Leicestershire Partnership NHS Trust

Staff Mobile Device Policy

This document provides guidance for managers and employees regarding the appropriate use of mobile communications devices provided by the Trust for work use.

Key Words:	Mobile phone, remote access, Smartphone, Tablet Devices	
Version:	5.2	
Adopted by:	Trust Policy Committee	
Date this version was adopted:	10 September 2021	
Name of Author:	Head of Data Privacy	
Name of responsible committee:	Data Privacy Committee	
Please state if there is a reason for not publishing on website:	N/A	
Date issued for publication:	September 2021	
Review date:	February 2024	
Expiry date:	31 March 2025	
Target audience:	All staff	
Type of Policy	Clinical ✓	Non Clinical ✓
Which Relevant CQC Fundamental Standards?	Person-centred care, Safety, Premises and equipment	

Contents

Version Control and Summary of Changes

Version number	Date	Comments (description change and amendments)
Version 3	04/11/2014	Draft version for review
Version 4	11/03/2019	Significant changes to first draft following expanded use of staff mobile devices in line with Agile working
	12/08/2019	Updates from consultation
	01/10/2019	Updates following staff side policy meeting
5 5.1 3 month ext July DPG 5.2 4 month ext Sept DPG	25/09/2020	Review and update following implementation. Changes on use of handsfree devices and use of personal phones.

For further information contact:

Senior HR Advisor, **Direct Line – 0116 295 7259**

Equality Statement

Leicestershire Partnership NHS Trust (LPT) aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the provisions of the Equality Act 2010 and promotes equal opportunities for all. This document has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

Due Regard

LPT will ensure that Due regard for equality is taken and as such will undertake an analysis of equality (assessment of impact) on existing and new policies in line with the Equality Act 2010. This process will help to ensure that:

- Strategies, policies and services are free from discrimination;
- LPT complies with current equality legislation;
- Due regard is given to equality in decision making and subsequent processes;
- Opportunities for promoting equality are identified.

Please refer to due regard assessment (Appendix 4) of this policy.

Definitions that apply to this Policy

Android	Mobile operating system
Tablet	A slim mobile touchscreen computer, capable of wireless connection to the internet.
WAP	Wireless Application Protocol'. Service allowing access to the internet on mobile devices.
iOS	**iOS** (originally **iPhone OS**) is a mobile operating system
Mobile device	Includes tablets and smart technology.
Lone Worker	Is used to describe a wide variety of staff who work, either occasionally or regularly, on their own, without access to, or out of sight of immediate support from managers or other colleagues
Due Regard	Having **due regard** for advancing equality involves: • Removing or minimising disadvantages suffered by people due to their protected characteristics. • Taking steps to meet the needs of people from protected groups where these are different from the needs of other people. • Encouraging people from protected groups to participate in public life or in other activities where their participation is disproportionately low

1.0 Purpose of the Policy

The purpose of this policy is to provide managers and employees with clear guidelines regarding the appropriate use of authorised mobile communication devices provided by the Trust in the course of carrying out their work duties.

Authorised remote and mobile communication devices are provided primarily for the following circumstances:

- The need for the employee to be contactable and to contact others
- If the job requires out of hours contact
- In order to easily access internet-based services including Apps for work purposes, remotely and securely
- To be able to take images for both clinical and diary management purposes securely

This policy does not provide information about how the mobile device works i.e. how to unlock, send email etc. For any advice on how to use your device, please contact Leicestershire Health Informatics Service (LHIS) on 0116 2953500.

2.0 Summary and Key Points

This Policy and Procedure provides clear guidance for managers and employees regarding the use of Trust supplied mobile communication devices in the course of carrying out their work duties. This includes for example mobile phones, including smartphones and Tablets**. This does not cover personal devices which are prohibited from being used for work purposes.** The policy does not apply to Trust supplied mobile working personal computers (i.e. Laptops including Toughbook's).

This Policy applies to all Leicestershire Partnership NHS Trust (LPT) employees, staff seconded to LPT from other organisations and whether located within or outside of LPT premises. It also includes the aforementioned persons connecting to LPT resources using mobile phones which have email and internet access.

This policy does not cover students undertaking placements, in line with University guidance, students should not be expected to use their personal devices for undertaking work activity and therefore local arrangements for establishing means of contact with mentors should be agreed, which may include the use of a 'pooled device' where this is deemed appropriate.

This Policy is closely associated with and must be read in conjunction with:

- The Trust Data Security and Protection Policy (DSPP);
- Social Media and e-Communications Policy
- LHIS Security Leaflets and the HIS Good Practice Guide found on the LPT Intranet
- Lone Worker Policy.

Any intention to use remote and mobile devices for e-communication with patients and/or carers must first comply with:

- Social Media and e-Communications Policy
- Own Professional Bodies' Code of Practice/Conduct
- E-Communications with Service Users Policy
- Data Protection and Information Sharing Policy.

The use of remote and mobile communication devices by patients and visitors is addressed in the Trust policy 'Social Media and e-Communications Policy.

Guidance on the use of mobile devices whilst driving exists in a number of Trust policies and guidance documents. These instructions are now replaced by the requirements in this document.

3.0 Introduction

As the use of mobile technology and computing devices is growing it is vital that the data held on them is not compromised by poor security practices. Mobile technology and devices are by their nature vulnerable to both being mislaid as well as being attractive to a potential criminal. It is important therefore that all users of Trust mobile phones, Smartphones, etc., are aware of the inherent risks associated with their use, particularly away from the work place. All NHS Data on portable and remote working devices should only be saved on a Trust device that is encrypted to NHS standards and procured through (LHIS).

The Trust is moving increasingly to remote and mobile working in order to improve the flexibility and efficiency of its service provision. Mobile communication devices will be provided where these are required to support a business function and the need identified in risk assessment. **The Trust does not support the use of personal devices for business purposes based on the risk of virus infection and the potential for introduction of cyber/information vulnerabilities to the network.**

4.0 Roles and Responsibilities

4.1 The Trust Board:

- Has a legal responsibility for Trust policies and for ensuring that they are carried out effectively.
- Trust Board Sub-committees have the responsibility for ratifying policies and protocols.

4.2 Service Directors and Heads of Services will be responsible for:

- Authorisation of the purchase /rental and issue of mobile telephones and other mobile devices to all staff via the designated person within each directorate.
- Ensuring compliance with the agreed local procedures within their areas.
- Ensuring local procedures are agreed for each Directorate they manage and that these are updated periodically.
- Directors/Heads of Services must notify the LHIS Service Desk of any transfers or withdrawal of authorised mobile communication devices, particularly when a member of staff leaves the Trust.
- Review of quarterly bills and authorisation for payment.

4.3 Managers and Team Leaders will be responsible for:

- Monitor compliance with the agreed local procedures within their areas.
- Ensuring there are identified areas for the use of mobile phones/device as described in this policy.
- Ensuring correct forms are used as per LHIS requirements when ordering mobile telephone or other devices, cancelling or transferring to another user. All forms can be found on the Trust's intranet. These, once signed by the employee, are to be kept secure for audit purposes
- Are responsible for ensuring all invoices for mobile phones or other devices are processed in a timely manner.
- All returned device(s) from staff leaving the Trust are either returned or reassigned to another member of staff with support from LHIS.
- Ensuring this policy is available to all staff.
- Ensuring employee's report any loss or misuse of a Trust mobile device using the Trust's e-irf incident reporting system and report the loss to LHIS service desk.

4.4 Employees Responsibilities:

- To be aware of the policy and their duty of care to others. To ensure that all personal information must be treated carefully and must not be disclosed to unauthorised persons which is line with the confidentiality clause of their contract of employment.
- Use authorised mobile communication devices responsibly, lawfully and in accordance with the terms of this policy.
- Comply with the Social Media and e-Communications Policy and the Remote and mobile working policy (ref DSPP).
- To report any breaches of the policy (abuse, loss, theft) using the Trust reporting process and immediately to the LHIS Service Desk so that steps can be taken to secure data (for example, remote wipe).
- To report all cases of suspected fraudulent usage of mobile communication devices to the Trust's Local Counter Fraud Specialist.
- Staff leaving the Trust must return their mobile communication device(s) to their manager.

5.0 Policy Requirements

Trust Equipment remains the property of the Trust and shall only be issued where there is a justified and authorised requirement in meeting business or operational needs of the Trust. It shall be configured by LHIS in accordance with defined standards, that are appropriate to its use and, takes account of NHS requirements, standards, recommendations and guidelines for such devices.

Allocation of Trust Equipment and access to its Mobile Working Solutions shall be controlled by authorisation and asset management processes. It is an express condition that where users are granted access to, and use of these resources, they shall assume responsibility for the physical security of equipment and information accessed or stored on the device. At all times they shall comply with the Trust's associated IT Guidelines and current safe working practices.

You may use a Trust supplied device where this has been authorised for work purposes. In either case, it is the employee's responsibility to ensure that appropriate security measures have been enforced or manually applied to the device in use. Security must be compliant with the Data Security and Protection Policy for

NHS owned devices. Further guidance and support can be sought from LHIS Helpdesk.

In particular, devices which are used to store personal confidential information of patients or staff for example in the form of voice mail, email, or text messages, must have strong passwords set on the device. These will also be subject to controlled onward use and secure disposal.

Failure to ensure that security measures are in place on a device used for work purposes, could be treated as misconduct or as gross misconduct leading to disciplinary procedures up to and including dismissal.

Security Measures

- Trust supplied smartphones which are synchronised to accept your emails, have enforced security including passwords, protection against data storage in the cloud, and remote wipe facility in case of loss or theft.
- Any Trust supplied smartphones that are not linked to synchronised emails and do not have enforced security must be reported to the LHIS service desk immediately in order that action can be taken to rectify this.

- Trust supplied phones which are not smartphones (e.g. Nokia phones) do not have enforced security. Therefore Users must set a pin number on their Nokia phone, so that if lost, the finder cannot access the phone content. It is also good practice to display your name and a landline number on the front screen of a device so that the finder is able to contact you – at least until the battery fails

Users shall comply with Trust policies and NHS best practice guidance concerning the requirement for access to information; in particular that information should be shared only on a 'need to know' basis. Storage of sensitive information on Trust equipment shall be kept to the necessary minimum (in respect to both content and duration).

Data on devices shall be regularly backed up to the Trust's file storage systems. It shall be the responsibility of users to ensure that equipment assigned to them is regularly connected to the Trust's network to ensure that backups are made.

Users must respond to device software updates that are communicated via LHIS in a timely manner to ensure that its operating system is up to date. If there are any queries about the authenticity of the update request please check with LHIS Service desk (0116 2953500).

Where Trust owned equipment is unavoidably used for personal purposes, please comply with the requirements in section 7.0 below

Usage of Trust devices must comply with the Good Practice Requirements in the Social Media and e-Communications Policy. In particular, with section 5.4 which states as follows:

> *"Do not access, create, send, forward, copy, post, or distribute any material (including information, questions, opinions, or images), which is libellous,*

defamatory or derogatory, pornographic, sexually explicit, obscene, indecent or extreme, or which is discriminatory or harassing, or includes hostile material relating to gender, sex, race, sexual orientation, religious or political convictions or disability, or incitement of hatred, violence, terrorism or any illegal activity.

Ask yourself "Would I like this content to be disclosed in a Court of Law?"

Do not knowingly send or post material which causes distress or offence to another user. Senior Trust Management is the final arbiter on what is or is not offensive material, or what is or is not permissible access, (other than for instances which demand criminal investigation.).

In addition, staff must not send or post communications which encourage behaviour that could be linked to safeguarding issues, for example:

- *Bullying*
- *Luring and exploitation*
- *Theft of personal information*
- *Encouraging self-harm or violence*
- *Glorifying activities such as excessive drinking or drug taking.*

It is the employee's responsibility to keep the mobile communication devices charged and ready for use and authorised mobile communication devices need to be switched on when the member of staff is on duty or on call.

Emergency contacts should be kept on device address books and/or speed dial as this will speed up the process of making a call to raise an alarm.

If you have a concern about the security of using a mobile communication device for work related purposes, please contact your line manager and the LHIS Service Desk in the first instance.

In the event of misuse, theft or loss this should be reported immediately to the LHIS Service Desk so that steps can be taken to secure data (for example, remote wipe). Theft or loss should be reported to the Police and in the case of theft a Crime Number must be obtained. LHIS will notify the current network providers where necessary. The manager will need to liaise with LHIS for procuring a replacement if appropriate. Report any breaches of the policy (abuse, loss or theft) using the Trust reporting process and quoting the LHIS service desk reference and police crime number where appropriate.

The employee is responsible for taking reasonable precautions to avoid loss or misuse of their mobile communication device. This includes not leaving it in view in unattended vehicles and storing it securely when not in use.

Any access to the internet should be for work purposes. Downloads of any materials for personal use applications or ring-tones are not permitted, as viruses can often be embedded in these materials, thereby rendering the mobile device inoperable. Should an application be required for business use then the employee should check with LHIS that it is part of the LHIS App Library for download [see LHIS App Guidelines for further information].

Potential and actual security breaches associated with Trust Equipment, the use of Information Assets and Mobile Working Solutions shall be reported and investigated in accordance with the Trust's incident reporting procedures.

6.0 Processes

6.1 Personal Use of Trust Mobile Devices

Other than in exceptional circumstances, such as emergency situations, Trust mobile phones and smartphones must only be used for the business of the Trust.

The Trust further recognises that in this age where personal e-communication devices are widely used, the need to use NHS owned devices for personal purposes should not happen unless in circumstances outlined below.

Staff are strongly advised to read the Trust Social Media & e-Communications Policy in relation to the blurring of the lines between business and personal communications.

6.2 Restrictions on the Use of Trust Mobile Devices

6.2.1 Use of camera on phone

The use of camera functionality on the Trust device is acceptable where it has been agreed that there is a service need i.e. taking images of patient wounds, taking images of visit lists as an aide memoir.

Where you are using the Trust device to take images of a patient or their relative/carer, you must obtain their consent before the image is taken and also inform them of the purposes for which the images will be used.

NB: The use of personal devices for taking images is strictly prohibited and could lead to disciplinary action being taken.

Refer to the Management of Electronic Health Records Policy for more detailed information

6.2.2 Transfer of call

Any transfer of calls from a Trust device to either a landline or another Trust device must be discussed and agreed with the responsible line manager and any relevant staff who are responsible for the device that the calls are being diverted to.

Under no circumstances should a Trust phone number be transferred to a personal device.

6.2.3 Patient Safety

Where mobile phone contact numbers are provided to a patient in order to access a service or contact a member of staff, the service must consider the implications of:

- Staff annual leave/sickness cover

- Voicemail access/out of hours contact details

Any mobile phone that is used for patient/service user contact should have a voicemail message providing details of alternative contact, which is preferably a landline number.

In addition a patient/service user must always be provided with details of an alternative contact number should they be unable to contact a member of staff on a mobile number.

Line managers should consider the need to develop a local Standard Operating Procedure when Trust mobile devices are used regularly as part of service provision to contact or be contacted by patients/service users

6.2.4 Confidentiality

Staff must refer to the principles of the Data Protection Act and Caldicott Principles to ensure that mobile devices are only used to discuss personal, sensitive or confidential issues in circumstances that are otherwise unavoidable. If another more secure method is available then staff should be using that method.

Texting is not a safe method of transmitting patient identifiable, sensitive or confidential information. If it is absolutely necessary to refer to a patient/service user or staff member in a text, the message should avoid identifying any individual. This can be achieved by, for example, using just initials and being careful not to include any additional information such as an address or post code that might identify them.

If including personal identifiable information in a text cannot be avoided then that individual's consent must be obtained in advance. Also avoid including anything in the text that identifies the Trust.

However, the Trust acknowledges that the use of text messages as a form of communicating with patients/service users is becoming more common as patients/service users are requesting this as their preferred method of exchanging dialogue with services. However, the above guidance must be followed and the choice of communication by the patient/service user must be recorded in the clinical record. Staff should refer to the 'Electronic Communications with Service User Policy'.

6.3 Authorisation of Use of Trust Equipment & Mobile Working Solutions

Requests for provision of Trust Equipment and access to Mobile Working Solutions will be considered by The Manager on a case-by-case basis. Authorisation may be granted where The Manager concludes that a business or operational need is justified, and must be formalised by the completion and signature of the authorisation form (refer to Appendix 1).

Authorised requests must be submitted by The Manager to the LHIS IT Equipment requests in accordance with its current ordering processes and procedures.

Requests will be processed by the LHIS in accordance with established procedures and published timescales.

6.4 Loss/Replacement of Trust Mobile Device

Recipients of Trust mobile devices are responsible for their security and care. Recipients must report any defects, damage or losses as soon as reasonably practicable to their line manager and the Issuing/Receiving Department. Recipients losing or damaging a Trust mobile device where they are deemed not to have taken appropriate care of it will be required to pay in full or in part for a replacement.

This applies equally to recipients and users of pooled devices.

6.5 Use of Personal Devices

The use of personal devices for clinical or any purposes that involve the sharing of personal information is not permitted owing to the increased risk of breaches of confidentiality and the introduction of network vulnerabilities which could lead to a cyber/information security threat to the individual or the network.

6.6 Driving and Mobile Devices

6.6.1 Legal Viewpoint

Using a mobile phone whilst driving is considered the biggest health risk posed by mobile phones. It is also contrary to the Road Traffic Act and Highway Code. It can increase your chances of having an accident, and it is illegal to use a handheld mobile phone whilst driving or riding a motorbike.

The penalties include 6 points on your licence and £200 fine for using a handheld device when driving. Individuals will lose their licence if they passed their driving test within the last 2 years; 3 points on your licence if you do not have a full view of the road and traffic ahead or proper control of the vehicle.

The use of hands free devices is not prohibited under legislation. However, the use of these devices still increases the likelihood of the driver being distracted and thereby involved in an accident. If this occurs, the driver risks prosecution for failing to have proper control of the vehicle because of careless or dangerous driving.

6.6.2 Trust requirement

The Trust requires its employees to follow the guidance issued by the Department of Transport on the safe use of mobile phones in cars:

- *Keep your mobile phone switched off when you are driving – you can use voicemail, a messaging service or call diversion to pick up messages at the end of your journey;*
- *If you need to use your mobile phone, stop in a safe place – do not stop on the hard shoulder of a motorway unless it is an emergency;*
- *Avoid using hands-free devices – these can be just as distracting as hand-held devices.*

It is illegal to hold a phone or sat nav while driving or riding a motorcycle.

The device must not block your view of the road and traffic ahead. You must stay in control of your vehicle at all times. The Police can stop you if they think you are not in control because you are distracted and you can be prosecuted.

No line manager will require any member of staff to receive or make calls whilst driving a vehicle. Staff are expected to switch their mobile devices to silent and activate the messaging service. If staff decide to use their mobile device while in a vehicle, the organisation expects them to stop the vehicle in a safe place and switch the engine off before checking their messages or making calls.

Staff must remember that they are responsible for driving safely and within the rules of the Road Traffic Act. Staff and not the organisation will be liable if they are found to be using a mobile device whilst driving for work purposes. The only occasion where a device can be used, is for dialling 999 in a genuine emergency and the driver judges it unsafe or impractical to stop the vehicle.

The organisation also discourages the use of hands free devices. There may be some exceptions where it is necessary for staff to be contactable at all times for business purposes. In such cases, this should be agreed following discussion with the appropriate line manager taking all actions to minimise risks to the health, safety and wellbeing of the staff member. These measures include the following:

You must have hands-free access such as:

- *A Bluetooth headset*
- *Voice command as part of your vehicle*
- *A dashboard holder or mat*
- *Windscreen mount*
- *A built-in sat nav*

6.7 Disposal Reference

All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. All removable media holding personal identifiable or other sensitive information and no-longer required, will be securely disposed of.

Disposal of assets in a secure and environmentally friendly manner (e.g. mobile phones) will be controlled by the LHIS Infrastructure and Support Manager to prevent possible unauthorised access to data. (Ref. LHIS Procedure for the Secure Disposal of Computer Equipment) (DSPP part 2, 4.9.2)

Where equipment has a change of purpose or owner, all patient-identifiable or other sensitive data will be removed by specialist software (deleting files is not adequate).

The LHIS Procedure for the secure disposal of computer equipment states as follows:

Disposal of other Portable Equipment (mobile phones, tablets etc).

- Redundant assets and confidential (patient-related or other sensitive) information must be disposed of in a safe, secure and environmentally friendly manner.

- Mobile Phones are received by the LHIS usually by internal mail from a central point in the Trust or sent individually by post. Users are expected to remove the sim card before returning the phone. On receipt of the phone, it is checked for a sim card. If there is no sim card, the phone is recycled by GreenWorld Electronics Ltd.

If there is a sim card, LHIS contact the service provider. If the sim card is active but out of contract, the user is tracked and asked if they want to terminate (if it is out of contract it does not cost anything to terminate). If there is a live contract the budget holder is asked to decide. If the budget holder chooses not to continue the contract it will end in 30 days and the sim destroyed by cutting.

There may be valid reasons for staff to retain the sim: the sim card may have a live contract and all the users contact details but they are due an upgrade or, if the contract is ceased, they may wish to destroy the sim so that they are confident that no confidential details have been destroyed.

Users and budget holders should be aware that to cancel a contract they need to complete a cancellation form – otherwise they will continue to be charged monthly for the contract.

- Trust owned smart phones; on receipt by LHIS, the device is checked for a sim card. If there is no sim they are not active. The device is then checked for an internal memory card which is erased.

The device is then disposed of through GreenWorld Electronic Ltd.

NHS owned Tablets will be erased and disposed of by GreenWorld.

7.0 PROCUREMENT

Leicestershire Health Informatics Service:

- Will process all orders upon receipt of the appropriate completed authorised requisition form (found on the Trust's Intranet – follow the LHIS links) from the Director/Head of Services via the designated person within each directorate.

- Will purchase all the LPT mobile telephones and other devices using the current contract network provider.

8.0 BREACH OF THE POLICY

Employees who do not follow the terms of this policy **may** be liable to disciplinary action in accordance with the Trust's Disciplinary Policy and Procedure and, recovery of any cost incurred by the Trust. Each instance will be considered on an individual basis.

Non employee users of the facilities who breach the policy may have their access to the facilities withdrawn.

9.0 RETURN / RECALL OF MOBILE PHONES/DEVICES

Trust owned mobile phones/devices remain the property of the Trust and may be recalled at any time at the discretion of the Trust. Managers are responsible for ensuring that mobile phones and devices are returned as part of their termination procedures. Should any member of staff's contract of employment terminate then the employee should obtain a signed receipt from their line manager to say they have returned their mobile phone/ other communication device.

10.0 HEALTH & SAFETY

Mobile phones should not be a substitute for good practice/safe systems of work in ensuring safety and security of staff. A mobile phone should never be relied upon as the only means of communication. Lone workers should always ensure that their manager or colleagues are aware of their visits; this would be more prudent within areas with poor signal strength to their mobile phone. Staff must follow the Trust's Lone Working Policy, team risk assessment and local arrangements.

Mobile phones are low power devices that emit and receive radio waves. Radio waves emitted above a certain level can cause heating effect to the body. All mobile phone sold in the UK meet international guidelines on emissions of radio waves.

The Trust will follow the current safety guidelines in regards the operation of mobile telephones and will advise and amend its operation procedures to reflect changes in government advice.

11.0 TRAINING NEEDS

There is no training requirement identified within this policy

12.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
	There is a locally agreed procedure for use of mobile devices aligned to this policy	Sections 4.2/4.3	Procedure is agreed through Clinical Directorate Governance Group	Clinical Governance Lead	Sign off and then 2 year review
	Misuse or abuse of policy is reported via e-IRF	Sections 4.4/5.12	Review of incidents relating to mobile device usage	Data Privacy Group	Quarterly
	Allocation of Trust Equipment and access to its Mobile Working Solutions shall be controlled by authorisation and asset management processes	Section 5.2	Review of authorisation records Review of asset register	Clinical Directorate Governance Data Privacy Group	Annually Annually
	Text messaging as preferred method of communication with service user is documented in their clinical record	Section 6.2.4	Part of record keeping auditing and monitoring process	Clinical Directorate Governance	Annually
	Reports of damage, loss or theft of devices	Section 6.4	Review of incidents	Data Privacy Group	Quarterly

13.0 LINKS TO STANDARDS/KEY PERFORMANCE INDICATORS

TARGET/STANDARDS	KEY PERFORMANCE INDICATOR
Care Quality Commission fundamental standards Person-centred care, Safety, Premises and equipment	That the trust maintains compliance with CQC fundamental standards.

14.0 REFERENCES AND ASSOCIATED DOCUMENTATION

- Health and Safety Executive [online] – Mobile phones and health: Guidance from the department of health (OC497/2) http://www.hse.gov.uk/foi/internalops/ocs/400-499/497_2.htm *[Accessed 1st August 2014]*

- LPT Data Protection and Information Sharing Policy
- LPT Social Media and Electronic Communications Policy
- LPT Audio and Visual Recordings Guidelines
- LPT Electronic Communications with Patients Policy
- LPT Information Security Policy
- LPT Lone Worker Policy Appendices 14 & 15

Appendix 1

The NHS Constitution

The NHS will provide a universal service for all based on clinical need, not ability to pay. The NHS will provide a comprehensive range of services

Shape its services around the needs and preferences of individual patients, their families and their carers	✓
Respond to different needs of different sectors of the population	✓
Work continuously to improve quality services and to minimise errors	✓
Support and value its staff	✓
Work together with others to ensure a seamless service for patients	✓
Help keep people healthy and work to reduce health inequalities	✓
Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance	✓

Appendix 2

Stakeholders and Consultation

Key individuals involved in developing the document

Name	Designation
Jyoti Chauhan	Senior HR Advisor
Chris Biddle	Cyber Security Manager, LHIS
Girish Kunigiri	Consultant Psychiatrist, CCIO
Ian Wakeford	Head of LHIS
Bernadette Keavney	Head of Health & Safety Compliance

Circulated to the following individuals for comment

Name	Designation
Members of Data Privacy Group	
Members of IM&T Delivery Group	
Katherine Roland	Operational Lead CINSS Team
Laura Browne	Operational Lead Tissue Viability
Simon Jones	IM&T Business Manager, LHIS
Claire Mott	Clinical Change Lead Document Scanning
Graham Calvert	Clinical Lead for IT & Information Governance, FYPC
Craig Parylo	Business Information Manager
Directors / Heads of Service and Direct Reports	
Operational HR Team	
Equalities Team	
Staffside	
Workforce & Wellbeing Group	

Appendix 3

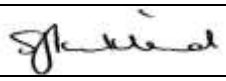
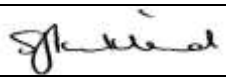
Due Regard Screening Template

Section 1	
Name of activity/proposal	Staff Mobile Device Policy
Date Screening commenced	17 July 2019
Directorate / Service carrying out the assessment	Enabling
Name and role of person undertaking this Due Regard (Equality Analysis)	Sam Kirkland, Head of Data Privacy
Give an overview of the aims, objectives and purpose of the proposal:	
AIMS: The purpose of this policy is to provide managers and employees with clear guidelines regarding the appropriate use of authorised mobile communication devices provided by the Trust in the course of carrying out their work duties.	
OBJECTIVES: The Trust is moving increasingly to remote and mobile working in order to improve the flexibility and efficiency of its service provision. Mobile communication devices will be provided where these are required to support a business function. The objective is to ensure that staff are aware of the perimeters in which using Trust devices can be utilised	

Section 2	
Protected Characteristic	**If the proposal/s have a positive or negative impact please give brief details**
Age	Positive – Trust mobile devices can be provided to all staff required to have one in the course of their duties
Disability	Positive – Trust mobile devices can be provided to all staff required to have one in the course of their duties
Gender reassignment	No Impact
Marriage & Civil Partnership	No Impact
Pregnancy & Maternity	Positive – Trust mobile devices can be provided to all staff required to have one in the course of their duties
Race	No Impact
Religion and Belief	No Impact
Sex	No Impact
Sexual Orientation	No Impact
Other equality groups?	

Section 3			
Does this activity propose major changes in terms of scale or significance for LPT? For example, is there a clear indication that, although the proposal is minor it is likely to have a major affect for people from an equality group/s? Please <u>tick</u> appropriate box below.			
Yes		No	
High risk: Complete a full EIA starting click here to proceed to Part B		Low risk: Go to Section 4.	✓

Section 4
If this proposal is low risk please give evidence or justification for how you reached this decision:

The Policy is to support the use of mobile devices across the organisation where there is a business need.			
Signed by reviewer/assessor		**Date**	08/12/2020
Sign off that this proposal is low risk and does not require a full Equality Analysis			
Head of Service Signed		**Date**	08/12/2020

Appendix 4

DATA PRIVACY IMPACT ASSESSMENT SCREENING

Data Privacy impact assessment (DPIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet Individual's expectations of privacy. **The following screening questions will help the Trust determine if there are any privacy issues associated with the implementation of the Policy. Answering 'yes' to any of these questions is an indication that a DPIA may be a useful exercise. An explanation for the answers will assist with the determination as to whether a full DPIA is required which will require senior management support, at this stage the Head of Data Privacy must be involved.**			
Name of Document:	Staff Mobile Device Policy		
Completed by:	Sam Kirkland		
Job title	Head of Data Privacy		**Date** 08/12/2020
Screening Questions		**Yes / No**	**Explanatory Note**
1. Will the process described in the document involve the collection of new information about individuals? This is information in excess of what is required to carry out the process described within the document.		No	
2. Will the process described in the document compel individuals to provide information about them? This is information in excess of what is required to carry out the process described within the document.		No	
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information as part of the process described in this document?		No	
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		No	
5. Does the process outlined in this document involve the use of new technology which might be perceived as being privacy intrusive? For example, the use of biometrics.		No	
6. Will the process outlined in this document result in decisions being made or action taken against individuals in ways which can have a significant impact on them?		No	
7. As part of the process outlined in this document, is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For examples, health records, criminal records or other information that people would consider to be particularly private.		No	
8. Will the process require you to contact individuals in ways which they may find intrusive?		No	
If the answer to any of these questions is 'Yes' please contact the Data Privacy Team via Lpt.dataprivacy@nhs.net **In this case, ratification of a procedural document will not take place until review by the Head of Data Privacy.**			
Data Privacy approval name:			
Date of approval			

Acknowledgement: This is based on the work of Princess Alexandra Hospital NHS Trust