Midlands and Lancashire Commissioning Support Unit

POL011 Midlands & Lancashire Commissioning Support Unit – Mobile Working Policy

Version	**1.1**
Ratified By	**CSU Information Governance Strategy Group**
Date Ratified	**June 2018**
Author(s)	**Frank Woodall, Cyber Security Manager, Midlands & Lancashire CSU**
Responsible Committee / Officers	**Technical Architecture Board and Integrated Governance**
Issue Date	**August 2018 – Following endorsement at QP held in July 2018**
Review Date	**12 months from date of issue**
Intended Audience	**All Organisation Employees**
Impact Assessed	**TBC**

Midlands and Lancashire CSU
Kingston House
438-450 High Street
West Midlands
B70 9LD

www.midlandsandlancashirecsu.nhs.uk

NHS

Midlands and Lancashire
Commissioning Support Unit

Midlands and Lancashire CSU
Kingston House
438-450 High Street
West Midlands
B70 9LD

www.midlandsandlancashirecsu.nhs.uk

Table of Contents

Midlands and Lancashire CSU
Kingston House
438-450 High Street
West Midlands
B70 9LD

Midlands and Lancashire Commissioning Support Unit

Further information about this document:

Document name	**Midlands & Lancashire Commissioning Support Unit Mobile Working Policy**
Category of Document in The Policy Schedule	**Corporate**
Contact(s) for further information about this document	**Ian Hart** **Assistant Chief Information Officer** **Telephone: 01244 650546** **Email: ian.hart@nhs.uk**
This document should be read in conjunction with	**All other MLCSU IT policies and the Information Governance Handbook**
Published by	**Midlands & Lancashire Commissioning Support Unit** **1829 Building** **Countess of Chester Health Park** **Chester** **Main Telephone Number: 0844 800 9982 (Freephone)**
Copies of this document are available from	**Ian Hart** **Assistant Chief Information Officer, IT Services**

Version Control:

Version History:		
Version Number	**Reviewing Committee / Officer**	**Date**
V0.1	Draft issued for comment	November 2017
V1.0	Minor Amendments made as per comments	January 2018
V1.1	Approved by IT Architecture Board	March 2018
V1.1	Endorsed by CCG QP Committee	July 2018

Midlands and Lancashire CSU
Kingston House
438-450 High Street
West Midlands
B70 9LD

www.midlandsandlancashirecsu.nhs.uk

Purpose

To ensure the physical and data security of portable devices issued, managed and used by the Midlands and Lancashire Commissioning Support Unit (MLCSU).

For the purpose of this policy, portable devices can be defined as any equipment upon which Health Service data is held and or transported.

At the time of writing this policy, would include portable devices, pen drives, Smartphones and mobile phones in addition to laptop and Tablet Personal Computers. Detailed below in definition

Scope

This policy sets out the management of mobile devices issued, managed and used by MLCSU.

Mobile Device Definition

Equipment protected by this policy can be any mobile device including but not limited to:

- Laptop Computers
- Tablet Computers
- Smartphones
- Mobile Phones
- Digital Cameras
- Digital Voice Recorders
- Mass Storage

Cloud Storage

MLCSU only supports the use of the CSU instance of Microsoft Office 365* (including OneDrive) which has met current NHS England Information Governance standards.

Commercially available Cloud storage **MUST NOT** be used in any circumstance e.g. Dropbox, OneDrive*, iCloud, GoogleDrive etc unless specific written approval has been granted by the Information Governance Lead.

* - Note only the CSU's instance of Microsoft Office 365 and OneDrive has been approved for use by MLCSU employees

Management Responsibilities

Before a mobile device is issued the Manager and employee should assess if there are any significant vulnerabilities. Please contact the IT Department if you require any advice or assistance.

The Organisation needs to be aware of mobile equipment and users, and to confirm the devices are being used responsibly. If relevant, this information is registered under the Data Protection Act 1998. This will involve liaising with the organisation's IG lead. The IG lead should also provide advice concerning compliance with the relevant data protection principles. For further information around data protection refer to the Information Governance Handbook.

Mobile devices issued and managed by MLCSU will be recorded in the CSU's Asset Management Database.

Management must ensure that all employees using mobile equipment are made aware of their personal responsibilities under the Data Protection Act, their contract of employment, Confidentiality Code of Conduct and policies and procedures relevant to the security and confidentiality of personal information.

Staff should also be made aware of any IT configured security features applicable to the equipment they will be using e.g. locking SIM cards, setting file and equipment passwords on handover.

Employee Responsibilities

Users must be aware they have personal responsibility for the equipment and all data/information stored on the equipment and any accompanying media.

Users must report any security breaches, or if the equipment is lost or stolen, to the IT service desk as well as their line manager as soon as possible after the event.

Users must ensure that all mobile media is remain encrypted to national NHS encryption standards and any updates applied as required. All users must deploy strong passwords and these must conform to their organisation's password policy.

Users must not alter the configuration of any anti-virus or security software installed on the portable devices issued by MLCSU.

Usage of MLCSU equipment shall be limited to employees only and must not be used by those other than employees of the organisation e.g. family members.

Protection of Hardware

The user is responsible for the safeguarding of the mobile device. In this case, it means:

- When not in use, devices should be kept (where possible) in a locked drawer.
- Whilst in transit, portable devices should be in a suitable carrying case and should be kept out of view wherever possible.
- Device security is your responsibility at all times.
- Do not leave the device unattended in a public place e.g. car park.
- Avoid leaving the device within sight of ground floor windows or within easy access of external doors.

Security of Data

Confidential data must only be installed and or saved on portable devices which have been supplied by MLCSU and have an appropriate level of access security/encryption implemented. All MLCSU issued devices will be encrypted to a level which meets NHS current standards.

If work is being carried out in public places, meeting rooms and other unprotected areas, care should be taken to avoid the unauthorised access to or disclosure of the information stored and processed by the portable device. Be cautious around using public WIFI particularly in an unfamiliar location, if in doubt consider tethering or using your phones personal hotspot or MLCSU issued VPN.

Care should be taken by the staff using the portable device to minimise the risk of unauthorised persons overlooking the screen.

Confidentiality Policies apply equally to information whether in the office or at home. Failure to maintain confidentiality may result in disciplinary action being taken.

A storage solution is provided centrally on the MLCSU data network or MLCSU's Office 365 and not on each portable device and it is the responsibility of users to utilise this.

The use of the portable device and the data on it must not be shared with family members.

Anti-virus Software

Where appropriate devices issued by MLCSU will have an Anti-Virus software package installed.

This package is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files on the portable device.

Users must not alter the configuration of this package.

The anti-virus system's database of virus definitions must be updated on a regular basis, each day if possible, but at least once a week as a minimum. This means connecting the portable device to the network for the virus updates to be applied. The device should also be re-booted (fully switched off) on a regular basis to ensure that any updates are properly applied.

Mobile Device Updates

From time to time software and hardware suppliers issue patches for security and bug fixes, it is important that these updates are applied in a timely manner to ensure the security and smooth running of the device. For Windows devices updates will be issued via MLCSU's data network as part of MLCSU's Patch Management process, it is therefore vital that the device id connected to the data network on a regular basis and the device is re-booted as required to fully install the update. If your device fails to update for any reason please contact your IT Service Desk.

Password Security

MLCSU's User Account Management Policy applies in all cases for password security.

Device Loss and Security\Confidentiality Breaches

Where there is a potential for breach in patient/staff confidentiality, Reporting the loss / theft of a device to the appropriate manager within MLCSU.

Any incident **MUST** also be reported to the Midlands and Lancashire Commissioning Support Unit IT Service Desk and must also be logged to the Information Governance Team for investigation.

Employees Leaving the Organisation

It is the Line Manager's responsibility to ensure they know what mobile devices are issued to the employee and that all devices are returned to the organisation. The Line Manager should then ensure that these are returned to MLCSU so that they can be securely reformatted for re-issue or specialist recycling.

Bring Your Own Device (BYOD)

MLCSU does not support the use of BOYD for accessing the corporate network

MLCSU does allow access to a number of approved apps which can be used on personal devices which include but not limited to Timesheet and expenses and MLCSU's instance of O365. Employees can also access NHSmail on personal devices, but these must meet standards set by NHS Digital for further information on accessing NHSmail please see www.nhs.net

Audit

The software and information held on portable devices are subject to the same audit procedures as any other MLCSU systems.

Legislation

Users of portable devices must comply with current legislation regarding the use and retention of patient information and use of computer systems. These include, but are not limited to:

- Copyright, Designs & Patents Act 1988
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- The Data Protection Act 1998
- The Human Rights Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2001

Review

This policy will be reviewed 12 months from its date of approval. Earlier review may be required in response to exceptional circumstances or relevant changes in legislation.