County Durham and Darlington NHS
NHS Foundation Trust

CDDFT Policy

Reference Number	POL/HI/0036
Title	**Mobile Devices Policy**
Version number	1.1
Document Type	Policy
Original Policy Date	November 2015
Review and Approval Committee	Information Governance Steering Group and Planning and Workforce Committee
Review and Approval Date	June 2019
Next review date	31 July 2019
Originating Directorate	Commercial Services
Document Owner	Head of Information Governance & Head of ICT
Last review date	September 2015
Lead Director / Associate Director	Andrew Izon, AD HI
Scope	Trust Wide
Equality Impact Assessment (EIA) Completed on	10/09/15
EIA sent to Equality Lead	November 2015
Status	Approved
Confidentiality	Staff in Confidence
Keywords	Mobile Devices Policy; replacing mobile equipment policy

Approval

Signature of the Sponsoring Director	
Name / job title of Sponsoring Director	Noel Scanlon, Executive Nursing Director
Signed paper copy held at (location):	IG DMH Office

Version control table

Date of issue	Version number	Status
Nov 2015	1.0	Superseded
June 2019	1.1	Approved

Table of revisions

Date	Section	Revision	Author
September 15	all	New policy for review	HOIG
Oct 15	all	review	ICT
June 2019		Policy extended till 31 July 2019	

Contents

INTRODUCTION

1.1 Executive Summary

Document Objectives

This policy sets out some high level principles that must be adhered to when using mobile devices to connect to Trust networks or to host Trust data. These are designed to ensure that Trust data is adequately protected from unauthorised access, both at rest and in transit over data networks, and to help ensure compliance with the NHS Code of Confidentiality, the Caldicott Principles and the Data Protection Act.

Group/Persons Consulted:

Health Informatics Department, Caldicott Guardian, SIRO, Information Governance Steering Committee (IGSC)

Monitoring Arrangements and Indicators:

Information Governance Toolkit, SIC, staff surveys and feedback, SIs/SIRIs, SIAO reports to SIRO, SIRO to Trust Executive.

Training Implications

All staff need to inter-relate this document with the specialist procedures and SoPs for Trust issued mobile devices

Resource Implications

Training carried out during working hours

Intended Recipients

All Staff Using Mobile Devices, All Information Asset Owners (IAOs)

Who should:

Be **aware** of the document and where to access it

All Senior Managers, Information Asset Administrators (IAA)

Understand the document

Staff dealing with and using mobile devices and mobile media.

Have a **good working knowledge** of the document

Mobile Device Users, Informatics Directorate, Caldicott Guardian, SIRO, staff of IG.

1.2 Policy Introduction

County Durham and Darlington Foundation NHS Trust (CDDFT) are reliant on electronic information that is captured, stored, processed and delivered by computers and their associated communication facilities. Such information plays a vital role in supporting business processes and customer services, in contributing to operational and strategic business decisions and in conforming to legal and statutory requirements.

Business use of mobile devices with data hosting and processing capabilities has increased dramatically in recent years.

Accordingly the electronic information and the enabling technology are important assets that must be protected to the level commensurate with their value to the Organisation. Special care must be taken to ensure that business information is not compromised especially when such equipment and data is used in conjunction with storage media that may be removed from the system to other locations by various means of mobile equipment and methods.

This policy addresses the security and confidentiality of equipment and data whilst separated from the main systems, and confidentiality of equipment and data whilst accessed or transported 'off site'.

2 Purpose

The purpose of this policy is to ensure that all staff are aware of their individual responsibilities in relation to the use of removable storage for the securing and storage of organisational data especially that of personal identifiable information.

This policy sets out some high level principles that must be adhered to when using mobile devices to

- Connect to Trust networks or to host Trust data.
- Connect to public networks
- Connect to private Wi-Fi hubs e.g. staff or patients' homes

2.1 Policy Objectives

These principles are designed to ensure that Trust data is adequately protected from unauthorised access, both at rest and in transit over data networks, and to help ensure compliance with the NHS Code of Confidentiality, the Caldicott Principles and the Data Protection Act.

This policy applies to all employees including contractors of County Durham and Darlington Foundation NHS Trust who use, or may have access to use removable storage devices. The purpose of this policy is to provide instructions on the security of equipment off the premises of the Trust, and ensuring patient identifiable information is kept confidential to the Trust when using mobile equipment.
If you use a mobile device (Trust provided) to store, access or transmit Trust data, it is vital that you read this policy carefully.

<u>If there is anything you do not understand, it is your responsibility to ask your line manager to explain or to contact the IT or Information Governance departments for clarification.</u>

If you fail to comply with this policy you may be subject to Trust's disciplinary procedures and / or legal proceedings. Your failure to comply may also result in legal proceedings against the Trust.

3 Scope

All mobile computing devices (Trust provided) used to receive, store and/or transmit TRUST data.

This includes, but is not limited to: Blackberry handhelds, smartphones, laptops, netbooks, tablet PCs, USB flash/hard drives, removable media and portable digital assistants (PDAs).

"Only Trust provided and approved devices may directly connect to the Trust network, all other devices are expressly prohibited and will contravene Trust Policy which will lead to disciplinary action. Other devices include any form of IT and communications equipment not owned and approved by CDDFT NHS Trust IT Department".

This policy sets out high level, generic security requirements – it does not include any platform specific configuration requirements. Where such requirements are defined in a more specific Trust standard, you are expected to adhere to that standard in conjunction with this policy.

4 Duties

This policy applies to all Trust staff, and all other parties who are given access to Trust data, including business users, technology providers, trainees and contractors.

Overall responsibility for the enforcement of this policy lies with the Chief Executive of the Trust, or anyone identified by them as having responsibility in this area.
To assist the Chief Executive with the discharge of these responsibilities, the Associate Director of Health Informatics and the Head of Information Governance and IT Security & Head of ICT have been delegated this responsibility. Further to this, designated members of staff within the Trust will be allocated responsibility for the maintenance of a register detailing the security arrangements in respect of Trust assets whilst away from the Trust. Oversight of IT security implementation is one of the responsibilities of the Planning and Workforce Committee through the Information Governance Steering Group.

It is the responsibility of the Planning and Workforce Committee to monitor the overall implementation of the policy on behalf of the CDDFT.

No deviation from the statutory and legal obligation of the Trust can be sanctioned whatsoever.

Any request to vary this policy must be considered by the Information Governance Steering Group before authorisation. In the event of an emergency, the Chief Executive will authorise and then submit the reasons for approval to the next meeting of the Information Governance Steering Group.

It is the responsibility of the Trusts Information Governance team to maintain the policy, reviewing it on an annual basis or following any major Trust changes, to ensure that it remains applicable.

This policy applies to all staff of the Trust and to any contractors involved in the secure storage, safe handling and secure disposal of such media and any associated data.

Each and every employee of the Trust is responsible for the implementation of this policy whilst operating any mobile computer or device, used in connection with business purposes and whilst utilising any removable storage device, used in connection with business purposes.

5 Mobile Devices Policy

5.1 Identified Risks

Most forms of removable media require no form of authentication, password protection, or configuration to install or use and they can make use of “plug and play” technologies and generally do not require any administrator privileges to install.

Unauthorised disclosure of sensitive data, along with the obvious potential of public embarrassment to the Trust, could occur if an item of removable media fell into the wrong hands.

In addition to their authorised data, users may also inadvertently transport, and therefore introduce, malicious software on to Trust systems.

Their capacity would enable the storage of databases not just individual records increasing exposure risks

The nature and tangible size of removal media is such that they are also prone to accidental loss and / or theft.

5.2 General Policy Statements applicable to Trust Owned Devices

Applicable policy statements are categorised below:

5.2.1 Audit and Monitoring

- All Trust supplied mobile devices and their contents remain the property of the Trust and will be subject to regular audit and monitoring.

5.2.2 Connecting to non-Trust equipment

- In order to protect the Trust from malware, you must not connect Trust owned mobile devices to your home computer unless that computer:
  - is running an up to date anti-malware product. **and**
  - is up to date with recent operating system and application security patches.

5.2.3 Data backup and synchronisation

- Trust data should only be stored temporarily on the device. The device should be regularly backed up to a secure location on the Trust secure network to minimise impact of data loss in the event of a hardware failure. (Minimum of every month). The devices will lock out after 6 weeks if not plugged into the trust network to update the Anti-virus and encryption.
- Trust owned devices should preferably be synchronised only to Trust equipment, to ensure that Trust data is not synched or backed up to devices that are insecurely configured, and to reduce the risk that the device becomes

infected with malware.

- Where there is a business requirement to synchronise Trust data to non-Trust equipment, care should be taken to maintain the security of that data[1]. Personal identifiable or sensitive personal data (see definition in section 11.1/2) must be protected as per the requirements of the Trust's Transfer of Personal Identifiable Information Policy.

5.2.4 Compliant Device Configuration

- Trust devices on managed services (e.g. the iOS Apple service) are supplied pre-configured in a compliant state. Once received the user is not authorised to change any security device settings without reference to the service desk, as they may affect the security of the device, or stop it functioning with the supplied service. (This does not apply to resetting the PIN or password)
- Trust devices on other services may not be supplied pre-configured in a compliant state, depending on the service being offered. Advice should be sought from the department supplying the device as to how to configure such devices to comply with this policy and any device specific Trust standards.
- See section 5.3 of this policy for more detailed configuration requirements for telephony capable devices.

5.2.5 Loss / Theft and Physical Security

- If a Trust owned device is lost or stolen, then the IT Service Desk should be contacted as a matter of urgency so that the Trust data network can be protected from the device and to enable it to be remote wiped where that functionality exists (see Section 5.3.2 below). Your call will be passed to the relevant service desk.

  Additionally, the Trust incident reporting form should be completed and the loss reported on safeguard, to the relevant line manager and to IG Department.
- Physical security – The device must be kept securely at all times. For example it should never be left unattended in a car, in a hotel room (except in a safe) or on the floor of a bar/restaurant in a bag or at home (visible through window). All devices must include a passcode setting to secure if lost or stolen in addition to encryption etc. ref: Transfer of Personal Information Policy

5.2.6 Installation of Software (on the mobile device)

- You must not install any software unless you have a licence that is valid for commercial use through the IT helpdesk as they may have a trust wide license and or an alternative approved solution to fulfil requirements.
- Please note for **Trust encrypted laptops**, you cannot install software yourself – you should request this via the IT Services Service Desk, as they may have a trust wide license and or an alternative approved solution to fulfil requirements.

5.3 Disposal or maintenance of all devices

Disposal of portable computer devices that may hold personal identifiable or highly sensitive information must be referred to the IT Service Servicedesk.

[1] For example, mobile phone backup tools bundled with synchronisation software are increasingly offering encrypted backup functionality. Access to such backups could then be secured using a strong password. Please contact Trust IT Service Desk for specific advice.

In liaison with the IT servicedesk, portable computer devices in need of repair should be returned to IT Services. It is the responsibility of the IT operations manager or the ICT manager to ensure that all sensitive information is deleted from the device prior to disposal.

5.4 Device Configuration Policy Statements

These generic configuration policies must be adhered to:

- As a condition for attaching your Trust Owned mobile device to certain Trust data services. (E.g. The Trust's Mobile E-mail Service - MES); and/or
- Where the device is used to store "Personal identifiable or sensitive personal data" see definition in section 6 below.

Where an approved platform specific configuration standard exists – that must be complied with.

Where functionality referred to does not exist for your device – refer to the approved platform specific configuration standard for applicable policies and guidance.

5.4.1 Encryption

- Phone memory encryption must be enabled. Insertable memory card encryption must be enabled[2].
- Please refer to the Trust's Data Encryption Policy for specific policy guidance on how to protect Confidential Data with encryption for Trust owned devices.

5.4.2 Device Locking

- Device lock must be enabled with a PIN of at least 4 digits (this should both include letters and numbers where supported) **or** a swipe pattern that uses at least 6 nodes or a biometric touch ID.
- Device lock must be set to auto engage after a maximum of 15 minutes
- SIM lock should be enabled with a PIN of at least 4 digits. 6 digits are recommended.
- Device lock and SIM lock codes must be required on phone boot in order to access phone functions and data.

5.4.3 Jailbreaking3

- This will be dealt with in platform specific configuration standards in accordance with risk associated with that platform. Jailbroken devices should be regularly reported on and removed from the network.

5.4.4 Anti-malware

- No high level policy statement. This will be dealt with in platform specific configuration standards in accordance with risk associated with that platform.
- Any applications downloaded must be scanned for malware prior to installation however except where the Trust software review policy clearly asserts that this is covered.

[2] This requirement refers to encryption services provided by the device, not third party encryption tools

[3] Jailbreaking refers to the practice of unlocking a device to enable root access and installation of applications from outside of authorised repositories. It increases the risk of malware infection on a device.

5.4.5 Remote disablement and wiping

- Remote wipe functionality must be configured where it is available on Trust owned devices.
- Remote wipe functionality should be configured on personal devices where it is available – the device owner will be required to sign a waiver agreeing that the Trust may action a remote wipe on a personal device if and when it is deemed necessary by the Trust, and only where authorised by Trust Information Security. Where technically feasible only Trust data will be wiped, but it may be necessary to wipe ALL data.
- Remote SMS locking functionality should be configured where it is available. (This functionality allows you to pre-set an alphanumeric code which when received as the sole component of an SMS message, will immediately lock the phone – requiring PIN entry to unlock.)
- Incorrect password entry functionality should be configured to wipe the device after 6 incorrect password entry attempts.

5.4.6 Touchscreen devices only

- Where available password/PIN entry mode should be configured to use a secure entry mode where the position of the characters on screen changes each time you log on.

5.5 Functionality dependent policies

This section contains policy statements that are only applicable to devices where the relevant functionality exists.

5.5.1 Specific points on the use of mobile devices with camera functionality

- The use of camera functionality on mobile devices must comply with other Trust policies on filming and photography:
- Trust issued mobile devices enabled with cameras should primarily be used for taking business related pictures. Storage must not interfere with Trust business use.
  - Inappropriate content prohibition on Trust owned devices applies equally to mobile phones as it does other forms of communication. Please refer to the Trust's Internet and Acceptable Use Policy.
  - Privacy, only take pictures of individuals with their permission to do so, or follow current policy where this is impractical.
  - Photographs taken for business reasons are recommended to be backed up to the Trust data network as soon as possible to prevent the risk of the data being lost should the device fail.

5.5.2 Specific points on the use of Bluetooth enabled devices (Trust owned devices only)

- Bluetooth must only be used for accessing passive devices – such as hands free kits.
- Bluetooth cannot be used to communicate with a device directly connected to the Trust data network (unless through a Trust owned or leased PC/laptop).
- Bluetooth connections must be accepted from other devices with care. Ensure the recipient is known and agree connection security criteria in advance.
- Never run a Trust owned device in broadcast mode, various viruses and

other schemes are prevalent whilst in this mode.

5.5.3 Specific points on the use of Infrared enabled devices (Trust owned devices only)

- Infrared must only be used for accessing passive devices, no sync should be performed using the interface (unless through a Trust owned or leased PC).
- Infrared cannot be used to communicate with other devices, and should be turned off.
- No Trust data can be sent to other devices (including Trust owned ones) using the Infrared protocol.

5.6 Non phone-based mobile computing devices

This section contains policy statements relating to mobile computing devices other than mobile phones/smartphones. It is organised by category.

5.6.1 Laptops / Netbooks / Tablets

- Use of McAfee Full Disk endpoint encryption product (standard on Trust desktop) is required as a condition for hosting Confidential Data. See the Trust Mandated Policy for the Transfer of Person Identifiable Information and other Sensitive or Confidential Information.
- Be aware that by default all the data files you create and save into your “my documents” folder, will be saved both locally on the laptop (or similar) and onto the network. Every time you connect to the Trusts network with your laptop (or similar device) your files will synchronise. In this situation your data files have been set to be made available “offline”.
- Ensure that, as a general rule, confidential and sensitive documents are saved only in “on line” folders and drives. This means that when you are not connected to the Trusts network, the files will be unavailable, as they are not saved locally on the laptop.
- Contact IT Service desk for advice when setting your folders to be “on line”.

5.6.2 USB attached data storage

This includes portable hard disks, flash or thumb drives and memory cards in digital devices (e.g. cameras/photoframes/mp3 players),USB sticks, portable hard drives, Blu-ray discs, DVDs, CDs, floppy disks, tapes and Iomega Zip/Jaz cartridges or equivalent

- Trust confidential data must not be stored on these devices unless an encryption method compliant with the Trust’s Data Encryption Policy is used to protect it.
- Devices must be scanned with the corporate anti-virus solution prior to copying any files to or from them. Trust owned confidential information must not be stored solely on removable devices.
- Care should be taken to ensure the security of such material and devices.
- The Trust states no storing or transferring of personal identifiable data in your USB or PDA Outlook calendar or email is acceptable. This can only be completed with an encrypted mobile device and encrypted email. Contact the IT department for further information.

- When using any mobile media e.g. USB port or CD rom perform a manual Anti virus scan on pc before opening any file held on the device.

- If you misplace or lose your USB / PDA or it is stolen, notify IT Service Desk immediately x 32777.
-

5.6.3 Digital music/video players (e.g. iPods)

- If the device is Trust owned, and you choose to store personal music or video (i.e. media that is not owned by the Trust), this must not be synched to the Trust data network.
- Trust owned media content must not be stored solely on personal devices. Care should be taken to ensure the security of such material.
- Digital music/video player devices should normally be connected in "Mass Storage" mode and scanned for malware at the point of connection. Synchronisation software that has been integrated for the Trust desktop can be used. Depending on the product -installation may be subject to Information Governance, IT Services or, exceptionally, Trust Board approval of the business case.

5.7 Storage devices

Only devices owned and supplied by the Trust may be used with Trust systems, to ensure full security of the information.

Personal Identifiable Data and other highly sensitive data must be protected at a minimum of 128bit encryption levels when stored on removable media. In the absence of this the Trust has in place a minimum requirement for the storage of data which is strong password protection on information sent via Trust (CDDFT) email. A strong password is defined as being at least 8 characters in length using random upper and lower case alphanumeric characters and symbols. If you need encrypted email please self-register for an nhs mail account and follow instructions given.

Only devices owned and supplied by the Trust may be used for business purposes. You must have written authorisation from your line manager before removing equipment from the premises and it is the responsibility of the IT department to ensure that the computer has up to date anti-virus software and hard disk encryption software installed. When using a Trust owned computer, you must comply with the Trusts policies and procedures which include the IT Security policy, IT Home working Policy, the E-mail code of practice and Internet acceptable use policy.

When using all storage devices, you must comply with the Trust IT Security policy.

Removable Media should only be used to transport or store data when other more secure means, e.g. internal e-mail or using network-shared folders, are not available. If there is personal information that is being transferred in this way there are security steps that must be taken to avoid loss of data. See appendix 1 – secure transfer of personal data. Your Divisional Information Asset Owner must be informed of any information flows to ensure these are added to the Divisional information asset log and risk assessed.

Ensure that data is only held on the removable data storage device for a specific purpose. As soon as is practicable, move the data file(s) back onto the Trusts network.

"On Access" anti-virus and malicious software scanner controls must be configured on servers and workstations to check for removable media devices. Rather than scanning whole systems, on-access scanners scan files and other objects, such as removable media and their associated drives when they are accessed. Access is not allowed to such objects until the scanner has checked them.

Staff should not use their own (or unauthorized) portable computer device or digital storage device for Trust business.

The use of patient identifiable data or staff identifiable data of a sensitive nature such as appraisal, complaint or disciplinary on staff owned equipment is strictly forbidden. Appendix 1

5.8 Use of electronic personal information files at home

The use of Trust personal identifiable data at home is **not permitted** and is referred to and governed by the Trust IT Home working policy and Trust Improving working lives Policy section 11 – home working.

- Data must only be used in accordance with the legitimate business of the Trust as detailed in its registration. A separate notification to cover use whilst away from the users base is not required.

- Formal written authorisation by your line manager must be obtained before personal identifiable data files can be taken off site.

- Personal identifiable data must not be sent via email without the data being secured by an approved encryption certificate.

- Personal (non-organisational) e-mail accounts must not be used to send or receive patient / client sensitive information.

- No unauthorized software may be added to the computer or any copies taken of the software on the computer's hard disk. An undertaking not to do so form part or the agreement signed when the loan is approved.

- Privately owned computers must not be used for business purposes, only computers owned and supplied by the organisation may be used to capture, store or access patient and business data.

- Information must not be stored on the hard disk drives of computers that do not have hard disk encryption enabled.

- Where a Trust computer is to be used at home then written confirmation that appropriate insurance cover is in place must be obtained before approval can be given to the loan. The Trust's insurance does not cover equipment loaned to staff.

- Furthermore all insurance must also cover the transport of Trust electronic data processing equipment. In particular portable computers that are regularly carried in cars, are not covered by the Trust's

insurance. Staff must check that their motor insurance covers such equipment under the business uses section and it is noted that an excess may be payable. If the vehicle is a Trust provided lease car, the Trust will cover the insurance excess whilst computers are in vehicles. However, it is the responsibility of the staff using the equipment to ensure that computer equipment is not left visible in unattended vehicles.

Staff who choose to drive vehicles which do not have a secure area, such as short wheel base four wheel drive cars should consult the Information Technology department proper to making an application, as often insurance companies will only provide cover if the equipment is carried in a secure container in the vehicle and is not visible within the vehicle.

5.9 Termination of Employment

On ending employment with the Trust, in liaison with your line manager, all equipment, software and data must be returned to the IT Department where it will be logged back in and your signature obtained.

5.10 Misuse

Any unauthorised removal of IT equipment from the premises may result in the user having their access rights removed, and may also lead to disciplinary action being taken.

Any unauthorised removal of personal identifiable data from the premises may lead to disciplinary action being taken against the individual.

5.11 Remote Connection to Trust Networks

- No equipment is to be remotely connected to the Trusts network without prior consultation with, and the approval of, the Trusts Associate Director of Health Informatics.

- Policy and procedures for remote access to the Trusts network is detailed within the Access Control Policy and dial-in procedures, please refer to these documents for further guidance.

- The NHSnet code of connection prohibits unauthorised users from accessing NHSnet. Where Trust owned computers are being used at home or away from Trust sites, then it must be ensured that family members/friends etc. do not access NHSnet or the Trusts network.

Ref: Dial in agreement form – Internal and external

5.12 Access to and use of Authorised information

You must not use a Trust portable computer to access or attempt to access any systems or networks that you are not authorized to use.

You must not connect any Trust supplied portable computer devices to any phone line or internet connection or other computer unless you have been approved to use remote access or home working procedures.

Ref: IT Home working Policy

5.13 Password Security

Password security is the responsibility of the individual, passwords should be formulated in such a way that they are easily remembered but difficult to guess and should be formulated using letters (upper and lower case), figures and other characters.

Passwords must not be displayed on screen as they are entered.

When allocated a new/temporary password for start-up purposes by the system administrator / manager the user must immediately change it.

- Passwords must consist of a minimum of 8 characters.
- Passwords must be changed on change of staff or staff resignation.
- Passwords must not be shared amongst users.
- Passwords must not be written down.
- Passwords should not relate to the system or the user, although passwords must be easy to remember.
- Password must be changed regularly, at intervals not exceeding 90 days.

Where sensitive data is to be kept on hard discs the use of encryption software or hardware package should be considered to provide protection to the data if the machine is lost or stolen.

Reference: Access Control Policy, RA Policy, IT Security Policy.

If you have any questions about this policy please contact the Information Governance Department via email to cdda-tr.informationgovernance@nhs.net

6 Dissemination Arrangements

All staff need to comply with this policy see scope.
This policy will be uploaded onto the trust staffnet (intranet) central Policy library.

7 Monitoring

7.1 Key performance Indicators

- To ensure the Trust complies with information rights law and practice, incident monitoring at the IG Steering group will review this on a quarterly basis.
- To adhere to the DoH codes of practice, monitoring at the IG Steering group will review this on a quarterly basis.
- To comply with the law in the related areas, monitoring at the IG Steering group will review this on a quarterly basis.

7.2 Compliance and Effectiveness Monitoring

Monitoring Criterion	Response
Who will perform the monitoring?	The Corporate Records Compliance Team
What are you monitoring?	1. Compliance with the Policy for Procedural Governance Documents as follows: a) Style, format and template. b) Explanation of terms used. c) Consultation process. d) Review/approval arrangements/process. e) Associated documents. f) Supporting references. 2. Compliance with the Policy for Procedural Governance Documents as follows: a) Ratification process; and b) Review arrangements.
When will the monitoring be performed?	1. Quarterly StaffNet Policies and Procedures site audit and report. 2. Quarterly advance warning report.
How are you going to monitor?	1. Analyse the export report from StaffNet Policies and Procedures site. 2. Monitoring of Register and StaffNet with regards to completeness and timeframes.
What will happen if any shortfalls are identified?	Any shortfalls identified will be reported to the appropriate Document Owner and Ratification Committee.
Where will the results of the monitoring be reported?	Monitoring reports will be provided as follows: 1. and 2. Quarterly monitoring report to the appropriate Ratification Committee and relevant Lead Directors / Associate Directors.
How will the resulting action plan be progressed and monitored?	Action Plans will be developed and progressed by the Trust Secretary and monitored by the relevant Ratification Committee.
How will learning take place?	Supplementary guidance will be issued in the form of Staff Bulletins via StaffNet, the Trust's intranet. If required, the Trust Secretary will provide support/training to Document Owners.

8 References

- Data Protection Act (1998)
- Freedom of Information Act (2000)
- Human Rights Act (1998)

9 Associated Documentation

This Policy refers to the following CDDFT trust policies and procedures:

- Email and code of practice Policy
- Internet Acceptable Use Policy
- Network Security Policy
- Registration Authority Policy

- Information Risk Management Policy
- Transfer of Personal Identifiable Information Policy
- Data Protection Act 1998 and Disclosure Policy
- IT Security Policy
- Clinical Confidential Information Policy
- Information Governance Policy
- IT Security Incident Management Policy

This Policy refers to the following guidance, including national and international standards:

DH: What you should know about Information Governance: DH 2008

NHS England: Everyone counts: Planning for Patients 2013/14

Information: to share or not to share: Caldicott 2

Information Governance Framework 2015/16

- Caldicott Principles
- BS7799 ; ISO27001 IT Security Management Standards
- ISO ISO31000/2009 – Information Risk Management Standards
- ISO 25999 - Business Continuity Standards
- BSI10012:2009 Data Protection Standard
- BS 17799 / ISO 27001 – 2005 IT Security Management Standards
- ISO ISO31000/2009 – Information Risk Management Standards
- ISO 25999 - Business Continuity Standards
- Guide to Confidentiality in Health & Social Care (2013).
- Department of Health Code of Practice – Records Management
- Department of Health Code of Practice – Information Security

10 Appendices

Appendix A – Transport and Storage of Trust owned IT devices and data – Do's and Don'ts
Appendix B –Definitions
Appendix C- Dissemination Plan
Appendix D - Equality Analysis / Impact Assessment

Appendix A – Transport and Storage of Trust Owned IT devices and data – Do's and Don't

No equipment or personal identifiable data may be removed from the premises without authorisation from your line manager.

When removing equipment and personal identifiable data from Trust premises, you are responsible for ensuring its safe transport and storage as far as it's reasonably practicable. The equipment is not insured and you may be held liable if you do not take reasonable precautions.

You must take precautions to minimise the risk from theft or damage. IT equipment and data must be transported in a secure environment. See appendix 1.
During the transfer between work and non-Trust premises, you must keep the equipment and data out of sight, and they must not be left unattended at any time.
IT equipment and data must not be left in your car overnight.
Manufacturers' instructions for protecting equipment must be observed at all times e.g. protection against exposure to strong magnetic fields.

Reasonable steps must be taken to minimise the visibility of the equipment and data from outside the premises, and to secure doors and windows when the home is unoccupied.

IT equipment and all confidential documents, when used away from an office location, must be stored in the most secure area available when not in use, to protect from unauthorised access/disclosure or theft, for example:

- Locked in a cupboard
- Locked in a filing cabinet
- Locked in a desk draw

Equipment that has been removed from site must have appropriate access control mechanisms in place. This may include:

- Access passwords
- Modification passwords
- Data encryption

When returning the equipment to the Trust or the information held is no longer needed, the information must be removed. It is the responsibility of the Trust's IT department to ensure that data has been removed from equipment prior to re-use.

All mobile Media is to be afforded the same level of physical protection as the most sensitive material stored thereon.
Any loss or theft of any item of mobile Media must be reported immediately on an IR1 form and the IT Department must also be infromed so that the level of compromise can be assessed, and necessary efforts can be made for recovery.

Appendix B - Definitions

Portable Computer Devices	This includes Trust Supported laptops, notebooks, iPhone, tablet computers and PDAs (personal digital assistants).
Network Devices	includes routers, firewalls, switches and other network components which may contain configuration information or encryption keys relating to the CDDFT network
Removable Data Storage Media	This includes any physical item that can be used to store and/or move information and requires another device to access it. For example, CD, DVD, digital storage device (flash memory cards, USB disc keys, portable hard drives). Essentially, anything you can copy, save and/or write data to which can then be taken away and restored on another computer.
Trust "Supported"	This includes portable computer devices and removable data storage media such as USB disc keys purchased or authorized by CDDFT NHS Trust. It does not include any devices brought into the Trust from a previous NHS organization (or other) and anything brought in without prior authorization by IT Services.
Confidential Data	Several classes of data may be designated as "Confidential Data" and therefore require encryption. From the perspective of this policy "Confidential Data" are any data that, if lost, could cause harm. Confidential Data includes (but is not limited to) the following: Personal data (DPA term defined in section 11.2 below), Sensitive Personal Data (DPA term defined in section 11 below), Contract information, Staff Information, Trust projects; and Business information. At the time of drafting, data loss cases are attracting substantial media interest. Organisations who have experienced major data losses have suffered significant damage to their reputation and can be fined up to £500,000
Personal Data	Personal Data is considered to be Confidential Data under this policy. Personal Data is defined by the Data Protection Act as data relating to a living individual who can be identified: (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller (definition in 11.4 below), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. For clarity the following must always be encrypted: All documents holding data where distress might result from the misuse or disclosure of that data, including data on major talent salaries, Sensitive Personal Data (see 11.3 definition below) and information that could be used in identity fraud attempts; All Children's contact details. This includes any data where children could be identified from the information (including

	personal addresses, email addresses, telephone numbers, gaming aliases, school names, names of sports teams and specific contact details); and Documents including individuals' financial information. (E.g. Bank or credit card details.)
Sensitive Personal Data	Sensitive Personal Data is specifically defined by the Data Protection Act and means personal data consisting of information as to: the racial or ethnic origin of the data subject (definition in 11.5 below), their political opinions, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992), their physical or mental health or condition, their sexual life, the commission or alleged commission by the data subject of any offence, or any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive Personal Data must always be encrypted. To ensure secure working practices all Trust owned devices should be encrypted where possible.
Data Controller	Data controller refers to the person who determines the purposes for which any personal data is to be collected and processed. In the context of the Trust this would normally be the owner of the process that collects and uses the relevant personal data.
Data Subject	Data subject means an individual who is the subject of personal data.

Appendix C - Dissemination Plan

(To be completed and attached to Policy and Guidance documents when submitted to the Committee approving this document)

Policy or Guidance (P&G) Title: Mobile Devices Policy			
Date finalized November 2015		**Dissemination Lead** (contact details) Head of Information Governance DMH x 43085	
Previous P&G already being used?	Yes	**If yes, what in what format and where? Trust Intranet IG Site**	
Proposed action to retrieve expired copies of P&G: This combines the trust mobile equipment policy into one policy. Old copied removed from staffnet.			
To be disseminated to	**How will be disseminated, who will do and when?**	**Paper or electronic**	**Comments**
Full Trust	Policy and procedure Intranet Site	E	

Dissemination Record – to be used once Policy or Guideline Approved

Date uploaded onto the Trust's Intranet 30/11/15

Disseminated To (either directly or via meetings, etc)	**Format (i.e. paper or electronic)**	**Date disseminated**	**No of copies sent**	**Contact Details / Comments**
IGSG via e-approval	E	Nov 2015	Full attendees	
General comments:				

Appendix D - Equality Analysis / Impact Assessment

Assessment Form **v3/2013**

Division/Department:	Commercial Services / Health Informatics
Title of policy, procedure, decision, project, function or service:	Mobile Devices Policy
Lead person responsible:	Head of Information Governance
People involved with completing this:	Information Governance;

Type of policy, procedure, decision, project, function or service:

Existing	☐
New/proposed	☑
Changed	☐

Date Completed: 10/09/15

Step 1 – Scoping your analysis

What is the aim of your policy, procedure, project, decision, function or service and how does it relate to equality?

To ensure Trust is compliant with legislation and staff abide by the Policy.

Who is the policy, procedure, project, decision, function or service going to benefit and how?

Full Trust staff;

What barriers are there to achieving these outcomes?

None

How will you put your policy, procedure, project, decision, function or service into practice?

Full distribution Trust wide; held on staffnet policy central register

Does this policy link, align or conflict with any other policy, procedure, project, decision, function or service?

No

Step 2 – Collecting your information

What existing information / data do you have?

Follows the current policy in the trust

Who have you consulted with?

IG Steering Group

What are the gaps and how do you plan to collect what is missing?

None

Step 3 – What is the impact?

Using the information from Step 2 explain if there is an impact or potential for impact on staff or people in the community with characteristics protected under the Equality Act 2010?

Ethnicity or Race

None

Sex/Gender

None

Age

None

Disability

None

Religion or Belief

None

Sexual Orientation

None

Marriage and Civil Partnership (applies to workforce issues only)

None

Pregnancy and Maternity

None

Gender Reassignment

None

Other socially excluded groups or communities e.g. rural community, socially excluded, carers, areas of deprivation, low literacy skills etc.

None

Step 4 – What are the differences?

Are any groups affected in a different way to others as a result of the policy, procedure, project, decision, function or service?

No

Does your policy, procedure, project, decision, function or service discriminate against anyone with characteristics protected under the Equality Act 2010?

Yes ☐ **No** ☑

If yes, explain the justification for this. If it cannot be justified, how are you going to change it to remove or mitigate the affect?

Step 5 – Make a decision based on steps 2 - 4

If you are in a position to introduce the policy, procedure, project, decision, function or service? Clearly show how this has been decided.

Review – IG Steering group; Approval PAW and loaded to staffnet with a Trust bulletin stating new reviewed policies available.

If you are in a position to introduce the policy, procedure, project, decision, function or service, but still have information to collect, changes to make or actions to complete to ensure all people affected have been covered please list:

How are you going to monitor this policy, procedure, project or service, how often and who will be responsible?

IG have continual assessments quarterly in place for all their policies and procedures.

Step 6 – Completion and central collation

Once completed this Equality Analysis form must be forwarded to Jillian Wilkins, Equality and Diversity Lead. jillian.wilkins@cddft.nhs.uk and must be attached to any documentation to which it relates.