall any member of staff process or use data in breach of Trust policies in such a way as to bring the Trust into disrepute.
- 8.2 The software and information held on portable computer systems is subject to the same audit procedures as all other Trust systems. This also applies to data stored on removable data media.
- 8.3 Users should also be familiar with the Trust IT Security Policy and [Access Control Policy](#)

9 Monitoring and Audit

IT Security will use audit tools to regularly monitor device usage and encryption compliance. Suspected breaches will be investigated and reported to HR and the Caldicott Guardian.

10 Disciplinary process

Violation of these policies may subject employees or contractors to disciplinary procedures up to and including termination.

Policy author: The Director of Human Resources in conjunction with the IT Director

Further Information:

This policy should be read in conjunction with:

Freedom of Information Act

[Information Security Policy](#)

[Records Retention Policy](#)

[Freedom of Information Act Procedure](#)

[Access to Health Records Procedure](#)

Caldicott Code of Conduct on Confidentiality

The NHS Code of Confidentiality.

Computer Misuse Act 1990.

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:	Laptop and Portable Computing and Data Storage 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:		
	• Race	No	This policy re-iterates the NHS policy on data transfer.
	• Ethnic origins (including gypsies and travellers)	No	Ditto
	• Nationality	No	Ditto
	• Gender	No	Ditto
	• Culture	No	Ditto
	• Religion or belief	No	Ditto
	• Sexual orientation including lesbian, gay and bisexual people	No	Ditto
	• Age	No	Ditto
	• Disability – learning difficulties, physical disability, sensory impairment and mental health problems.	No	Ditto
2.	Is there any evidence that some groups are affected differently?	No	Ditto
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>	No	Ditto
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: There are some significant changes as this policy combines the previous data transfer and Laptop policies. Changes surround the requirements to encrypt data in transit.	Action Plan due (or Not Applicable): Not Applicable.
--	---

Name and Designation of Person responsible for completion of this form: Richard Oliver IM&T Security Manager Date:.....18th May 2010.....

Names & Designations of those involved in the impact assessment screening process:..... Andy Jardine IT Director – Tim Walls Caldicott Guardian