Wrightington, Wigan and Leigh NHS
NHS Foundation Trust

PROCEDURE:	**Use of IT Equipment Procedure**
SOP NO:	**TW12-008 SOP 2**
VERSION NO:	**1**
APPROVING COMMITTEE:	**IM & T Strategy Board**
DATE THIS VERSION APPROVED:	**November 2013**
RATIFYING COMMITTEE:	**PARC (Policy Approval and Ratification Committee)**
DATE THIS VERSION RATIFIED:	**March 2014**
AUTHOR(S) (JOB TITLE)	**Head of Information Governance**
DIVISION/DIRECTORATE	**Finance**
TRUST WIDE SOP (YES/NO)	**Yes**
LINKS TO OTHER POLICIES, SOP'S, STRATEGIES ETC:	**TW12-008 IT Acceptable Use Policy**

Date(s) previous version(s) approved (if known**):**	**Version:**	**Date:**
DATE OF NEXT REVIEW:	**March 2017**	
Manager responsible for review (Job title**)** *N.B. This should be the Author's line manager*	**Associate Director of IM & T**	

AT ALL TIMES, STAFF MUST TREAT EVERY INDIVIDUAL WITH RESPECT AND UPHOLD THEIR RIGHT TO PRIVACY AND DIGNITY

Contents		Page No.

1. INTRODUCTION

This document must be read in conjunction with the Trust IT acceptable use policy.

2. IT EQUIPMENT

Where appropriate Trust staff member will be granted personal access to computers.

2.1 Desktop, Laptop and Tablet Computers

Most Trust staff have access to desktop computers placed throughout the Trust.

2.1.1 Requests for access must be made by a line/senior manager on behalf of the member of staff requiring access. The line/senior manager must justify the reason access and must notify all applicable information asset owners of any end user intention to access information systems.

2.1.2 Any removable storage device used by any computer must be either fully encrypted or all files must be individually encrypted when removed.

2.1.3 Only authorised staff are allowed access and use of laptop/tablet computers.

2.1.4 Requests for laptop/tablet computers must be made by a line/senior manager on behalf of the member of staff requiring access. The line/senior manager must justify the reason for laptop issue and must notify all applicable information asset owners of any end user intention to access information systems using a laptop computer.

2.1.5 The Laptop/Tablet, together with any other materials issued with the laptop/tablet (bag, mouse, charger, 3G card) is the property of The Trust and remains the property of The Trust until formally disposed of.

2.1.6 Trust owned Laptops/Tablets must not be connected to any NON-NHS network connection except for the purposes of remote access to The Trust network.

2.1.7 All Laptops/Tablets will be protected by full Hard Disk Drive Encryption.

2.1.8 Non-NHS Trust owned (personal) Laptops/Tablets must not be directly connected to any Trust or NHS network connection unless specifically approved (see 5.10 Bring Your Own Device).

2.2 PDA's, Smart Phones and Blackberries.

2.2.1 Personal Digital Assistants (PDA's), Smart Phones and Blackberries all have limited computing ability and have the ability to store confidential business/clinical information, allow access to the internet/email and in the case of Smart Phones and Blackberries act as telephones.

2.2.2 Requests for PDA's, Smart Phones or Blackberries must be made by a line/senior manager on behalf of the member of staff requiring access. The line/senior manager must justify the reason for device issue and must notify all applicable information asset owners of any end user intention to access information using the device.

2.2.3 Non-NHS Trust owned (personal) PDA's, Smart Phones or Blackberries must not be directly connected to any NHS network connection unless authorised by a Head of Service or Director.

2.2.4 The device together with any other materials issued with the device (bag, charger, memory Card, SIM card, Bluetooth Headset) is the property of The Trust and remains the property of The Trust until formally disposed of.

2.2.5 All PDA's, Smart Phones and Blackberrys must be protected by whole device encryption and must have pin lock enabled.

2.2.6 Use of Smart Phones and Blackberries as telephones is governed by the Trust Telecommunications policy and Driving for Work and Occupational Road Risk Policy; all users of these devices in this manner are referred to these policies.

3. GENERAL USE OF TRUST EQUIPMENT

3.1 Acceptable Use

The following is a list of acceptable **'Trust business only'** uses for trust computers/devices;

3.1.1 Receiving and sending e-mail
3.1.2 Organising Calendars
3.1.3 Accessing Contacts
3.1.4 Accessing Tasks
3.1.5 Compose memos, letters and documents
3.1.6 Create Spreadsheets
3.1.7 Use custom Applications
3.1.8 Web browsing

All other activities must be Trust business purposes only and must not be used for non-business purposes. Personal use of e-mail and internet is acceptable within defined limits.

3.2 Unacceptable Use

The following is a list of unacceptable uses for computers/devices, it is not comprehensive;

3.2.1 Transmitting obscene, profane or offensive messages
3.2.2 Transmitting messages that violate the Trusts policies or create an intimidating or hostile work environment
3.2.3 Broadcasting personal views on social, political, or other non-business related matters
3.2.4 Soliciting to buy or sell goods or services unrelated to the Trust.

4. SPECIFIC USE OF EQUIPMENT

4.1 Messaging

4.1.1 It is permitted to use computers/devices to receive and send e-mail, to use business telephony, corporate video messaging, corporate instant messaging and fax for business purposes.
4.1.2 It is permitted to use the system to receive and send e-mail for personal purposes.
4.1.3 It is not permitted to use any other form of messaging.
4.1.4 This includes but is not limited to;
4.1.4..1 non-corporate Video Messaging,
4.1.4..2 non-corporate Instant Messaging,
4.1.4..3 VOIP / SKYPE.

4.2 Software

4.2.1 Users of computers/devices are not authorised to load any software onto the computer/tablet/device.
4.2.2 Software downloaded from the Internet must not be loaded onto the computer/tablet/device, see above (not authorised).
4.2.3 Software obtained illegally must not be loaded onto computers/devices.
4.2.4 If you require additional licensed software to be loaded please contact the ICT Service Desk.

4.3 Data

4.3.1 It is permitted to store data on the Desktop/Laptop/Tablet/Device as long as the data is required for business use.
4.3.2 If large volumes of patient identifiable data, or large volumes of business critical / business confidential information are stored, both a Line Manager and the

Information Governance Service must be informed to enable a specific risk assessment. Contact ICT Service Desk for further information.

4.3.3 All such data stored on laptop/tablet/device will be encrypted by full Hard Disk Drive/Device Encryption, or if transferred by e-mail or to a portable storage method (floppy, CD, DVD, USB Memory Stick, Portable HDD etc) will be protected using file encryption.

4.3.4 It is NOT permitted to store personal/private data on the computer/table/device. Personal data includes (but is not limited to);

4.3.4.1 family/personal photos,

4.3.4.2 family/personal correspondence,

4.3.4.3 any data not used in the day to day business related tasks of the desktop computer users.

4.4 Network Connectivity

4.4.1 Laptops/Tablets/ PCs can connect to devices in one of six possible manners;

4.4.1.1 Hard Wire Network - Only to connect to NHS network connections including VPN via home broadband.

4.4.1.2 Wi-Fi - If permitted only to connect to NHS network connections including VPN via home broadband.

4.4.1.3 Modem/Dial up - **DO NOT USE**

4.4.1.4 Bluetooth - Disable **DO NOT USE**

4.4.1.5 Infra-red - Disable **DO NOT USE**

4.4.1.6 Mobile Wireless 3G Card / Dongle - if permitted.

4.5 Camera

4.5.1 Some Laptops/Tablets/Devices have a built in camera, these can be used for business purposes only, the taking of images in relation to patient care (clinical images) is expressly prohibited. See TW11-014 Policy & SOP

4.6 Virus Control

4.6.1 The Desktop/Laptop/Tablet systems will have an Anti-Virus software package installed. This package has been installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

4.6.2 Users must not attempt 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 once a week.

4.6.3 To update your virus definitions then it is necessary to connect to the Trusts local area network. This must be done each day if possible, but at least once a week. Where a laptop/tablet is out of use for a period of time (staff holiday or illness) it is the line managers responsibility to ensure the virus definitions are updated in accordance with this policy.

4.6.4 If a virus is discovered the following actions must be carried out:

4.6.4.1 Disconnect immediately from any network,

4.6.4.2 Turn the computer off,

4.6.4.3 Put a label over the front of the machine (preventing it from being used) stating that the machine has a virus infection and should not be used,

4.6.4.4 Isolate any removable media that have been used on that machine,

4.6.4.5 Inform the IT Service Desk.

4.6.5 The IT Service Desk and Systems Team will have the software and technology available to eradicate most infections.

4.6.6 All virus infections are to be reported to the IT Service Desk using the risk/incident form.

4.7 NHS Patient Systems Token/ Smart Card Security

4.7.1 Access to NHS spine and Connecting for Health national applications is strongly authenticated. Authentication is by a National Care Records Service (NCRS) smartcard issued to the individual and entry of a secure pass code known only to the user.

4.7.2 The Strong Authentication Device (smartcard) must be afforded a high degree of protection.

4.7.2.1 Security and confidentiality of patient/staff information could be breached if a smartcard is lost or stolen.

4.7.2.2 The smartcard may in the future be used with Single Sign On to access Trust networks and clinical/corporate systems and if so, the security of the smartcard and the user's pass code will become even more critical.

4.7.3 If a card is lost or stolen it is to be reported immediately to the IT Service Desk and as an incident on the Trust Datix incident reporting system.

4.7.4 It is not permitted to share smartcards with another user. Users should lock their screen whenever leaving their station, and should remove their smartcard from the reader and keep it secure.

4.7.5 Acceptance of further terms and conditions for using NCRS smartcards is required by users when they go through the registration process to be issued with a smartcard. Failure to follow these terms and conditions for smartcard use may lead to disciplinary action – see Section 11 of this document.

4.8 Secure ID Tokens

4.8.1 Access to The Trust networks must always be strongly authenticated. That is, a strong authentication (Remote Access Service (RAS)) hardware token is used to authenticate the user before access is granted.

4.8.2 The Strong Authentication Device must be afforded a high degree of protection.

4.8.2.1 Security and confidentiality of patient information could be breached if a card/token is lost or stolen.

4.8.2.2 The card provides the owner with access to The Trust networks and ultimately any clinical system connected to the network if access rights and privileges are provided/breached.

4.8.3 If a token is lost or stolen it is to be reported immediately to the IT Service Desk.

4.8.4 It is not permitted to share secure ID tokens with another user

5. REMOVABLE STORAGE

Requests for removable storage devices/media must be made by a line/senior manager on behalf of the member of staff requiring the device. The line/senior manager must justify the device use and must notify all applicable information asset owners of any end user intention to store information from information systems.

5.1 USB Memory Sticks

5.1.1 Non-NHS Trust owned (personal) USB memory sticks must not be connected to any NHS computer.

5.1.2 Trust issued memory stick, together with any other materials issued with the memory stick is the property of the Trust and remains the property of The Trust until formally disposed of.

5.1.3 Only authorised staff are allowed access and use of Memory Sticks.

5.1.4 All USB memory sticks will be protected by file/device Encryption.

5.1.5 Staff should note that the primary purpose of USB Memory Sticks is the secure transport of information where other information transport systems are not available or suitable.

5.1.6 Removable Storage Devices must not be used to hold unique copies of information where the Removable Storage Device is used for purposes of information transport. Loss of such a device would mean loss of the information.

5.2 Recordable CD's, Recordable DVD's, Floppy Disks, Memory Cards, Removable Hard Disk Drives

5.2.1 Trust issued CD's, DVD's, Floppies, memory cards and removable hard disks memory stick, together with any other materials issued with them are the property of the Trust and remain the property of The Trust until formally disposed of.

5.2.2 Only authorised staff are allowed access and use such devices.

5.2.3 Where the media/device is to be used for data transfer the media/device will be protected by file/device Encryption.

5.2.4 Where the media/device is to be used as backup storage the media/device must be asset tagged and stored securely.

5.2.5 Staff should note that the primary purpose of such storage media/devices is the secure transport of information where other information transport systems are not available or suitable.

5.2.6 This media/device must not be used to hold unique copies of information where the media/device is used for purposes of information transport. Loss of such a device would mean loss of the information

5.3 Digital Cameras

5.3.1 Trust owned or authorised cameras can be used for business purposes only. The taking of images in relation to patient care (clinical images) is only permitted in accordance with the Trusts Clinical Photographic and Videographic Policy.

5.4 Digital Voice Recorders

5.4.1 Trust owned or authorised digital voice recorders can be used for business purposes only. When not in use the device must be stored securely. Unless encrypted all data must be removed from the voice recorder as quickly as possible.

5.5 Digital Pens

5.5.1 Trust owned or authorised digital pens can be used for business purposes only. These pens must be used in accordance with manufacturer's instructions. Where the pen contains easily extractable and easily decidable clinical/business information the device must be encrypted.

6. REMOVABLE DEVICES

6.1 Printers

6.1.1 It is permitted to install Trust owned Removable Printers, initial installation of software to control the printer will have to be carried out by a member of IT staff.

6.2 Scanners

6.2.1 It is permitted to install Trust owned Removable Scanners, initial installation of software to control the scanner will have to be carried out by a member of IT staff.

6.3 Mobile Phones, Smart Phones, PDA's & BlackBerrys

6.3.1 It is permitted to connect Trust owned Mobile Phones and PDA's & BlackBerrys, on machines with the Windows XP / Windows 2000 operating systems, however connection must be only for charging the device. No device specific software may

be installed. It is not permitted to install such devices on machines with Windows Vista or Windows 7 Operating System installed.

6.4 USB Hubs

6.4.1 It is permitted to install Trust owned USB Hubs.

6.5 Memory Card Readers

6.5.1 It is permitted to install Trust owned Memory Card Readers.

6.6 MP3 Players / IPods, USB Toys (Missile Launchers, Fans, Lights, Photo Frames) and other removable devices.

6.6.1 It is not permitted to install any of these devices without specific written permission. If permission is granted installation and removal must be carried out by staff from IT Service desk.

7. DEVICE CARE

7.1 The user of Trust IT Equipment must always adhere to the following guidelines:

7.1.1 Treat the equipment as you would your own property, with due care and attention to its physical condition and the security of the device.
7.1.2 Laptop/tablet/ and portable devices must be securely locked away when not in use.
7.1.3 Security is the users responsibility at all times.
7.1.4 If you have and use a Laptop security cable, keep one key with you and the other in a secure separate location.
7.1.5 Do not leave the Laptop/Tablets/computer devices unattended in a public place.
7.1.6 Do not leave the Portable Equipment in view in the inside of your car. Ensure it is secured out of sight.
7.1.7 Do not leave your strong authentication (RAS) token(s) or smart card (if you use one) in the same location as the Computer/Laptop/Tablet/Device.
7.1.8 Avoid leaving the portable equipment within sight of ground floor windows or within easy access of external doors.
7.1.9 Ensure portable devices are protected from heavy vibration and physical shock.
7.1.10 It is not advisable to place heavy objects on the case of a laptop.
7.1.11 It is not advisable to touch the screen of a desktop/laptop computer.
7.1.12 Take care of network cables as the connectors can be easily broken.
7.1.13 Always turn off Laptops/Tablet PC's before storing in a travelling bag.
7.1.14 Avoid subjecting the Laptops/Table PC's to extremes of temperature, for example leaving it in your car during hot days or cold nights.
7.1.15 Please keep all liquids and food away from IT computer equipment.

7.2 Maintenance is to be controlled by IT Service Desk in conjunction with IT support. The following is for their guidance: -

7.2.1 All equipment that requires repair or maintenance must have patient sensitive/confidential information removed from it.
7.2.2 It is not sufficient just to delete files using the computer operating system. The data must be removed correctly using a third party software application that guarantees approved deletion of files.
7.2.3 Where it is not possible to delete the files e.g. screen failure. The Hard Disk Drive should be removed from the machine before it is forwarded for repair.
7.2.4 If the hard disk has failed and the maintenance engineer is required to replace it with a new device then the old hard disk must be physically destroyed.

8. BACKUP

8.1 Desktop computers/Laptops/Tablets/Devices are not backed up automatically. Users must back up all critical/sensitive data on a regular basis to a separate system (your local area network personal drive where possible) to help prevent the loss of critical information. The restoration of backed up data must be tested on a regular basis.

9. BRING YOUR OWN DEVICE

9.1 The Trust is aware that there are potential benefits from allowing staff to use their own Laptop/Tablet/PDA/Phone. The Trust reserves the right to allow staff to use their own device subject to an appropriate business case for device use, appropriate risk assessment and appropriate technical and procedural controls around the use of the device. The Trust will communicate the availability of any Bring Your Own Device initiative via the Trusts intranet and will issue a separate policy with regards such devices.

10. HUMAN RIGHTS ACT:

Implications of the Human Rights Act have been taken into account in the formulation of this policy and they have where appropriate, been fully reflected in its wording.

11. ACCESSIBILITY STATEMENT:

This document can be made available in a range of alternative formats e.g. large print, Braille and audiocd.

For more details, please contact the HR Department on 01942 77 (3766)or email equalityanddiversity@wwl.nhs.uk