Derby Hospitals NHS
NHS Foundation Trust

TRUST POLICY AND PROCEDURES FOR MOBILE DEVICES

Reference Number **POL-IG/252/2014**	**Version: V1**		**Status:** Final	**Author: Job Title** – Deputy Information Governance Manager
Version / Amendment History	Version	Date	Author	Reason
	1	Jan 2014	Anne Woodhouse	New policy
Intended Recipients: All Trust staff, visiting staff from other organisations, employees of temporary employment agencies and third party users and contractors.				
Training and Dissemination: All staff using Trust IT Systems will be made aware of the IT Policies and Procedures. Training sessions given to appropriate staff by the IT Training Team. Dissemination via the Trust Intranet.				
To be read in conjunction with: Trust Policy for Information Governance; Trust Policy & Procedure for Information Technology Operations, Trust Policy for Data Protection; Trust Policy and Procedures for the Use of Internet and Email (including Access via Mobile Devices); Trust Policy and Procedures for Incident Reporting, Analysing, Investigating and Learning; Trust Disciplinary Policy;				
In consultation with and Date: Information Governance Steering Group				
EIRA stage one Completed Yes Stage two Completed N/A				
Procedural Documentation Review Group Assurance and Date	February 2014			
Approving Body and Date Approved	ME – February 2014			
Date of Issue	February 2014			
Review Date and Frequency	February 2017 extended to 30 April 2018 at Jan 2018 Trust Delivery Group meeting TDG EXTENDED DEC 2020			
Contact for Review	Information Governance Manager			
Executive Lead Signature	Director of Finance and Information			
Approving Executive Signature	Director of Finance and Information			

Contents

TRUST POLICY AND PROCEDURES FOR MOBILE DEVICES

1 Introduction

Technology is developing rapidly enabling small and or portable electronic devices, such as smart phones, laptops, tablet notebooks and other mobile storage devices to be utilised for communications, accessing information, capture, transmission and storage of records. It also allows access to internal networks from locations other than the normal working environment, e.g. at home, in a vehicle or whilst moving from one location to another. Whilst there are many benefits, the use of these devices brings many risks. They can be lost, mislaid or stolen and there are also risks to the integrity of networks.

2 Purpose and Outcomes

The purpose of this Policy and Procedures is to ensure that

- The organisation has clear procedures for the use of portable devices.
- All risks associated with portable devices are addressed and minimised.
- Legal requirements relating to security and confidentiality of equipment and information are adhered to.

3 Definitions Used

Acceptable Use	Users of the Trust information systems understanding their responsibilities regarding appropriate and proper use.
Encryption	An encryption tool will 'translate' your data into unreadable code, for which only you or another authorised user will have the key or password to decode it.
Mobile Device	Smart phones, laptops, tablet notebooks, phone SIMS and other media, i.e. any mobile storage device.
Network	The network is a collection of communication equipment such as servers, computers, printers, and modems, which has been connected together by cables or wirelessly. The network is created to share data, software, and peripherals such as printers, modems, fax machines, and Internet connections.

4 Key Responsibilities/Duties

4.1 Associate Director of IM&T

The Associate Director of IM&T is responsible for ensuring the Trust Policy and Procedure is effectively implemented.

4.2 Head of IT Services

The Head of IT Services is responsible for overseeing the operational management of this policy and will ensure that effective security countermeasures are produced and implemented.

4.3 IT Service Desk

The IT Service Desk is responsible for recording all incidents relating to loss or misuse of mobile devices to ensure information held on the device is erased.

4.4 Records and Information Governance Manager

The Records and Information Governance Manager ensures that the Trust has a managed and co-ordinated standard based approach to Information Governance, providing staff with clear policies and procedures that ensures the organisation meets its statutory and legal obligations.

4.5 Line Managers

Line Managers must:

- Ensure that the security of the network, i.e. information, hardware and software used by staff and, where appropriate, by third parties is consistent with legal and management requirements and obligations.
- Ensure that staff are made aware of their security responsibilities and have had suitable security training.
- Ensure that staff only use the mobile device for what is was originally purchased for.

4.6 All Staff (including visiting staff/contractors)

All Staff are responsible for complying with this Policy and any additional security requirements.

All Staff must:

- Safeguard hardware, software and information in their care
- Prevent the introduction of malicious software to Trust IT systems
- Report any loss of device or suspected/actual breaches in security

4.7 Information Governance Steering Group

The Information Governance Steering Group is chaired by the Caldicott Guardian and reports to ME. The group is responsible for ensuring that the standards and requirements for information governance are implemented and understood across the Trust.

5 Implementation of the Policy for mobile devices

5.1 Smart phones used for NHS mail

All staff who use a trust Smartphone to access NHS mail must adhere to the NHS mail Acceptable Use Policy which is automatically applied:

- A password is required to unlock the device
- The inactivity timeout should be set at a maximum of 20 minutes. After this time, or if the device goes into standby mode, the password has to be entered to unlock the device
- If an incorrect password is entered 8 times in succession, the phone will be automatically wiped of ALL data and restored to its default factory settings.
- The maximum message size is 500KB. You can receive messages over this size in your NHSmail mailbox but not on your phone.
- You are required to change the device password every 90 days
- Encryption at rest will be enabled on devices with the built-in capability to support it.

Once the policy has been applied to the device it can only be removed by performing a factory reset of the device.

Many phone manufacturers offer a 'Cloud' service (e.g. iCloud, Skydrive, Google Drive) where you can synchronise data, photos or email from your phone over a wireless internet connection to a Cloud service. If you configure your device to use a Cloud service and access your NHSmail account, you must ensure that email is not set up to be synchronised to the Cloud service. This is important as synchronising NHSmail to the Cloud service means that patient data will be transmitted over a potentially unsecured wireless network putting sensitive data at risk. Data stored on Cloud cannot be removed.

Patient identifiable information must not be stored on any mobile phone, other than the information processed via NHS mail.

If the device is lost you must inform IT service desk of the loss. You must also ensure that you remotely wipe the device. For assistance with this please contact the IT Service desk.

5.2 Trust tablets and laptops

All laptops issued by the Trust are encrypted with approved software to a minimum of 256 bit encryption with strong password protection.

Sophos Mobile Device Management software will be installed on to all Apple iOS, Android and Windows tablets. This enforces built-in security features such as passwords and device encryption. It also provides the ability to remotely manage, configure and update tablets. Furthermore, it gives the Trust a tool to monitor device activity and wipe the device.

Lost devices must be reported immediately to the IT Services Service Desk on 01332 785777. IT will use Sophos to send an instruction to remotely wipe the tablet of all data.

Standard functions from the tablet manufacturer may be disabled for security purposes and application installation can be prevented. Before any application can be used to store patient identifiable information, approval from Information Governance must be sought.

Staff must not attempt to disable any of the security measures which are in place, or install a non-approved version of the manufacturer operating system and firmware.

Sensitive information should only be saved onto a mobile device when an alternative method is unavailable. If a device is used to collect patient information it must be kept secure at **ALL** times. If it is necessary to use a mobile device to process information, the information must not be stored permanently on the device - It must be transferred to the Trust server at the earliest opportunity and deleted from the device. A shared device must have a named custodian who will be responsible for booking it in/out and recording usage. All passwords must be reset on change of custodian.

Anti-virus software is installed on all Trust IT equipment and kept as up to date as possible. Devices should be connected to the network monthly to enable them to receive the latest anti-virus updates. All staff must take precautions to avoid contamination of data for example by use of unauthorised software that may contain a computer virus. Never attempt to access files from any removable media that you may have found, not even to determine to whom it might belong – it could contain a computer virus. Instead you should pass it on to IT Services.

As with all Trust IT equipment, mobile devices must not be used for personal and recreational use and should NOT be accessible to family members or visitors.

If the mobile device develops a fault this must be reported to the ITService desk and they will arrange for a technician to look at the problem and if necessary report it to a third party organisation. The ITService desk must be made aware of any patient identifiable information stored on the system. Hard drives must be removed before the device can be sent offsite for repair.

5.3 Confidentiality

All users should be aware that the use of mobile devices in public places will likely draw the attention of those in the vicinity. It is possible that information viewed on the screen could lead to unauthorised disclosure of the information being processed.

Users should not draw attention to the confidential or sensitive nature of data stored on removable media by the way that they are labelled, even if the data has been encrypted.

Devices being used outside the usual workplace should adhere to the Clear Desk Policy:

- Ensure the screen is locked
- Remove smartcards or other access management devices
- Ensure paper and other media is locked away, especially Person Identifiable Data or Sensitive Data
- Secure any multi-function systems so that only authorised personnel can use them

Staff should also ensure that they are meeting the requirements of the Data Protection Act, and at all times behave in accordance with UK law.

5.4 Physical / Hardware Security

Any hardware or software provided by the Trust remains the property of the Trust and shall be returned at the end of the working arrangement.

Mobile devices, even when protected by encryption, should not be left in the care of any person who has not been authorised by the Trust to access the data.

Mobile device security is the custodian's responsibility at all times. The following principles must be adhered to by the user of the device:

- Mobile devices are valuable and susceptible to theft. These devices must not be left unattended in public places and should only be stored in car boots for a short period of time; NEVER OVERNIGHT AND NOT WHILST PARKED IN A PUBLIC CAR PARK.
- Do not leave your Strong Authentication token in the same location as the device.
- All removable media such as CD-ROM and USB Flash Drives should be removed unless absolutely necessary.
- Do not keep password details in the same location as the device.
- Avoid leaving the device within sight of ground floor windows or within easy access of external doors.
- Carry mobile computers in protective anonymous bags or cases (i.e. those without manufacturer logos on them) when not in use.
- Be aware of the potential for opportunist or targeted theft of mobile computer bags in public places including airports, train stations, hotel lobbies, exhibition halls etc and on public transport e.g. buses and trains.
- Do not leave mobile devices unattended in unsecure areas, for example meeting rooms next to areas of public access, and hotel rooms where others may have access. Make use of room locks and lockable storage facilities where available.
- Staff must not install additional hardware or storage devices to PCs or laptops without the prior approval of IT Services.

5.5 Visiting staff/contractors

Speakers or lecturers may arrive at the Trust with presentations saved on mobile devices. To protect the Trust's network, mobile devices must be virus checked and must only be connected to the Trust's guest network. For guidance or advice, please contact the ITService desk.

If an external organisation visits the Trust and wishes to use a mobile device to deliver or collect information, the IT Services Department must be contacted prior to use.

6 Monitoring Compliance and Effectiveness

Monitoring Requirement:	General issues regarding non-adherence to policy, i.e.: ⌄ Lost equipment being reported immediately so that devices can be disabled/wiped. ⌄ Employees who are leaving the Trust ensuring that all equipment is returned to the IT Services Department so accounts can be disabled on the last day of employment
Monitoring Method:	ITServicedesk calls (recorded on HEAT) and subsequent Incident Reports (IR1 / Datix) - Monitored as one of the standards in the Information Governance Toolkit.
Report Prepared by:	Information Governance Manager
Monitoring Report presented to:	Information Governance Action Group (as part of Toolkit monitoring)
Frequency of Report:	6 monthly

7 References

NHS Care Records Guarantee (2009)
BS ISO/IEC 27002:2005
BS ISO/IEC 27001:2005 BS7799-2:2005
Department of Health (2007) Information Security NHS Code of Practice
NHS Connecting for Health (2007) Remote Access Good Practice Guidelines
NHS Connecting for Health Good Practice Guidelines on the Secure Creation and Management of Data on Removable Media

NHS Connecting for Health Good Practice Guidelines in Information Governance – Information Security
NHS Connecting for Health (2007) Firewall Technologies: Good Practice Guidelines
NHS Connecting for Health (2006) Secure Use of the New NHS Network (N3): Good Practice Guidelines

NHS Connecting for Health (2005) Wireless LAN Technologies: Good Practice Guidelines
Data Protection Act (1998) www.dataprotection.gov.uk

Connecting for Health (2006) Disposal and Destruction of Sensitive Data: Good Practice Guidelines

NHS Information Authority (2003) Business Continuity Planning Manual, Business Continuity Planning for NHS Organisations