HBL PARTNERSHIP in IT

Mobile Device Security Policy

Owner: Keith Fairbrother

Version: 4.7.0

Hertfordshire, Bedfordshire, and Luton ICT Shared Services is hosted by NHS Hertfordshire and West Essex Integrated Care Board

Copyright

Document Control

Document Owner	Keith Fairbrother	**Approved by**	HBL ICT SMT
Document Author(s)	Keith Fairbrother, Alex McLaren, Metaish Parmar	**Date of Approval**	14th November 2023
Version	4.7.0	**Date for Review**	12 months

Version Control

Version	Status	Commentary	Date	Author
0.A	Draft	Initial Draft (replacing Policy on use of portable computers and storage devices)	11/2014	K Fairbrother
0.B	Draft	Added restrictions on cloud backup and blocked Apps. Add Appendix 3.	11/2014	M Parsons J Jordan D Muir
0.C	Draft	Various grammatical/spelling changes. Minor sentence changes to improve clarity. Some duplication removed.	14/11/2014	D Muir
1.0	Live	HBL ICT SMT Approval	27/11/2014	HBL ICT SMT
1.1	Live	HBL ICT SMT Approval . Format change	2/10/2015	HBLICT
1.1.1	Draft	Annual review, initial template change	16/8/2016	A McLaren
1.1.2	Draft	Review GC, KF Replace Trust with Partner, update job roles, consistency in ICT Department through document, update Acronyms	23/8/2016	A McLaren
1.1.3	Draft	Update Appendix Devices	27/9/2016	N Ketcher, J Jordan
2.0	Live	Authorized by SMT	3/10/2016	HBLIT SMT
2.1	Draft	Update Security and Care	03/2017	M Parmar
2.1.1	Draft	Update Security and Care, GDPR	11/2017	A McLaren
3.0.0	Live	Sign off by P Turnock	29/11/2017	A McLaren

3.0.1	Draft	2.0, 3.1, 3.3, amendment to devices in scope including Appendix A	13/09/2018	M Parmar
4.0.0	Live	Signed off by SMT	27/11/2018	A McLaren
4.1.0	Live	Updated to remove examples from appendix. Authorised by P Turnock	6/12/2018	A McLaren
4.1.1	Draft	Remove Password section which is stated within Information Security Policy Inclusion of DPO as sign off References, capitalisation updated	Aug 2019	A McLaren
4.2.0	Live	Authorised by S Carey	16/8/2019	A McLaren
4.2.1	Draft	Annual review Update to equipment lists within Appendix; job titles; Replace “Partner” with “Organisation” for consistency with other policies. Reference documentation to include Home Working Policy	August 2020	A McLaren, K Fairbrother
4.3.0	Live	Authorised by SMT	1/9/2020	A McLaren
4.3.1	Draft	Update to Implementation plan replacing IG Toolkit with DSPT and the updated training level 1	Oct 2020	A McLaren
4.4.0	Live	Authorised by SMT	3/11/2020	A McLaren
4.4.1	Draft	Annual updates – change to job titles, dept names within HBL ICT	Nov 2021	A McLaren
4.5.0	Live	Authorised by SMT	16/11/2021	A McLaren
4.5.1	Draft	Document template/format updated CCG references updated to ICB HBL ICT Department names updated Internal References – document names updated. Inclusion of Flexible Working Policy External legislation – Reference to EU legislation removed. GDPR changed to UKGDPR Device appendix updated	Oct 2022	S Hassall, J Jordan
4.6.0	Live	Approved by HBL ICT SMT	22/11/2022	S Hassall
4.6.1	Draft	Annual review Example device types updated. Windows Phone references removed. Appendix A - Device models updated HWE ICB modifications– Reference to Agile Working Policy included. Frequency of device connection changed to “weekly” in section 4.3	September 2023	J Jordan S Hassall
4.7.0	Live	Authorised by HBL ICT SMT	14/11/2023	S Hassall

Terms and Acronyms

Term	Definition
DH	Department of Health
DPIA	Data Protection Impact Assessment
DSPT	Data Security and Protection Toolkit
DVD	Digital Versatile Disc
EIA	Equalities Impact Assessment
EU	European Union
HDD	Hard Disk Drive
IG	Information Governance
HBL ICT	Hertfordshire, Bedfordshire and Luton ICT Shared Services
ICT Department	For the purposes of this document, the term ICT Department refers to HBL ICT
Mobile Stick/Dongle	This small USB device contains a mobile modem and allows the connected computer to send and receive data using the Mobile Network. Like a mobile phone they are dependent on being in an area with sufficient signal.
PCD	Personal Confidential Data
PCs	Personal Computers
SD	Secure Digital
SIRO	Senior Information Risk Owner
SSD	Solid State Drive
USB	Universal Serial Bus

Implementation Plan

Development and Consultation	Digital Solutions and with Partner organisations Hertfordshire, Bedfordshire and Luton ICT Shared Services (HBL ICT) is committed to the fair treatment of all, regardless of age, colour, disability, ethnicity, gender, gender reassignment, nationality, race, religion or belief, responsibility for dependents, sexual orientation, trade union membership or non-membership, working patterns or any other personal characteristic This policy / procedure will be implemented consistently regardless of any such factors and all will be treated with dignity and respect. To this end, an equality impact assessment has been completed on this policy.
Dissemination	Staff can access this policy via the Intranet and will be notified of new/ revised versions via the staff briefing. This policy will be included in the ICB's Publication Scheme in compliance with the Freedom of Information Act (FOI) 2000
Training	None for this policy specifically
Monitoring	3rd Party Audit, Data Security and Protection Toolkit (DSPT), spot check The Partner via the Information Governance Toolkit provides the means by which the NHS and Organisation can assess our compliance with current legislation, Government and National guidance.
Review	The policy will be reviewed annually
Equality, Diversity and Privacy	Completed separately

References

External : Legislation, Guidance and Standards	♦ All applicable UK Laws including but not limited to: ▪ Data Protection Act (2018) & UK General Data Protection Regulation (2018) ▪ Health and Safety at Work and Personal Safety ▪ NHS wide Counter Fraud service policies and procedures ▪ UK Law with regard to usage of mobiles in Vehicles ♦ Department of Health (DH) and NHS Regulations and Guidance including but not limited to: ▪ Data Security and Protection Toolkit (DSPT) ▪ DH Information Security Management: NHS Code of Practice (2007)
Internal : Related Documentation	♦ Information Security Policy ♦ Acceptable Use Policy ♦ Telecoms Policy ▪ Records Management & Information Lifecycle Management Policy (which includes Data Quality) (HWE ICB) ♦ Information Governance Framework ♦ Management of Records Policy and Procedure ♦ Data Quality Policy ♦ Incident Policy ♦ Confidentiality Policy ♦ Health and Safety at Work and Personal Safety ♦ Standing Financial Instructions ♦ Flexible Working Policy (HWE ICB) ♦ Agile working Policy (HWE ICB)
Enclosures	none

Contents

1 Executive Summary

This policy sets out the Organisation's position on the use of mobile devices in order to minimise the risks of unauthorised disclosure, modification, removal or destruction of the Organisation's information assets.

The term 'mobile device' includes but is not limited to the following:

- Mobile computer devices including:
  - Laptops, tablets, smartphones, wearable technology (e.g. smart watches)
  - Any other 'mobile' computer device which has the potential to store Personal Confidential Data (PCD).
- Mobile Storage devices including:
  - Digital cameras, digital dictaphones, secure digital (SD) cards
  - External USB devices (stick), external hard disk drives (HDD)
  - Any other externally connected device which has the potential to store PCD.

Mobile Computer/Storage Devices issued to staff by the organisation and in their possession are the property of the Organisation. Equipment is supplied for official Organisation business and must not be used for any personal purpose.

Requirements are stricter than for office-located devices because of the much greater risk of loss or damage to the Organisation's information and property.

Any mobile device issued by the Organisation to any member of its staff must only be used in accordance with the organisation's policies and procedures. The device is the responsibility of the assigned user, who is personally responsible for its care. Failure to comply with the Organisation's policies and procedures or to comply with the guidance in this document could result in disciplinary action and legal proceedings.

Application of the policy will assist in compliance with the Organisation's *Information Security Policy*, information related legislation, Information Security Management: NHS Code of Practice or NHS DSPT.

2 Introduction

The Organisation works to a framework for handling personal information in a confidential and secure manner to meet ethical and quality standards. This enables National Health Service organisations in England and individuals working within them to ensure personal information is dealt with legally, securely, effectively and efficiently to deliver the best possible care to patients and clients.

3 Scope

This policy covers but is not limited to:

- All mobile computer/storage devices that are in use on any information system owned or operated by the Organisation
- Any mobile computer/storage device used to store or process any information belonging to the Organisation

Examples of mobile computer/storage devices include:

- Laptop/Ultrabook (HP, Lenovo, Dell)
- Tablets (Apple iPad, Samsung Galaxy Tab, Microsoft Surface Pro)
- Smartphones (Apple iPhone, Samsung Android Devices)
- Wearable technology
- Digital cameras
- Digital dictaphones
- External Memory devices (SD) cards
- External USB devices (Stick, HDD)
- External Hard Disk Drives (Solid State Drives (SSD), iPod, MP3 Player)
- Magnetic Storage:
  - Cassette Tape
  - Floppy Disk
- Optical Storage:
  - Compact disc (CD)
  - MiniDisc (MD)
  - Digital Versatile Disc (DVD)
  - High Definition DVD (HD DVD)
  - Blu-ray Disc (BD)

All other permutations will need written approval from the ICT Department Associate Director of Digital Solutions and Organisation's Senior Information Risk Owner (SIRO), Information Governance (IG) Lead or Data Protection Officer (DPO). For example: an external training provider/consultant who requires access to an Organisation computer to deliver training material/presentations by use of an external USB device.

For a comprehensive list of supported mobile computer/storage devices see *Appendix* or the ICT Department.

4 Responsibilities

4.1 Authority for Use

- Each business unit will identify its business requirements for the use of mobile computer/storage devices and the number of devices needed to satisfy those requirements. These requirements will be reviewed periodically by the business unit.

- Mobile computer/storage devices must only be used when there is a clear and documented business requirement that has been approved at the appropriate level within the Organisation (see *Appendix*). The use of removable media by subcontractors or temporary workers must be risk assessed and be specifically authorised by the organisation.
- Staff and contractors must not use any mobile computer/storage device that has not been provided by, or explicitly approved by, the Organisation. Approved devices will be appropriately identified and a central register of devices issued will be maintained. A local register of devices in use must also be maintained.
- Mobile computer/storage devices will be supplied (and/or approved) by the ICT Department when requested by the responsible authority level within the Organisation (see *Appendix*) and when there is no suitable alternative method of meeting the business requirement.
- All bulk data extracts and transfers of person-identifiable or other confidential information using a mobile computer/storage device must be authorised by the Organisation's SIRO / IG Lead / or DPO who must also ensure that a record is maintained of all such extracts and transfers.
- The Organisation's Caldicott Guardian must also approve bulk extracts and transfers containing person-identifiable information relating to patients.
- The security level and configuration of mobile computer/storage devices will be specified by the ICT Department's Associate Director of Digital Solutions in consultation with the Organisation's Information Governance Lead or DPO and will be installed, configured and maintained by the ICT Department.
- The use of any mobile computer/storage devices may be restricted or blocked if the ICT Department's Associate Director of Digital Solutions or the Organisation's Information Governance Lead or DPO considers:
  - They create an unnecessary risk to the Organisation's information assets.
  - There is a breach, or potential breach, of the Organisation's policies or the NHS DSPT
- Individuals are responsible for their own devices
- Managers are responsible for the day-to-day management and oversight of mobile computer/storage devices used within their work areas to ensure the Organisation's policies and guidance are followed. This will include:
  - Ensuring devices that have not been allocated or are not currently in use are stored securely.
  - Maintaining a record of mobile computer/storage devices within their area of responsibility, the staff who have been authorised to use them and the devices allocated to those staff. For example: asset number, device, employee name, storage location and date of allocation.
  - Ensuring that devices are only used for the purposes and business requirements for which they were supplied.
- Members of staff who have been authorised to use mobile computer/storage devices for the purposes of their job roles are responsible for the secure use of those removable media as required by the Organisation's policies and guidance.

4.2 Security and Care

- Only authorised and approved mobile computer/storage devices can be used within the organisation. Requests for additional devices must be made in writing to the ICT Department's Associate Director of Digital Solutions and the Organisation's IG Lead or DPO for review and approval.
- PCD must not be stored on any device that is not approved for this purpose. Approved devices will have additional safeguards to protect their contents
- Mobile computer/storage devices must only be used to store, transfer and share NHS information for the agreed business purpose. When that business purpose has been satisfied the devices must be returned for re-use or recycling as appropriate.
- The information on mobile computer/storage devices must be a copy of information that is held securely elsewhere. These devices must not be used to hold the only, or the primary, copy of information.
- A record must be kept of the data on each mobile computer/storage device. The devices must be physically protected against their loss, damage, abuse or misuse when in use, when stored and when in transit.
  - Devices should be stored appropriately (e.g. in the protective case where supplied for laptops, tablets and smartphones, etc.) when not in use.
  - In public places, computers and protective cases should be as understated as possible. Smaller devices (smartphones, etc.) should be located securely in another bag or in an inside pocket.
  - Ensure devices are handled carefully to avoid being dropped or damaged in any way. Protect from direct sunlight, excess heat and moisture/rain.
  - Where relevant, any security locks or alarms supplied must be attached and activated when devices are unattended.
  - Any unattended device, even in your own home, should be secured against unauthorised access.
  - Devices must not be left in cars overnight or any other location where there is a risk of theft or damage.
  - Peripherals and accessories provided by the Organisation must not be used on any other device or computer. Only peripherals and accessories supplied by the Organisation may be used on Organisation issued devices whilst they are connected to the network.
  - Do not allow any unauthorised person to use an Organisation issued device; this includes patients/service users, family and friends.
- All incidents involving theft or malicious damage of a mobile computer/storage device must be notified to the ICT Department's Service Desk immediately. The police must be notified if the incident occurred away from Organisation premises. On Organisation premises, the senior or site manager must be informed. The Finance Department must be notified in accordance with the Losses and Compensation procedures documented in *Organisation Standing Financial Instructions*.
- All incidents involving the use, loss or damage of any mobile computer/storage device must be reported immediately in accordance with the Organisation's incident reporting procedures.

- Android phones will be deployed with Anti-Virus software
- Anti-Virus software is not required to be installed on an iPhone or iPad. The reason for this is that iOS is designed and built to only accept and install software that has been approved by Apple and run through the App store states that it "designed the iOS platform with security at its core. Keeping information secure on mobile devices is critical for any user, whether they're accessing corporate and customer information or storing personal photos, banking information, and addresses. Because every user's information is important, iOS devices are built to maintain a high level of security without compromising the user experience."

4.3 Mobile Computer Devices

The device will be configured for the purpose it is to be used and all the necessary software will be installed. Any changes to the configuration and/or installation of additional software will be performed by the ICT Department. Requests should be made through the ICT Department's Service Desk. **Do not** attempt to make any changes yourself.

To ensure that corporate mobile devices are used appropriately this policy includes certain constraints, such as:

- Anti-virus software must be installed on all Android devices. To ensure that this restriction is adhered to the device will cease to download any emails or offer access to corporate information should the anti-virus be missing, disabled or removed.
- Each organisation has a pre-approved list of applications (safe list) that can be downloaded to the smart device from the corporate store. Access to standard Google Play applications is barred due to the inherent security vulnerabilities. Any software that is required for business purposes and is not currently in this list must be requested via the appropriate process.
- All Android and Apple mobile phones issued by the ICT department and configured according to the setup guides are securely encrypted.

You must safeguard all information on the mobile computer device from loss, damage, corruption and unauthorised access or disclosure.

- Backup the data on the Mobile Computer Device regularly to the network.
- Keep back-up copies of data safely and separately from the mobile computer device.
- Do not use the mobile computer device in a public place where the screen can be observed.
- Do not use unapproved cloud-based backup, storage or data sharing solutions (see *Appendix*).

You must have the express permission from your Department Manager or other Organisation authority (see *Appendix*) to store or process any confidential or sensitive information on the mobile computer device, particularly if this is personal data about patients, staff, etc.

You must also have the express permission of the Caldicott Guardian if any of the personal data relates to Patients, Service Users or Clients. Any conditions as to the scope and content of the information and to time periods must be strictly observed.

All mobile computer devices that may be used to store or process personal data must have special data encryption software installed. This will either be supplied with the computer or can be installed retrospectively by the ICT Department. Please contact the ICT Department's Service Desk accordingly.

Tablet and smartphone devices that will be used to access Organisation resources (e-mail, Intranet, documents) must be provisioned with an appropriate Mobile Device Management (MDM) platform. This is to ensure that the appropriate level of security is active to comply with the DSPT.

Some mobile computer devices are used as a shared resource amongst a group of staff. Where this happens there must be a clear and up-to-date record of the current holder of the device.

Any unauthorised person must not use Organisation mobile computer devices. These are principally people not employed by the Organisation: patients, family, friends etc., but may include colleagues particularly if they are not part of the same workgroup or they should not have access to sensitive or confidential information on the mobile computer device.

The mobile computer device will be supplied with virus protection software installed. Virus protection must remain active at all times and not disabled, bypassed or removed.

Members of staff are responsible for ensuring that security software (Anti-Virus, Anti-Malware, Firewall and Operating System updates) is maintained and kept up-to-date. Most mobile computer devices will update automatically when connected to the Organisation's network. Staff must connect their mobile computer device to the Organisation network at least weekly to update the security software in addition to exercising vigilance and good practice to keep the mobile computer device free of malicious software. In particular:

- Check regularly for security updates to Windows (Tools/Windows Update in Internet Explorer).
- Do not open suspicious e-mails and do not open attachments you don't recognise.
- Do not download programs or executable files from the internet; including screen savers.

- Remote access using Strong Authentication Token can be arranged if you need to use the Organisation's network services, such as e-mail, when you are away from the office. This will also provide remote Internet access. Requests for remote access should be made by completing the appropriate forms available from via the ICT Department's Service Desk. Instructions for the use of Strong Authentication Token will be supplied as part of the installation process.
- Mobile computer devices must not be connected to broadband or internet services unless you have been authorised and issued with the appropriate Strong Authentication Token. The connection must be made using the network cable provided or via a wireless connection which utilises WPA2 encryption as a minimum security standard.
- Connections should not be made to public or proprietary wireless networks that do not utilise WPA2 encryption (this includes but not limited to Internet cafes and public Wi-Fi hotspots). It is strictly forbidden to connect to the internet or other online services except through the Strong Authentication Token service provided or unless given written permission to do so by an approved authority (*Appendix*).

5 Requests for New Devices

All requests for mobile computer/storage devices should be made to the ICT Department's Service Desk. Requests for mobile storage devices must be supported by a business requirement with the appropriate level of authorisation (see *Appendix*). Devices will not be issued until the ICT Department's Associate Director of Digital Solutions and/or the Organisation's IG Lead or DPO has approved the request.

Devices will be issued to a named individual who will be responsible for its safekeeping and appropriate use. All devices that can be encrypted or password protected will be issued with the protection already in place. Instructions for use will be supplied.

All mobile computer/storage devices will be tagged and must be made available whenever a reasonable request is made to inspect or audit the device.

Appendix A. Supported Mobile Computer/Storage Devices

The list below is the current supported environment at the point of writing. Due to the rapid development of technology and devices, this list is liable to change. For an updated list of available and supported devices please refer to ICT Department.

1. Laptop Devices

Supported Devices (Laptop)	Supported OS
HP , Laptop, EliteBook, 640 G10 HP , Laptop, EliteBook, 650 G10 HP, Tablet, Folio, Dragonfly G3 Lenovo, Tablet, ThinkPad, L13 Yoga G3 Lenovo, Laptop, ThinkPad, T16 G1 Lenovo, Laptop, ThinkPad, P16S G2 HP , Laptop, EliteBook, 640 G9 HP , Laptop, EliteBook, 840 G9 HP , Laptop, EliteBook, 650 G9 Lenovo, Tablet, ThinkPad, X13 Yoga G2 Lenovo, Tablet, ThinkPad, X12 Detach G1 Lenovo, Laptop, ThinkPad, T15 G2 HP , Tablet, EliteBook, X2 G8 Detach HP, Laptop, EliteBook, 840 G8 HP, Laptop, ZBook, Firefly G8 HP, Laptop, ZBook, Studio G8 HP, Tablet, EliteBook, Dragonfly G2 HP, Laptop, ProBook, 650 G8 Lenovo, Laptop, ThinkPad, T15 G1 Lenovo, Tablet, ThinkPad, X13 Yoga G1 Lenovo, Tablet, ThinkPad, X1 G3 HP, Tablet, EliteBook, Dragonfly G1 HP, Laptop, EliteBook, 840 G7	Windows 10 Enterprise 64-bit Windows 11 Enterprise 64-bit

2. Tablets

Supported Apple iPads	Supported iOS
Apple iPad Pro with Wi-Fi + Cellular (11-inch, 1st generation) (64 GB Space Gray) Apple iPad Pro with Wi-Fi + Cellular (9.7-inch, 1st generation) (32 GB Space Gray) Apple iPad Pro with Wi-Fi + Cellular (12.9-inch, 6th generation) (256 GB Space Gray) (Global) Apple iPad with Wi-Fi (10.2-inch, 9th generation) (64 GB Space Gray) Apple iPad Air LTE (9.7-inch, 1st generation) (16 GB Silver) Apple iPad with Wi-Fi + Cellular (10.2-inch, 8th generation) (128 GB Space Gray) Apple iPad with Wi-Fi + Cellular (10.2-inch, 9th generation) (64 GB Silver) (Global) Apple iPad (5th generation)	12.4.8 and above
Supported Samsung Tabets	**Supported OS**
Galaxy Tab A 10.1 Galaxy Tab A 10.1 (2019)	
Supported Microsoft Tablets	**Supported OS**
Surface Hub 2S	Windows 10 22H2

3. Smart Phones

Supported Apple iPhones	Supported iOS
Apple iPhone 6s Apple iPhone 6s (128 GB Space Gray) Apple iPhone 7 (32 GB Black) Apple iPhone 7 (32 GB Rose Gold) Apple iPhone 11 Apple iPhone 12 (128 GB Black) Apple iPhone 12 (256 GB White) Apple iPhone 12 Pro Max (128 GB Graphite) Apple iPhone 13 (128 GB Midnight) Apple iPhone 14 Apple iPhone 14 Pro Max Apple iPhone SE Apple iPhone SE (32 GB Space Gray) Apple iPhone SE (2nd generation)	, 12.4.8 and above

Apple iPhone SE (3rd generation) (64 GB Midnight) Apple iPhone XR (128 GB Black)	
Supported Samsung Android Phones	**Supported OS**
Samsung SM-G525F Samsung SM-J330FN Samsung SM-J415FN Samsung SM-A202F Samsung SM-A505FN Samsung SM-T736B Samsung SM-T636B Samsung SM-F926B Samsung SM-A217F Samsung SM-F916B Samsung SM-X205 Samsung SM-J530F Samsung SM-A336B Samsung SM-G398FN Samsung SM-G390F Samsung SM-T636B Samsung SM-X205 Samsung SM-F926B Samsung SM-G525F Samsung SM-T736B Samsung SM-A105FN Samsung SM-A236B	9.0 and above

4. Wearable Technology

- None confirmed to date

5. Digital Cameras

- Canon
- Flip Video Camcorder (Flip Video Camcorder USB Device)

6. Digital Dictaphones

- Olympus DS 7000/9000 voice recorder
- Olympus Digital Dictator (OLYMPUS DVR USB Device)
- Olympus Digital Dictator (OLYMPUS DVR DM SERIES USB Device)

7. External Memory Drives

- SD Cards for use in Digital Cameras and Digital Dictaphones

8. External USB Devices

- Integral Courier (Integral Courier TL USB Device)
- Integral Courier (Integral Courier FIPS 197 USB Device)
- Integral Courier (Integral Crypto USB Device)
- Kingston Data Traveller (Kingston DTVault Privacy USB Device)
- Kingston Data Traveller (Kingston DTVaultPrivacy30 USB Device)
- diskGenie (diskGenie USB Device)
- MXI (MXI Private USB Device)
- SafeStick (BM SafeStick BE USB Device)
- SafeXS (Ctwo SafeXs USB Device)
- SanDisk (SanDisk Enterprise USB Device)
- SanDisk (SanDisk Enterprise FIPS USB Device)
- O2 Mobile Broadband Dongle (ZTE MMC Storage USB Device)
- O2 Mobile Broadband Dongle (CWID USB SCSI CD-ROM USB Device)
- One Touch Mobile Broadband Dongle (ONETOUCH SUZUKA USB Device)
- One Touch Mobile Broadband Dongle (ZTE MMC USB Device)
- Thera Trainer (USB2.0 Flash Disk USB Device)
- RBA HCC RAS (USB Flash Disk USB Device)
- RBA HCC RAS (SMI USB DISK USB Device)

9. External Hard Disk Drives (SSD, iPod, MP3 Player)

- Western Digital My Passport Drives (Additional Authorisation Required)

Appendix B. Authority Levels

The list below is the approved authority levels as described within the policy.

- Director
- Assistant Director
- Associate Director
- General Manager
- Locality Manager
- Head of Service
- SIRO
- Caldicott Guardian
- DPO
- IG Manager

Appendix C. Prohibited Mobile Device Applications

For an updated list of prohibited applications please contact HBL ICT Service Desk

Appendix A. Comment Form

As part of HBL ICT Services Department continuous improvement regime, would you please complete this form. Any comments or feedback on this document should be addressed to the Owner. Please provide your name and contact details in case clarification is required.

Name Click here to enter text.

Address Click here to enter text.

Click here to enter text.

Phone Click here to enter text.

Email Click here to enter text.

Please return to:

HBL ICT Services
Charter House
Welwyn Garden City
Hertfordshire, AL8 6JL

Please confirm the document you want to give response to as:

HBL ICT Policy/Procedure: Click here to enter text.

Please rate the document using the topics and criteria indicated below:

	Very Good	Good	Average	Fair	Poor
Format and Layout	□	□	□	□	□
Accuracy	□	□	□	□	□
Clarity	□	□	□	□	□
Illustrations (tables, figures etc.)	□	□	□	□	□

When using the document, what were you looking for?

Click here to enter text.

How could the document be improved?

Click here to enter text.

How often do you use the document?

Click here to enter text.

If you have additional comments, please include them below:

Click here to enter text.

Thank you for your time.