University Hospitals of Leicester NHS
NHS Trust

MOBILE DEVICE MANAGEMENT POLICY

(formerly The Security of Information Processing Equipment Policy)

Approved By:	Policy and Guideline Committee
Date Originally Approved:	13th February 2007
Trust Reference:	**B7/2007**
Version:	3
Supersedes:	2 – October 2008 (formerly the Security of Information Processing Equipment Policy)
Author / Originator(s):	Saiful Choudhury - Head of Privacy
Name of Responsible Committee/Individual:	Andrew Carruthers – Chief Information Officer & Senior Information Risk Owner
Latest Review:	20 November 2020 – Policy and Guideline Committee
Next Review Date:	June 2024

NB: Paper copies of this document may not be most recent version. The definitive version is held in the policy and guideline library on INsite

CONTENTS

Section		Page
1	Introduction	3
2	Policy Scope	3
3	Definitions	4
4	Roles and Responsibilities	5
5	Policy Statements	8
6	Education and Training Requirements	10
7	Process for Monitoring Compliance	11
8	Equality Impact Assessment	12
9	Supporting References, Evidence Base and Related Policies	12

Appendices		Page
1	Trust Mobile Terms and Conditions	13

REVIEW DATES AND DETAILS OF CHANGES MADE DURING THE REVIEW

This is a re-written policy developed to support the use mobile equipment and Bring Your Own Devices. Changes have been made to updated reference to external documents, up to date security requirements, and the inclusion of Bring Your Own Device.

4.3 – Minor adjustments and formatting

KEY WORDS

Information governance, confidentiality, security, mobile, device, encryption

SUMMARY

This document provides a policy statement on the use and management of information in the Trust and describes the arrangements for providing assurance to the Trust Board that IG compliance standards are defined and met and IG incidents appropriately managed.

NB: Paper copies of this document may not be most recent version. The definitive version is held in the policy and guideline library on INsite

1 INTRODUCTION

1.1 The Trust recognises mobile phones and Web/Internet enabled devices as an effective form of communication for clinical and operational emergencies and accepts they are a part of everyday life and essential to maintain communication with friends, family and loved ones. However, in a Hospital setting they can be a nuisance to other patients and visitors and pose a risk to privacy and dignity. They can also in certain circumstances have an impact on electronic medical equipment. The Trust recognises that the usage of these devices needs to be balanced against this policy.

1.2 This policy has been developed to ensure that all staff, patients, service users, volunteers, contractors and visitors are aware of the need to use mobile communication devices responsibly, in designated areas where their usage will not inconvenience or infringe upon the rights of others in accordance with Article 8 of the Human Rights Act 1998.

1.3 The policy aims to promote and protect patient confidentiality, safeguarding and privacy and dignity

1.4 The Policy also defines staff use of trust issued and bring your own (BYOD) devices.

1.5 The Policy has been approved by the Steering group as well as going through a task and finish group which covered non IM&T colleagues by default.

2 POLICY SCOPE

2.1 This policy covers all forms of mobile devices portable communication media held within the Trust, including (but not limited to):

- Trust Issued Devices (including Mobiles and Laptops)
- Personal Mobile Device
- Bring your Own Device (BYOD)

2.2 This policy applies to all Trust employees and third parties responsible for the delivery of contracted NHS services on behalf of the organisation.

2.3 Staff wishing to use their own devices and their mobile data are permitted to according to the guidelines within this policy:

- Staff will only be allowed access to the Trusts WiFi network;
- Staff will NOT save/store confidential or personal confidential data (PCD) on their own devices.

NB: Paper copies of this document may not be most recent version. The definitive version is held in the policy and guideline library on INsite

2.4 The policy should also be used in conjunction with B32/2005 Social Photography Policy and Policy For The Control of Access to Electronic Systems, B25/2007'

3 DEFINITIONS

3.1 "**Bring your own device" (BYOD**) refers to the use of personal mobile devices to access UHL administrative and clinical applications through the secure trust wifi network internally or over their mobile internet if externally accessing. Further guidance can be obtained from the Head of Privacy on 0116 2586053

3.2 **Caldicott Guardian;** The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner. The UHL Caldicott Guardian is the Medical Director

3.3 **Data Security and Protections Toolkit (DS&PT);** The toolkit is supported by both NHS Digital (NHSD) and NHS England and is a self-assessment tool for Trusts which incorporates a knowledge base and guidance on all aspects of IG. The DS&PT is updated annually to reflect new NHS guidance, legislation and NHS Codes of Practice. The Trust must also show compliance and adherence to the Toolkit

3.4 **Information Governance (IG);** IG is the organisational practice of managing information from its creation to final disposal in compliance with all relevant information rights legislation. IG is focused on ensuring that standards and services are introduced to ensure that Trust information is managed securely, compliant with legislation and available for access by both staff and external parties, including the public and regulators.

3.5 **Information Governance Steering Group;** The Information Governance Steering Group is a standing committee accountable to the Board. Its purpose is to support and drive the broader information governance agenda and provide the Board with the assurance that effective information governance best practice mechanisms are in place within the organisation

3.6 **Mobile device;** is defined as any device that may synchronise with another computer, and may be any of the following items:

- Laptop and notebook computers
- iPads/Tablets
- Smartphones including iPhones and other system that may fall into this category
- Webcams
- USB Memory sticks
- MP3 players

Any other device that may be utilised to record/store or transport data/information (but not limited to) audio, video (including video conferencing) and still images.

The above list is not exhaustive. Any mobile device used in connection with Trust related work must be encrypted and this can be done via placing a call to service desk on x8000. **Any personal devices will not be encrypted please refer to 5**

3.7 **Video conferencing-** allows users in different locations to hold face to face meetings online without having to move to a single location.

3.8 **Virtual Private Network (VPN)** allows users to connect to the trust network and resources securely over the public network via trust devices (internet)

3.9 **Virtual Desktop Info structure (VDI)** allows users to connect to the trust network and resources securely over public network via personal devices (internet)

4 ROLES AND RESPONSIBILITIES

4.1 **Chief Information Officer- Senior Information Risk Officer (SIRO):** The trust Senior Information Risk Owner (SIRO) is the Executive Director Lead for this policy. The SIRO is accountable and responsible for overall application of mobile devices across the organisation. The key responsibilities of the SIRO for this policy are:

- To review the implementation of this policy.
- To overall assess the risk assessment process for information governance, including review of the annual information risk assessment and the applicability of the assertions within to support and inform the Annual Governance Statement and compliance submissions including IG & DS&P Toolkits related to portable devices.
- To determine actions for breaches of this policy with Head of Privacy,

4.2 **Medical Director – Caldicott Guardian:** The Caldicott Guardian's main responsibility is to be responsible for protecting the confidentiality of service user information and enabling lawful and ethical information sharing. This links directly to SIRO and will require the Head of Privacy to liaise directly to discuss information sharing issues in the context of this policy. The additional responsibilities of the Caldicott Guardian are;

- Ensuring that mobile data processes satisfy the highest practical standards for handling patient information in line with Caldicott Principles for information sharing;
- Advising on policy issues to update standards with regard to patient data within mobile devices

- Advocating policy requirements at board level to protect patient interests.

4.3 **Executive Information Management and Technology Board**: The EIMT Board is responsible on behalf of the Chief Executive for all matters relating to this policy including;

- developing, implementing and maintaining a IG strategy and associated standards, an implementation strategy including an annual work programme to provide assurance to the Trust that effective arrangements are in place;
- reporting to the SIRO on annual basis to clarify performance and risks issues identified during audit and training cycles for executive level consideration.

4.4 **Information Management and Technology Security Board:** The IMTS Board is responsible on behalf of the EIMT Board for all matters relating to this policy including;

- Identify funding from budget to finance mobile devices for members of staff where required.
- To determine staff have a legitimate business need for a Trust issued device or BYOD connection as well as ensuring that the mobile device is being used as a business tool.

4.5 **Head of Privacy- Data Protection Officer:** The Trust's Head of Privacy has responsibility for managing the overall co-ordination, publicising and monitoring of the Trust IG Framework.

The Trust's IG Lead Head of Privacy has specific responsibility for;

- The development of the IG strategy and procedure and guidance related to this policy
- Leading training and audit strategies to raise IG standards and services within this policy
- To complete the relevant sections in the IG DS&P toolkit in relation to this policy on the central returns on behalf of the Trust.
- Ensuring compliance with Legal requirements

4.6 **Employees & staff working on behalf of the Trust:** All Trust employees, whether permanent, temporary or contracted, and students and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis. This policy requires all staff to understand the need;

- To comply with all policy standards
- To report any breaches of Mobile Device Management to a line manager.
- Report any incidents such as inappropriate use or security breaches to their line manager

- Action will be taken as a result of non-compliance with this policy in line with the Trust disciplinary procedure.
- All employees are required to undertake annual Trust mandatory training in IG to ensure that they are fully aware of their individual responsibilities and have the relevant knowledge to ensure compliance. Misuse of or a failure to properly safeguard information will be regarded as a disciplinary offence.

UHL approved video conferencing solution is Microsoft Teams any other video conferencing solution should have appropriate safeguards where the following guidance is followed:

- Must be in secure password protected rooms
- Notify all members at the start of meeting if the meeting is being recorded
- To be vigilant for any unintended party entering the room. If this person is not identifiable this should be reported to IM&T and Datix as an incident.

4.7 Patient Confidentiality, Privacy and Dignity (All devices)

Prohibiting the use of mobile communication devices with cameras in certain areas of hospitals such as private areas (for example, bathrooms, toilets, secluded areas) may not sufficiently ensure medical confidentiality or indeed protect each patient's right to respect for their private life. Therefore, in order to protect fully these rights, use of cameras, mobile communication devices with cameras/recording capability are not permitted in patient wards unless authorisation is given by the Ward Manager, or those in delegated responsibility from them.

Managers of the area e.g. wards, patient areas must stipulate and clearly designate the areas where mobile communication devices can be used. See 'Policy For The Control of Access to Electronic Systems, B25/2007'.

In cases of Safeguarding, The Mental Health Act and deceased patients policies for consent/authorisation staff are to follow the individual policies for this when in private areas.

In the wards, privacy curtains must be used in order to ensure the patients privacy and dignity is maintained.

Staff are permitted to us mobile devices in ward areas provided it is for patient care only staff should be vigilant for members of the public using mobile devices in patient ward areas where they are seen to be taking pictures or videos of other patients due to a risk of posting on social media. See the B32/2005 Social Photography Policy

4.8 Appropriate Use of Mobile Phones and Web/Internet enabled Devices (All devices)

With the exception of certain circumstances which are detailed within this section the Trust has decided that the use of mobile communication devices must be

restricted and where users have their own device, should be requested to use the Trust iPhone devices if available. This is to protect and preserve the privacy and dignity and safeguarding issues of all persons including patients, service users, staff and visitors.

Staff should be aware that many devices contain cameras and that images can be uploaded to a range of social media sites, e-mailed or sent as a text attachment directly either immediately or at a later date.

Staff, Patients, service users, volunteers, contractors, and visitors are asked to check when using a mobile device in an authorised area as indicated by signage.

Staff should have due regard for the privacy and dignity and safeguarding issues of all persons and should ensure personal mobile communication devices are not used in clinical or ward areas where they may disturb others. Devices left in staffroom lockers should be turned off or set to silent to avoid disturbance.

5 POLICY STATEMENTS

5.1 Bring your Own Device (BYOD)

Mobile devices will be provided to those staff whose duties require them to be contactable/on-line when away from their normal place of work.

Sometimes a duty will be covered by issuing a shared mobile device.
In all cases approval to issue a device must be given by the Line Manager.
Examples of need are (note: this list is not exhaustive):

- Duties require working across multiple sites
- There is a genuine need to be easily and immediately contactable during and outside of normal working hours and the user may not have access to a Trust phone.
- Staff who work in several locations within the hospital
- Staff contractually required to be on call

This policy applies to all members of staff of this Trust wishing to apply for a mobile device for business use or to transfer an existing mobile device from another organisation.

Staff to follow the following guidelines if they are in receipt of a BYOD:

- To sign for receipt of a Trust mobile device (where applicable), in the case of “Bring your own device” (BYOD), to acknowledge that they have read, understood and will comply with the requirements of this policy (Appendix A)
- Ensure staff have a legitimate business need for a Trust issued device or BYOD connection as well as ensuring that the mobile device is being used as a business tool.
- To take good care of the mobile device and take all reasonable precautions to ensure that the device is not damaged, lost or stolen. In the event that the

Trust issued device is stolen, staff will be expected to raise an Incident Report (Datix), report the theft to the police and obtain an incident number.

- If the Trust issued device, or a personal device connected to Trust systems is lost, staff must inform IT Helpdesk immediately by calling x8000 so it can be disabled and where possible wiped remotely. The device must be protected via a device case at all times to prevent damage as best as possible if dropped.
- Staff using a Trust issued mobile device or personal mobile device must ensure that the device has a sufficiently charged battery to last a working shift.
- Staff leaving the Trust must return their Trust provided mobile device to their line manager.
- Staff members leaving the Trust that have been connected to the BYOD service must inform the IT Helpdesk so that their device can be removed from the system.
- The IT Helpdesk will perform a system clean-up on BYOD devices not seen on the Network for a 3 month period. Any such devices will be removed from the system.

5.2 Trust issued devices

- Line Manager to always note the TAG reference numbers on the NHS sticker

- If there are any issues or if the device goes missing staff must report to line manager then report to IM&T.

- Take good care of the mobile device and take all reasonable precautions to ensure that the device is not damaged, lost or stolen. In the event that the Trust issued device is stolen, staff will be expected to raise an Incident Report (Datix), report the theft to the police and obtain an incident number.

- Staff leaving the Trust must return their Trust provided mobile device to their line manager.

5.3 Personal Mobile Device

- Where confidential information is approved for storage on a mobile device, only the minimum amount of personal information necessary for the specific business purpose must be used. Where possible it should be S number only.

- Information must not be stored permanently on mobile devices.

- If it is necessary to work away from the Trust, information should be retained on the Trust server and deleted from the mobile device as soon as possible.

- Information must be virus checked before transferring onto Trust computers. This will be done automatically for non-confidential information that is sent via email. (Confidential information may only be sent outside the Trust if it is encrypted using an approved method in line with the Trust e-mail policy).

- Only personal devices that have been authorised by IM&T and the respective line manager shall be authorised for use.

- All Personal devices authorised shall be configured and operated in accordance with and supporting data and information governance policies

- Personal devices used for work purposes should be converted to the BYOD Programme (see BYOD section in this policy)

5.4 Support and update

All devices are supported and managed centrally by IM&T who will regularly update and refresh the software. Any updates that will affect the day to day use of the device will be communicated to all users in advance.

5.5 Exemptions to the Policy

Having given consideration to the benefits offered by mobile communication the Trust believes there are some special circumstances where it is acceptable for such technology to be used within designated areas. These are considered to be:

- In a Wi-Fi enabled designated area for accessing clinical information systems
- Clinicians and managers who may need to be urgently contacted whilst in a patient area for work related issues.
- Where there is a clinical need that negates the use of all other means of communication – not accessible by landline or messaging via Clinical System where applicable.
- Where there is an urgent need for translation at the bedside of a patient and no advocate is available to attend. Please also refer to the translation and interpreting policy.
- Where staff are classed as Lone Workers in the community e.g. require contact with other clinical service whilst working in the community or people's homes
- On call maintenance and IT staff who require a mobile device for a specific work purpose.
- Major incident declared

Staff who meet the criteria for a temporary exemption to the policy are politely asked to show consideration to the points within this section of the policy to NHS colleagues, patients and visitors.

5.5 Compliance with this policy

The privacy and dignity of patients and compliance with health and safety is the duty of all staff, patients, service users, volunteers, contractors and visitors whilst on the Trust premises.

Patients, volunteers, contractors or visitors who fail to adhere with this policy will be asked to leave the prohibited use area. Any patient, service user or visitor failing to comply with this policy/local procedure may be requested to leave the premises.

Patients are asked to follow the following guidance when visiting or staying in hospital:

- Do not take anyone's photo without • permission, and you do not capture people (including staff) in the background of your photos, as this breaches privacy and can cause distress.

- Ensure people are not captured in the background of video calls • (only you should be seen on the screen).

- Limit disturbance to others when making calls/using your phone. • Consider the volume of any videos or calls.

- Do not use your mobile device around sensitive equipment. • Signs will make it clear that you shouldn't use your phone in that area. Switch it off or enable 'airplane mode' (leaving on silent or vibrate setting could still affect medical equipment).

The Trust does not accept the display of violence or aggression towards NHS staff whilst undertaking their work, any person so doing may find themselves subject to prosecution.

Where the Trust installs Wi-Fi Internet access systems for use by staff, patients, service users, volunteers, contractors or visitors these should be commissioned with due regard to the protections relating to privacy and dignity contained within this policy.

Staff members who use mobile communication devices improperly should have the requirements of this policy made explicit to them. Persistent failure to comply with the policy must be reported via the line manager and may be dealt with under the Trust's disciplinary procedures.

5.6 Inappropriate Images, Videos and Recordings taken

If there is reason to believe inappropriate images are taken, the person responsible will be asked to delete the inappropriate image/(s). Examples of inappropriate images could be:

1) Any patient who is exposed

2) A minor (under 18) without consent of parent.

Staff need to make senior staff member on duty aware of their belief that inappropriate and then under the direction of the senior staff member ask that the

NB: Paper copies of this document may not be most recent version. The definitive version is held in the policy and guideline library on INsite

mobile communication device is handed over to Trust staff and make it explicitly clear that this is being done because we have concerns for the privacy and dignity of others on the ward/clinical environment, also state that the person may have contravened Data Protection law and therefore have put themselves in a position where they may be prosecuted under this act.

5.7 Lost/found devices

If a device is lost or stolen, please contact the IM&T Help desk x8000 and complete a DATIX form immediately to prevent any risk of losing patient data. In addition, please inform the device owner (wards or clinics) as soon as possible, so they can arrange for a replacement.
If a device is found, please contact the IM&T Help desk x8000 (with the device ID) and hand it in to Security.

5.8 Damaged/faulty devices

If a device is not working, please contact the IM&T Help desk x8000 (with the device ID).

Damaged or broken devices should be reported to the IM&T Help Desk x8000 for repair or replacement if necessary.
All Trust provided mobile devices are supplied with an appropriate protective cover which must not be removed except for the purposes of cleaning.
Devices which are damaged will not be replaced if they do not have an appropriate protective case in situ

6 EDUCATION AND TRAINING REQUIREMENTS

6.1 The Trust is committed to the provision of IG training and education to ensure the workforce is informed, competent, prepared and possesses the necessary skills and knowledge to perform and respond appropriately to the demands of clinical care and service delivery. All UHL staff are required to complete the mandatory Cyber Security Level 1 train on the Trust's online training site https://uhlhelm.com/

6.2 The Trust has a mandatory training programme which includes maintaining awareness of IG, data protection, confidentiality and security issues for all staff. This is carried out by regular training sessions covering the following subjects:

- personal responsibilities;
- confidentiality of personal information;
- relevant IG Policies and Procedures;
- general good practice guidelines covering security and confidentiality;
- record management.

6.3 All staff will be required to complete annual IG training (including data protection and confidentiality training) commensurate with their duties and responsibilities. All new starters will be given IG training as part of the Trust mandatory induction

NB: Paper copies of this document may not be most recent version. The definitive version is held in the policy and guideline library on INsite

process. Additional training in these areas will be given to those who require it due to the nature of their job, for example for system administrators who required further data protection and information risk training. Please see Core Training Policy B21/2005

7 PROCESS FOR MONITORING COMPLIANCE

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements
IG Training	Head of Privacy	HELM, IG Training Tool and DATIX	Daily (departmental) & Monthly (IGSG)	Reports to the IG Steering Group and EIMT
IG/DS&P Toolkit	Head of Privacy	IG Toolkit online tool reportable to the board	Monthly	Reports to the IG Steering Group and EIMT
Computers and Public Areas Should be Risk Accessed	General Manager and ward managers	Appropriate risk management tool	Monthly	Reports to the IG Steering Group and EIMT

8 EQUALITY IMPACT ASSESSMENT

8.1 The Trust recognises the diversity of the local community it serves. Our aim therefore is to provide a safe environment free from discrimination and treat all individuals fairly with dignity and appropriately according to their needs.

8.2 As part of its development, this policy and its impact on equality have been reviewed and no detriment was identified.

9 SUPPORTING REFERENCES, EVIDENCE BASE AND RELATED POLICIES

9.1 The Senior Information Risk Owner (SIRO) will direct the IG Lead to take actions as necessary to comply with the legal and professional obligations set out in the key national guidance issued by appropriate commissioning bodies in particular;

- The General Data Protection Regulation 2016
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality; and
- The NHS Confidentiality Code of Practice.

9.2 There are a number of policies and procedures within the Trust that should be read in conjunction with this document for a complete understanding of how the Trust is organised and the strategies in place to fulfil its obligations. The key documents are listed below:

Freedom of Information Policy A9/2004

Policy for the Retention of Records B10/2004

E-mail and Internet Access and Monitoring Policy A9/2003

Policy for Documenting in Patients' Health Records B30/2006

Information Security Policy A10/2003

University Hospitals of Leicester NHS
NHS Trust

Mobile Device Terms & Conditions

NB: Paper copies of this document may not be most recent version. The definitive version is held in the policy and guideline library on INsite

Trust Issued Mobile Device and Bring Your Own Device (BYOD) Service Terms and Conditions

By using a Trust issued device ("Trust") or a device that you wish to use for Trust purposes ("BYOD"), you agree to the following terms and conditions of use:

• The IT Helpdesk and the Trust Network team will provide technical assistance to staff with issues with issued mobile devices or mobiles belonging to the colleague for Trust use, even where those devices have been authorised to be used for Trust business purposes.

• The Trust reserves the right to wipe all information from a member of staff's device should they deem it necessary, this will wipe all information from the device completely – this includes both corporate and personal information (contacts, messages, photo's, apps, etc.) By accepting this Terms and Conditions document you are giving your explicit consent for the Trust to wipe your mobile device (Trust or BYOD).

• Staff members **MUST** inform the IM&T service desk **IMMEDIATELY** if their mobile device (Trust or BYOD) is lost or stolen. You also confirm that the any BYOD has suitable insurance procured personally and relevant steps to inform your own insurer of the loss or theft.

• Should a member of staff's mobile device be required for any investigation into a member of staff's conduct or as part of a Subject Access Request, the mobile device requested will be surrendered immediately to the Trust's Information Governance team once the request has been made.

• Staff members understand that access is restricted to view and access their email, calendar, contacts and access the corporate instant messaging service and any clinical systems that are approved for use on the device (e.g. NerveCentre and ICE). Staff will also be able to access the internet using a secure Wi-Fi connection from their personal mobile device

• The Trust reserves the right to withdraw access to the Mobile Device services at any time. By agreeing to these Terms and Conditions you are explicitly stating that you understand that the Trust, or the Trust as a whole, will accept **NO** legal liability for any unlawful activity conducted on the mobile device in question nor damage or operational issues to devices that were not issued by IM&T.

Signed*……

Print……

Date……

*If sending form from the requestor email account – this will also count as authorisation

NB: Paper copies of this document may not be most recent version. The definitive version is held in the policy and guideline library on INsite