CONTROLLED DOCUMENT

Mobile Devices Procedure

CATEGORY:	Procedure
CLASSIFICATION:	Governance
PURPOSE	To ensure staff using mobile devices outside Trust premises do so safely and securely.
Controlled Document Number:	1043
Version Number:	001
Controlled Document Sponsor:	Executive Medical Director
Controlled Document Lead:	Lead Security and Test Manager
Approved By:	Executive Medical Director
On:	May 2017
Review Date:	May 2020
Distribution: • **Essential Reading for:** • **Information for:**	 Information Asset Owners, IT Services, Staff with Mobile Devices All Staff

Contents

1. Purpose

1.1. This procedure sets out the processes to be followed to ensure that the use of mobile devices outside University Hospital's Birmingham NHS Foundation Trust (the 'Trust') Trust premises is undertaken safely and securely and in accordance with the Trust's IT Acceptable Use Policy.

1.2. This procedure aims to ensure users operate devices securely, preventing theft and risk to themselves, and ensuring the protection of the information contained on the device. While the device remains the property of the Trust at all times, the user is wholly responsible for the security and care of the device, regardless of where it is used.

1.3. This procedure provides guidance on what mobile devices are provided by the Trust and how they will be configured, requested, distributed and used.

1.4. This Procedure may be amended from time to time with the authority of the Executive Medical Director.

1.5. The terms used in this Procedure have the meaning given to them in the Policy.

2. Scope

This procedure applies to all areas and activities of the Trust and to all individuals employed by the Trust including contractors, volunteers, students, locum and agency staff and staff employed on honorary contracts.

3. Definitions

Asset Register of Mobile Devices	A register of all Trust-Approved Mobile Devices containing specified information.
Confidential Information	Any information or combination of information that contains details about an organisation or an individual person that was provided in an expectation of confidence. This includes for example, non-personal corporate or technical information that is commercially sensitive, drafts of documents that are not ready for publication, restricted information & documents, etc. as well as personal data about patients, service users and staff.
Mobile Device	For the purpose of this Procedure, a Mobile Device is any device provided by the Trust which directly accesses the Trust network. This excludes mobile devices which access the Trust network via a secure VPN connection. This most commonly includes, but is not limited to, Smartphones, tablets and laptops.

Remote Working	This describes how staff work away from Trust premises via a connection to the Trust network which is remotely accessed.
SIRO	Senior Information Risk Owner – The Director of Corporate Affairs
Unique Identifier	This is the unique number which identifies a device, such as an IMEI number for Smartphones or tablets and a serial number for laptops.
VPN	Virtual Private Network

4. Process

4.1. Permitted use of Mobile Devices

4.1.1. Only Trust-approved Mobile Devices may be used by staff to directly access the network off-site. The use of VPN to access the network is covered by the Remote Working Procedure. If the Trust makes a decision in the future to implement a "bring your own device" (BYOD) procedure for staff, this Procedure and any other related policies and procedures will be updated to include non-Trust owned devices for staff.

4.1.2. No other Mobile Devices may be provided without the express permission of the Caldicott Guardian or SIRO.

4.2. Procurement of Mobile Devices

All procurement of Mobile Devices must be undertaken by IT Services in accordance with the Trust Procurement Policy.

4.3. Secure Configuration of Mobile Devices

4.3.1. IT Services must appropriately secure the Mobile Device prior to giving it to the member of staff. The security configurations will allow for the Mobile Devices to be remotely wiped or geolocated. This process will be documented in an internal IT Services work instruction.

4.3.2. The Mobiles Devices must be configured to ensure that users cannot make any unauthorised changes.

4.3.3. IT Services must configure all Mobile Devices to prevent users writing to optical drives or unencrypted USB sticks.

4.3.4. IT Services will configure Mobile Devices to an encryption level stipulated by the Department of Health.

4.4. Requesting and Authorising Mobile Devices

4.4.1. Mobile Devices must be obtained from IT Services by making a request via LANDesk. IT Services must not issue Mobile Devices to any member of staff without the approval of the relevant budget holder.

4.4.2. IT Services must maintain an Asset Register of Mobile Devices to include the following information as a minimum:

- The unique identifier of the device, such as IMEI number or serial number;
- name of the member of staff to whom it is issued;
- name of relevant budget holder who approved the issue;
- name of staff member's department;
- date of issue;
- name of issuing IT Services staff member; and
- date the Mobile Device Terms & Conditions was signed.

4.4.3. It is the relevant budget holder's responsibility to:

- check that the member of staff is requesting the Mobile Device for a genuine business need and that it is for a purpose allowed under the Trust's Data Protection and Confidentiality Policy and this Procedure;
- ensure that the member of staff is aware of their responsibility to only use the Mobile Device as allowed under the Trust's Data Protection and Confidentiality Policy and this Procedure;
- inform IT Services if the staff member no longer requires the device so that the register and other logs can be amended and arrangements made for the return or redeployment of the device; and
- ensure that staff report any losses of Mobile Devices to IT Services and onto Datix.

4.5. Distributing Mobile Devices

4.5.1. IT Services must not provide a staff member with a Mobile Device unless the staff member has signed the Terms & Conditions at Appendix A. Signature of the Terms & Conditions is confirmation that the staff member will abide by the contents of the document and this Procedure.

4.5.2. The signed Terms & Conditions must be attached to the LANDesk support call. IT Security Services will conduct audits at least quarterly to check that those on the register detailed in 4.4.2. have signed Terms & Conditions which are attached to the LANDesk support call.

4.5.3. IT Services must keep the Asset Register of Mobile Devices up to date.

4.5.4. Where appropriate, IT Services must register the unique identifier with a designated list.

4.5.5. IT Services must explain to staff that some Mobile devices have software which enables the device to be geolocated and that this will only be done in accordance with the process described in 4.8 below.

4.6. Appropriate use of Mobile Devices

4.6.1. Staff must use the Mobile Device in accordance with the Trust's Mobile Devices Procedure, Access Control Procedure, IT Acceptable Use Policy, Data Protection & Confidentiality Policy and any other associated policies or procedures. Line managers and IT Services must report any serious non-compliance to the Trust Human Resources department.

4.6.2. Staff must ensure that Mobile Devices are not left unsecured and are protected from theft; particularly from cars or other easily accessible areas

4.6.3. Staff must ensure that unauthorised people are not able to access the Mobile Device.

4.6.4. Staff must not share the passwords to Mobile Devices with third-parties. Staff must comply with the password requirements stipulated in the Access Control Procedure.

4.6.5. Staff must not make excessive personal use of the Mobile Device and if any additional charges are to be incurred as a result of their personal use of the Mobile Device they must

inform their line manager and IT Services. IT Services or the line manager cannot seek reimbursement for the additional charges without the approval of the SIRO.

4.6.6. Staff must ensure that they use the device in accordance with the Road Traffic Act 1988 and any other relevant legislation.

4.6.7. Staff must not transfer confidential data from the Mobile Device to any personal devices.

4.6.8. Staff must ensure they install any Mobile Device security updates that are made available.

4.6.9. Data must not be stored locally on the Mobile Device and staff must be aware that no back up of individual Mobile Devices is made by IT Services.

4.6.10. Staff must pass mobile devices to IT Services for secure disposal.

4.7. Reporting the Loss or Theft of Mobile Devices

4.7.1. Staff must immediately report any lost or stolen mobile devices to IT Services. The Service Desk is available 24 hours a day, 7 days each week.

4.7.2. Staff must then report the loss or theft via the Trust's online incident reporting system.

4.7.3. IT Services Security will conduct an audit at least quarterly to ensure that staff have reported loss or theft of mobile devices on Datix after the initial report to IT Services. This audit report will be presented to the Information Governance Group. IT Services Security will inform the line managers of staff who have not complied with 4.7.2. of this Procedure.

4.7.4. IT Services Security will liaise with the Trust Security Management Specialist and the SIRO to decide if any incidents will be reported to the police.

4.8. Securing Lost or Stolen Mobile Devices Process

4.8.1. *BlackBerry Phones or Tablets*

The process is detailed in internal IT Work Instructions.

4.8.2. *Laptops*

The process is detailed within internal IT Work Instructions.

4.9. Monitoring use of Mobile Devices

4.9.1. If a staff member no longer requires a Mobile Device as part of their job role, the staff member must inform their line manager and IT Services. IT Services will liaise with the line manager to decide if the device may be returned to IT Services for reallocation within the same or another department.

4.9.2. IT Services must generate appropriate usage reports for line managers who will then be responsible for addressing lack of use with their members of staff. Any exceptions must be reported to the Information Security Access Group

4.9.3. It is the line mangers responsibility to ensure all allocated devices are returned to the Trust when an employee leaves the Trust or moves to another role.

5. References

Access to Health Records Act 1990

Caldicott Principles (Revised, to include 7th principle, 2013)

Commission Common Law Duty of Confidentiality

Computer Misuse Act 1990

Confidentiality NHS Code of Practice 2003

Data Protection Act 1998

Freedom of Information Act 2000

Information Security Management: NHS Code of Practice – DoH 2007

N3 Code of Connection

NHS Code for Records Management 2016

Processing of Sensitive Personal Data Order 2000

Regulation of Investigatory Powers Act 2000

6. Associated policy and procedural documentation

Assessment of Risks and Management of Risk Registers Procedure

Data Protection and Confidentiality Policy

Freedom of Information Act and Environmental Information Regulations Procedure

IT Acceptable Use Policy

Information Asset Guidance

Information Security and Access Control Policy

Privacy Impact Assessment Procedure

Record Management and Information Lifecycle Policy

Reporting and Management of Incidents, Including Serious Incidents, Requiring Investigation Policy & Procedure

Risk Management Strategy and Policy

Appendix A – Terms & Condition for the use of Trust-approved Mobile Devices

University Hospitals Birmingham NHS Foundation Trust ('The Trust') approves Mobile Devices for staff whose job performance requires or would be enhanced by their use. Mobile devices and their service agreements are provided for official Trust business use and are made available to staff in positions where the associated benefits justify the additional operating costs.

I, …… agree that:

I will use the Mobile Device in accordance with the Trust's Mobile Devices Procedure, Access Control Procedure, IT Acceptable Use Policy, Data Protection & Confidentiality Policy and any other associated policies or procedures. I understand that failure to comply with these may result in revocation of the Mobile Device and possible disciplinary action.

I will only use passwords for access to the Mobile Device in accordance with the password requirements stipulated in the Access Control Procedure.

I will ensure that the device is kept secure to protect against loss or theft.

I will use the Mobile Device in a vehicle only in accordance with the Road Traffic Act 1988 and other relevant legislation.

I will not make excessive personal use of the Mobile Device. If any additional charges are to be incurred as a result of my personal use of the Mobile Device, I understand that the Trust reserves the right to seek reimbursement from me.

IT Services have explained to me that the Mobile Device may contain software which is able to locate the device if it is reported lost or stolen, only if the correct process in the Mobile Device Procedure is followed.

If the device is lost or stolen I will immediately inform IT Services to allow the appropriate security actions to be undertaken. I will also report any loss or theft on the Trust's online incident reporting system.

I agree that if I lose more than one Mobile Device, I may be held responsible for paying for the cost of a replacement device.

If I no longer require the use of the device in my role, or if I leave the Trust, I will inform IT Services and my line manager and return the Mobile Device to IT Services so that the security registers can be amended appropriately.

I will install updates on the device as requested by IT Services.

Name	
Job Title	
Date	
Signature	