Management of Mobile Devices Policy

Target Audience
All users of the Trust’s mobile devices including, employees, contractors, partner organisations and volunteers, patients or service users.
**CONTENTS**

<table>
<thead>
<tr>
<th>SECTION</th>
<th>PAGE NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>2. PURPOSE</td>
<td>3</td>
</tr>
<tr>
<td>3. SCOPE</td>
<td>3</td>
</tr>
<tr>
<td>3.1 Definitions within the scope of the policy</td>
<td>3</td>
</tr>
<tr>
<td>4. RESPONSIBILITIES, ACCOUNTABILITIES AND DUTIES</td>
<td>4</td>
</tr>
<tr>
<td>5. PROCEDURE/IMPLEMENTATION</td>
<td>5</td>
</tr>
<tr>
<td>5.1 Management of Devices</td>
<td>5</td>
</tr>
<tr>
<td>5.1.1 Device Management</td>
<td>5</td>
</tr>
<tr>
<td>5.1.2 Multiple User Devices</td>
<td>5</td>
</tr>
<tr>
<td>5.1.3 App Stores</td>
<td>5</td>
</tr>
<tr>
<td>5.1.4 Installation of Applications and Software</td>
<td>5</td>
</tr>
<tr>
<td>5.1.5 Trust Owned Mobile Devices For Use By Patients Or Service Users</td>
<td>6</td>
</tr>
<tr>
<td>5.1.6 Issuing and Distribution of Mobile Devices</td>
<td>6</td>
</tr>
<tr>
<td>5.1.7 Lost or Stolen Devices</td>
<td>6</td>
</tr>
<tr>
<td>5.2 Compliance</td>
<td>6</td>
</tr>
<tr>
<td>5.2.1 Staff</td>
<td>6</td>
</tr>
<tr>
<td>5.2.2 Service Users</td>
<td>6</td>
</tr>
<tr>
<td>6. TRAINING IMPLICATIONS</td>
<td>7</td>
</tr>
<tr>
<td>7 MONITORING ARRANGEMENTS</td>
<td>7</td>
</tr>
<tr>
<td>8. EQUALITY IMPACT ASSESSMENT SCREENING</td>
<td>7</td>
</tr>
<tr>
<td>8.1 Privacy, Dignity and Respect</td>
<td>7</td>
</tr>
<tr>
<td>8.2 Mental Capacity Act</td>
<td>8</td>
</tr>
<tr>
<td>9. LINKS TO OTHER TRUST PROCEDURAL DOCUMENTS</td>
<td>8</td>
</tr>
<tr>
<td>10. REFERENCES</td>
<td>8</td>
</tr>
<tr>
<td>11. APPENDICES</td>
<td>8</td>
</tr>
</tbody>
</table>

None
1. INTRODUCTION

The Trust recognises that mobile devices are an essential part of everyday life for many people. The availability and use of mobile devices is commonly perceived to increase the efficiency of an organisation’s workforce.

The Trust will issue a mobile device to relevant staff to use on duty to assist with access to corporate, clinical and reference information whilst away from their base.

It is important to find a balance between the needs of patients, visitors and employees to maintain communication with the need to protect people against the misuse of advanced technology.

The Trust expects that everyone who uses a mobile device will respect patient confidentiality and show consideration for others.

2. PURPOSE

The aim of this policy is to provide guidance to all staff on the appropriate use and management of mobile devices whilst at work and/or on Trust premises while protecting the safety, privacy and dignity of patients, carers, visitors, and staff in line with guidance from the Department of Health.

3. SCOPE

The policy applies to all users of the Trust’s mobile devices to access Trust IT systems and services; including, but not limited to employees, contractors, partner organisations and volunteers.

This policy also covers the use of Trust owned mobile devices by patients or service users. Where this is permitted, there must be local guidelines in place regarding supervision of use.

The use of personal mobile devices (Bring Your Own Device (BYOD)) to access Trust information systems is not currently available but may be in the future.

This policy is based on the following guiding principles:

- The use of a mobile device is reasonable, appropriate, lawful and in accordance with Trust requirements;
- Staff are aware and comply with this policy;
- Mobile devices provided by the Trust are owned by the Trust; and individuals are responsible for the care and security of any mobile device issued to them.

3.1 DEFINITIONS WITHIN THE SCOPE OF THE POLICY

A mobile device is defined as a smartphone, tablet, laptop, notebook, or ultrabook which is capable of connecting to the Trust network infrastructure.
or to the mobile phone network to send and receive data.

These devices are typically built around the Apple, Android, or Microsoft operating systems.

4. RESPONSIBILITIES, ACCOUNTABILITIES AND DUTIES

The Chief Executive has overall accountability and responsibility for the maintenance and implementation of the policy.

Line Managers are responsible for the implementation of the policy within their business or clinical area, and for adherence by their staff.

It is the responsibility of each employee to adhere to this policy and all related documents.

The Information Technology and Information Governance (IG) teams are responsible for the implementation and enforcement of the Management of Mobile Devices Policy and will have organisational security management responsibilities for:

- monitoring and reporting on the state of mobile device management within the organisation
- ensuring that the management of mobile devices policy is implemented throughout the organisation
- developing and enforcing detailed procedures to maintain security
- ensuring compliance with relevant legislation
- ensuring compliance with Trust IT related policies

Detailed responsibility for mobile devices will be delegated to the relevant registered person.

Management responsibilities

All mobile devices provided by the Trust will be registered to a named individual who is responsible for ensuring the security and correct usage of that device.

All line managers should ensure that all staff are instructed in the safe use and security of devices in their possession.

Managers are responsible for ensuring that staff are trained in all aspects of their work that includes use of computer equipment and that they only use systems for their intended purpose.

Help and training materials can be requested through the IG Security Specialist or the IT Training Department.

User responsibilities

All users are responsible for operating the equipment in accordance with the Guidelines for the Safe and Secure Use of Mobile Devices and any local
operating procedures.

5. **PROCEDURE/IMPLEMENTATION**

5.1 **Management of Devices**

5.1.1 **Device Management**

All mobile devices will be connected to a central management system to ensure security and system integrity of that device.

Laptops will be secured through the Trust encryption, anti-virus, and configuration management systems.

All tablet devices will be secured through the Trust mobile device management (MDM) solution.

All smartphones that require additional apps to be installed will be secured through the Trust mobile device management (MDM) solution.

**The Trust solution will enable different configurations to be applied to devices to meet the disparate needs of staff, patients, and service users. It will be flexible and adaptable to the different operational requirements for these groups.**

5.1.2 **Multiple User Devices**

Laptops or tablet devices shared by multiple users still require individual unique login credentials.

Any device which cannot be set up with multiple user profiles (e.g. smartphones and iPads) must not be used by multiple users as they are configured to access an individual’s Trust emails. Sharing such devices may contravene the Data Protection Act and IG Security principles.

5.1.3 **App Stores**

All access to Apple iCloud, Google Play, Windows Store, and any other online app stores will be restricted.

The Trust will make available any approved clinical and non-clinical apps, whether public or purchased, through its own managed app store. The approved apps can be installed to designated devices for the purposes of complementing service delivery.

Staff will be able to download any licensed applications from the Trust managed app store to the tablet or smartphone device.

5.1.4 **Installation of Applications and Software**

The IT Department will maintain a central store of approved applications and software. These will be distributed by the IT Department using appropriate
centralised management tools.

All devices will only be permitted to use these approved applications and software.

Any application or software packages to be added to the approved list should be submitted through the Change Management Board for consideration. Further approval may be sought through recognised clinical and technical evaluation groups.

Any non-approved application or software package will be blocked or removed until such time as it has been reviewed and accepted to the standard list to ensure licence and security compliance.

5.1.5 Trust Owned Mobile Devices for Use by Patients or Service Users.

Where devices are provided for use by patients or service users, all devices will be appropriately configured to maintain network and data security and confidentiality.

5.1.6 Issuing and Distribution of Mobile Devices

Laptops and tablet devices will be configured, issued and supported by the IT Department. Smartphones will be configured, issued and supported by Purchasing.

If a member of staff leaves the department, all assets must be dealt with in accordance with the Notice Periods Policy and any standard operating procedures.

Equipment to be reissued to other users will be processed by the IT Department or Purchasing Department in accordance with standard operating procedures.

5.1.7 Lost or Stolen Devices

Lost or stolen devices must be reported immediately to the IT Department who will implement security protocols to wipe or disable the device.

Lost or stolen devices should also be reported to line managers and an IR1 report completed.

5.2 Compliance

5.2.1 Staff

Failure to comply with this policy may lead to disciplinary action and / or legal or Civil action being taken.

5.2.2 Service Users

Failure to comply with this policy may result in the removal of access to the
equipment and / or legal or Civil action being taken.

Please refer to the Information Technology Security Policy for full details of legal compliance requirements.

6  TRAINING IMPLICATIONS

There are no specific training needs in relation to this policy; however the following staff will need to be familiar with its contents: managers, staff and any third party having access to Trust information and/or Trust IT systems.

As a Trust policy, all staff need to be aware of the key points that the policy covers. Staff can be made aware through regular communication channels such as Team Brief, Weekly Newsletter, etc.

7.  MONITORING ARRANGEMENTS

<table>
<thead>
<tr>
<th>Area for Monitoring</th>
<th>How</th>
<th>Who by</th>
<th>Reported to</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring of the number of devices owned by the Trust</td>
<td>Report on the number of devices registered to the management solutions or recorded in the IT Asset Management system.</td>
<td>IT Support Manager</td>
<td>Head of Information Technology Health Informatics Sub Committee</td>
<td>Annual</td>
</tr>
<tr>
<td>Reports of loss of misuse of a Trust mobile device</td>
<td>IR1 Incident Reporting</td>
<td>Information Governance Manager</td>
<td>Information Governance and Records Management Steering Group</td>
<td>Quarterly</td>
</tr>
</tbody>
</table>

8.  EQUALITY IMPACT ASSESSMENT SCREENING

The completed Equality Impact Assessment for this Policy has been published on the Equality and Diversity webpage of the RDaSH website [click here](#).

8.1 Privacy, Dignity and Respect

The NHS Constitution states that all patients should feel that their privacy and dignity are respected while they are in hospital. High Quality Care for All (2008), Lord Darzi’s review of the NHS, identifies the need to organise care around the individual, ‘not just clinically but in terms of dignity and respect’.

As a consequence the Trust is required to articulate its intent to deliver care with privacy and dignity that treats all service users with respect. Therefore, all procedural documents will be considered, if relevant, to reflect the requirement to treat everyone with privacy, dignity and respect, (when appropriate this should also include how same sex accommodation is provided).

| Indicate how this will be met | No issues have been identified in relation to this policy. |

Page 7 of 8
8.2 Mental Capacity Act

Central to any aspect of care delivered to adults and young people aged 16 years or over will be the consideration of the individuals capacity to participate in the decision making process. Consequently, no intervention should be carried out without either the individuals informed consent, or the powers included in a legal framework, or by order of the Court.

Therefore, the Trust is required to make sure that all staff working with individuals who use our service are familiar with the provisions within the Mental Capacity Act. For this reason all procedural documents will be considered, if relevant to reflect the provisions of the Mental Capacity Act 2005 to ensure that the interests of an individual whose capacity is in question can continue to make as many decisions for themselves as possible.

9. LINKS TO OTHER TRUST PROCEDURAL DOCUMENTS

- Information Technology Security Policy
- Access Control Protocol
- Business Continuity Management Protocol
- Communications and Operations Management Protocol
- Human Resources Security Protocol
- Information Asset Management Protocol
- Information Security Incident Management Protocol
- Information Systems Acquisition, Development and Maintenance Protocol
- Notice Periods Policy
- Data Protection Policy
- Information Risk Management Policy
- Guidelines for the Safe and Secure Use of Mobile Devices
- Mobile Phone Policy

10. REFERENCES

None

11. APPENDICES

None