Policy Document

Reference: IT14

University Hospitals of North Midlands NHS Trust

Trust Mobile Devices and Remote Working including Removable Devices

Version:	**2.1**
Date Ratified:	**June 2022 by Executive Digital and Data Security & Protection Group**
Minor Amends:	**August 2024**
To Be Reviewed Before:	**June 2025**
Policy Author:	**Cyber Lead**
Executive Lead:	**SIRO**

Version Control Schedule

Version	Issue Date	Comments
1	March 2021	New Policy to support DSP toolkit
2	June 2022	No Changes
2.1	August 2024	Added Section 9

Statement on Trust Policies

The latest version of 'Statement on Trust Policies' applies to this policy and can be accessed here

NHS
University Hospitals of North Midlands
NHS Trust

Review Form / Equality Impact Assessment (EIA)

The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. The Equality Impact Analysis Form is designed to help consider the needs and assess the impact of each policy. To this end, EIAs will be undertaken for all policies.

Policy Reference, Title and Version Number	IT14 Trust Mobile Devices and Remote Working including Removable Devices V2
Summary of changes made on this review	No changes.
Please list which service users, staff or other groups have been consulted with, in relation to this	CSOG
Were any amendments made as a result? If yes, please specify	No
Does this policy involve the administration or control of medicines? If yes, have the Safe Meds Group been consulted with?	N/A
Which Executive Director has been consulted on?	Director of Digital Transformation
Does this policy have the potential to affect any of the groups listed below differently - please complete the below. Prompts for consideration are provided, but are not an exhaustive list	

Group	Is there a potential to impact on the group? (Yes/No/Unsure)	Please explain and give examples	Actions taken to mitigate negative impact
Age (e.g. are specific age groups excluded? Would the same process affect age groups in different ways?)	No		
Gender (e.g. is gender neutral language used in the way the policy or information leaflet is written?)	No		
Race (e.g. any specific needs identified for certain groups such as dress, diet, individual care needs? Are interpretation and translation services required and do staff know how to book these?)	No		
Religion & Belief (e.g. Jehovah Witness stance on blood transfusions; dietary needs that may conflict with medication offered)	No		
Sexual orientation (e.g. is inclusive language used? Are there different access/prevalence rates?)	No		
Pregnancy & Maternity (e.g. are procedures suitable for pregnant and/or breastfeeding women?)			
Marital status/civil partnership	No		

Group	Is there a potential to impact on the group? (Yes/No/Unsure)	Please explain and give examples	Actions taken to mitigate negative impact
(E.g. would there be any difference because the individual is/is not married/in a civil partnership?)			
Gender Reassignment (E.g. are there particular tests related to gender? Is confidentiality of the patient or staff member maintained?)	No		
Human Rights (E.g. Does it uphold the principles of Fairness, Respect, Equality, Dignity and Autonomy?)	No		
Carers (E.g. is sufficient notice built in so can take time off work to attend appointment?)	No		
Socio/economic (E.g. would there be any requirement or expectation that may not be able to be met by those on low or limited income, such as costs incurred?)	No		
Disability (E.g. are information/questionnaires/consent forms available in different formats upon request? Are waiting areas suitable?) Includes hearing and/or visual impairments, physical disability, neurodevelopmental impairments e.g. autism, mental health conditions, and long term conditions e.g. cancer.	No		
Are there any adjustments that need to be made to ensure that people with disabilities have the same access to and outcomes from the service or employment activities as those without disabilities? (e.g. allow extra time for appointments, allow advocates to be present in the room, having access to visual aids, removing requirement to wait in unsuitable environments, etc.)			**Yes/No**
			No
Will this policy require a full impact assessment and action plan? (a full impact assessment will be required if you are unsure of the potential to affect a group differently, or if you believe there is a potential for it to affect a group differently and do not know how to mitigate against this - please contact the Corporate Governance Department for further information)			**Yes/No**
			No

CONTENTS **Page**

1. INTRODUCTION

The Trust aims to take advantage of the many benefits offered by portable computing technology and enabling the workforce to be mobile and flexible as part of the overall Trust strategy. Along with the obvious advantages of using portable computing devices there are also additional risks which must be effectively managed to protect the Trust, its staff, patients and the services and data on which they rely, against known and emerging threats.

Within the context of the NHS, mobile computing is a term used to describe the use of mobile devices that process NHS data. Typically this will include items such as laptops, memory sticks, tablets, mobile email devices and mobile telephones and tablets.

Any user of a portable computing device used to store and/or process Trust information must comply with this policy. Given the confidential nature of much of the information held by the Trust, it is essential that robust information security arrangements are in place where mobile devices are used or where information is accessed from Trust devices which are not located on Trust sites.

This policy provides specific and detailed instructions that must be followed whilst using, transporting and acting as custodian of any Trust procured portable computing or any other portable computing device approved by the IM&T Department for use within the Trust business environment. It describes what information can be stored and processed on portable computing and how Personal and Non-personal information must be protected physically and/or electronically.

The purpose of this policy is to provide guidance to staff regarding accessing the Trust's information when working from remote locations or using mobile computer equipment.

The aims of this policy are:

- To ensure the Trust complies with its legal obligations.
- To promote the safe and secure use of mobile and remote working equipment in support of the clinical and operational work of the Trust
- To provide a secure working practice for personnel working from home.
- To ensure that IM&T resources provided to staff are not misused and are properly looked after.
- To ensure that the security of computer systems and the information they contain is not compromised in any way.
- To prevent The Trust's reputation from being damaged by the inappropriate or improper use of its information resources

2. SCOPE

- This policy covers users that work on Trust owned portable computing devices and those who use Trust provided remote access technologies to connect from home or other non-Trust machines.
- This policy applies to all full-time and part-time employees including agency staff, students/trainees, and third partied contracted to the Trust.
- The rules contained within this policy and its related materials apply to mobile computing and remote working equipment which are used for the processing of the Trust's information assets of all types.
- Trust information must not be processed on any non-Trust device, other than those operated by an approved partner agency with which the Trust has an approved information sharing agreement.
- On equipment not covered by an approved information agreement, e.g. home personal computer, Trust information may only be processed using the Trust's approved Remote Access technology, in this case, information must never be saved to the local hard drive of the processing device.

3. DEFINITIONS

Mobile devices are those which allow the ability to access and process and transfer information without a direct / hardwired network connection, these include, but are not limited to, the following:

- Laptops

- Removable Media (DVD/CD
- Memory Sticks
- Memory Cards
- External Hard Drives)
- Mobile Phones
- Smartphones
- Tablet Devices
- Personal Digital Assistants (PDA)
- Digital Cameras
- Video Cameras
- Web Cams
- Dictation Devices
- Digipens
- ipods
- E-Readers

Remote Access is the ability using defined technical solutions to access Trust information whilst away from the Trust, this includes access both through Trust issued devices, and, in approved circumstances with personal home computing equipment.

FIPS140-2 Cryptographic module specification
MTP Media Transfer Protocol, for example mobile phones.
PTP Picture Transfer Protocol, for example digital cameras.

4. ROLES AND RESPONSIBILITIES

Trust Board
The Trust Board is ultimately responsible for ensuring the Trust meets its legal responsibilities, and for the adoption of internal and external governance requirements. The Transformation and People Committee will be updated on DSP issues via highlight report.

Senior Information Risk Owner (SIRO)
The Trust SIRO is responsible to the Chief Executive for Data Security & Protection and acts as an advocate for information risk on the Trust Board.

Caldicott Guardian
The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of Personal Identifiable Data (PID). The Caldicott Guardian is responsible for ensuring PID is shared in an appropriate and secure manner.

Head of Data Security & Protection/Data Protection Officer
The Head of Data Security & Protection/Data Protection Officer (DPO) has overall responsibility for managing the data security & protection function and as DPO will advise and monitor compliance with the GDPR and DPA. They are responsible for ensuring effective management, accountability, compliance and assurance for all aspects of the data security & protection agenda. They will also be the first point of contact with the Supervisory Authority – the Information Commissioner's Office.

Information Asset Owners (IAO)
Designated Information Asset Owners (IAOs) are responsible for providing assurance to the SIRO that information risks, within their respective areas of responsibility, are identified and recorded and that controls are in place to mitigate those risks.

Information Asset Administrators (IAA)
Information Asset Owners can appoint Information Asset Administrators (IAAs) to support them in the delivery of their information risk management responsibilities. IAA ensure that policies and procedures

are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date. Where an IAA is not in place, this function is carried out wholly by the IAO.

Data Security & Protection Manager
The Trust's Data Security & Protection Manager is responsible for supporting the Data Protection Officer in the implementation of the Trust's DSP agenda.

Data Security & Protection Facilitator
The Trust's Data Security & Protection Facilitator(s) is responsible for supporting the Data Security & Protection Manager in the delivery of the DSP agenda.

Executive Digital and Data Security & Protection Group (EDDSPG)
The SIRO and Caldicott Guardian are joint chair of the Trust's EDDSPG. This group is responsible for receiving assurances relating to the day to day management of the individual components of the Trust's Data Security & Protection Framework.

Data Security & Protection Operational Group (DSPOG)
The Data Protection Officer chairs the Trust's DSPOG. This group is responsible for overseeing the day to day management of the individual components of the Trust's Data Security & Protection Framework.
The Data Security & Protection Governance pack provides more detail on the make-up of the Groups which provide assurance that the Trust meets its obligations around data security & protection.

Information Security Manager (RA and Privacy)
Provides advice to the Trust, ensuring compliance, and conformance, with local and national requirements, and, generally, on information risk analysis/management incorporating the Privacy Officer role which focuses on ensuring privacy related alerts from electronic systems (e.g. Summary Care Record) are investigated for appropriateness, as well as other privacy compliance work as necessary.

Cyber Security Lead
Provides advice to the Trust, ensuring compliance and conformance, with local and national requirements and, generally, on cyber security issues across the Trust

IM&T Department
- Will ensure that Trust issued portable and mobile devices are encrypted to NHS standards. In exceptional cases where a device cannot be encrypted this must be approved by the Trust Senior Information Risk Officer.
- Provide advice on implementation of this policy as requested.
- Ensure that User access rights are correctly implemented
- Ensure that the asset details for all portable and mobile devices are kept up to date.
- Ensure that all relevant software licences are procured and installed.

Assistant Director of Human Resources/Governance Lead
Has responsibility for ensuring that the HR function meets the legislated requirements of the Data Protection Act 2018 in terms of security of information and access to records by staff (both current and former).

Managers of staff with mobile devices are responsible for:
- Ensuring that all staff allocated mobile IM&T equipment have a genuine need for mobile computing and that if authorised to work at home, all other staff regulations are met e.g. Health and Safety requirements.
- Ensuring that the risks associated with the particular work styles adopted by their staff are adequately assessed and that, where necessary, suitable arrangements are put into place to minimise those risks.
- Ensuring that their staffs receive sufficient information and training to assist them with identifying and assessing the risks associated with their work activities and to know how they can carry out their work without putting themselves or others at risk.

- Ensuring that where devices are used in a shared environment it is registered against a single responsible owner and a formal handover process is in place to record device usage at any given time.
- Ensure all staff complies with this policy and associated procedures;
- Ensure they take disciplinary action as appropriate against any member of staff in breach of this policy
- Notifying any suspected breaches of this policy to the IM&T Department;
- Ensure all Trust devices and supporting media are returned by owners leaving the Trust or no longer requiring them;
- Ensure measures are in place to appropriately maintain and protect mobile devices and promptly report any technical issues or damages to IM&T.

All Staff
All staff, via job roles and contracts of employment/professional registrations must comply with specific data security related legal and ethical obligations and therefore must be aware of the related standards which impact within their area of responsibility. Individual staff must ensure that they make themselves aware of all policies and associated Standard Operation Procedures referenced in this document and abide by their contents. Any personal and corporate information, is managed legally, securely, and efficiently in order to assist in the delivery of the best possible care/practice. Staff can email the Data Security & Protection team on DSPUHNM@uhnm.nhs.uk with any data security related queries.

Transformation and People Committee
The Transformation and People Committee is the Board Sub-Committee responsible for receiving assurances, on behalf of the Trust Board, that the day to day management of the individual components of the Trust's Data Security & Protection Framework are appropriate and fit for purpose.

5. MOBILE COMPUTING

All users of mobile devices are required to use them in accordance with this policy, IT02 and SOP IT14 (S1)

IM&T will ensure mobile devices are configured and monitored in line with IT13 (S2).

Mobile Device Security
Portable devices such as laptops or tablets are highly desirable items with many being stolen from vehicles or by being left in places unattended. It is a user's responsibility to ensure these are kept secure at all times.

Removable Media Devices
All removable media devices must be encrypted to NHS Digital standards and managed in line with SOP IT14 (S1)

Removable Media Security Auditing and Management
Removable media will be controlled by SOPHOS console with only approved devices being white listed.

Mobile Phones & tablet devices – Mobile device management (MDM)
All Trust issued mobile phones and tablet devices will be managed by the Trust mobile device management solution (MDM)

Digital Cameras, Video Cameras and Web Cams
All camera and video devices must only be used in line with the Trust photographic policy RE02

Dictation Devices
Managed in line with SOP IT14 (S1)

Exceptions to the above

There are circumstances where the pattern of usage prohibits the operation of some of the above controls. In these cases, the owner of the device may apply to the Data Security and Protection team.

Loss or Theft or Criminal Damage of Mobile Devices
Loss of theft of any devices must be reported in line with Trust incident management procedures.

Passwords & PIN Codes
All mobile devices must use passcodes or pin codes as an additional layer of security.

Storage of Data & Backups
Users of these devices are responsible for ensuring their data is backed up to network drives as appropriate and only kept for a minimum time necessary

Protection of Sensitive and confidential data / Encryption
Where departments or individuals process, or identify a new requirement to process, sensitive or confidential data on portable / mobile devices they must contact DSP team for advice DSPUHNM@uhnm.nhs.uk

Return of Devices
When no longer required all devices must be returned to IM&T by logging a job with the service desk and arranging collection of device

Wireless Connections
Trust devices must use current approved Wi-Fi technologies and should not be connected to public WiFi. If non approved devices are connected then these will be blocked by the network.

6. WORKING WITH REMOTE ACCESS TO TRUST SYSTEMS AND DATA

Remote Access
Remote access to the Trust network can only be made through approved secure technologies – requests should be logged through IM&T service desk and will require management approval.

Handling of information
Users are responsible for ensuring that any data they have access to remotely is kept secure at all times, see IT02 & SOP IT14(S)1 for full details.

Monitoring Usage/Audit
The IM&T service delivery team monitor the contents of files stored on Trust Devices, along with access to Trust networks.

Security of trust devices outside the Trust
Laptop computers and other mobile devices are a prime target for theft because they can be easily snatched. In addition any documentation also needs to be protected for theft or loss. All reasonable measures should be taken by staff to protect Trust IT assets and Trust data whether electronic or paper. This applies in transit and in the home/remote work place.

Additional guidance
Comprehensive guidance can be found in SOP IT14 (S1) in relation to both using mobile devices and working remotely.

7. EDUCATION/TRAINING AND PLAN OF IMPLEMENTATION

Mandatory Data Security & Protection training for all staff (whether permanent, temporary or contracted) is included in the Trusts statutory and mandatory training requirements.

All staff will receive training on commencement (Induction) and thereafter the training must be completed via the Trust's on-line e-learning portal on a yearly basis as per the requirements of the Statutory and

Mandatory Training Policy (HR53) and Corporate Induction Policy (HR17) as well as the Trust's User Awareness Policy.

Staff that require enhanced/specialised DSP training for their role will be identified on an annual basis and required to also achieve this training requirement. The Trust's Training Needs Analysis can be found at Appendix 1 of policy DSP18.

In accordance with the Training Needs Analysis in Trust Policy HR53 Statutory and Mandatory Training, all staff have an individual responsibility to ensure that they undertake mandatory Data Security & Protection training. All training should be recorded within staff personal record, ideally in ESR. The Statutory & Mandatory Training module will be reviewed on an annual basis by the Data Security & Protection Operational Group to ensure that it is current and up to date and meets the requirements set by NHS Digital.

8. MONITORING AND REVIEW ARRANGEMENTS

8.1 Monitoring Arrangements

IM&T technical teams and service delivery teams will undertake routine monitoring of the Trusts IT systems, who will use a variety of monitoring tools both automated and manual, this includes but is not limited to;

- Web Filtering Services to record and monitor web sites visited (live time)
- Mail content filtering to block certain file types (live time)
- Antivirus software to monitor for virus's and malware (live time)
- Ad hoc Audits of access to, and permissions to Trust Systems
- Ad hoc audits of file types stored on Trust network storage
- Monthly audits of unused domain accounts
- Network monitoring tools (live time)

All monitoring and investigation work will be carried out in accordance with HR01

All remote connections to the Trust are logged, with relevant technologies in place to prevent unauthorised connections.

Investigations/Disciplinary Proceedings

- Breaches of this or other IM&T policies will result in disciplinary action being instigated.
- In the event of a requirement to investigate user activity or disciplinary proceedings being conducted, the DSP Team will gather and make available all appropriate information from various sources to assist the investigator(s);

8.2 Review

This policy will be assessed against the NHS Digital information governance and security requirements (Data Security & Protection Toolkit) and alongside the DSP Governance Pack to assure the Trust that full DSP requirements are being met

9. PROTECTING NETWORKED NON INTERNET DEVICES

These are devices that are connected to your network (but not the internet) either because they are legacy systems, medical devices or untrusted systems that cannot be patched.

UHNM will protect our systems and wider network by applying the following techniques

9.1 Protection techniques

Network separation (such as VLANs), Deny access lists, Virtualisation, Sandboxing, Separate Firewall rules and non-routable subnets.

9.2 Obsolete Status

Devices which can't be managed by the above methods will be considered obsolete and therefore, unmanaged or untrusted.

It is important to note that systems being restricted in this way may not perform as intended and it is vital that UHNM departments and suppliers keep systems accessible, and patched as described in UHNM Policy IT15 and IT18.

10. REFERENCES

The Trust is obliged to comply with all relevant UK legislation. Some requirement to comply with this legislation will be devolved to employees and agents of the Trust, who then may be held personally accountable for any breaches of security.

The Trust will comply with legislation as appropriate including:

- The Data Protection Act 2018 (including the relevant specific codes of practice e.g.
- Employment Practices & CCTV) Freedom of Information Act 2000 (FOIA)
- The Computer Misuse Act 1990
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Health & Social Care Act 2000
- Children Act 2004
- Public Interest Disclosure Act 1998;
- Audit & Internal Control Act 1987;
- Public Health (Code of Practice) Act 1984;
- NHS (VD) Regulations 1974;
- National Health Service Act 1977;
- Human Fertilisation & Embryology Act 1990;
- Abortion Regulations 1991;
- Prevention of Terrorism (Temporary Provisions) Act 1989;
- Regulations under Health & Safety at Work Act 1974.
- Copyright, Designs and Patents Act, 1988 (as amended by the Copyright
- (Computer Programs) Regulations, 1992;
- Crime and Disorder Act, 1998;
- NHS Digital Data Standards
- RE02 Clinical Photographic and video Policy
- HR01 Disciplinary Policy
- SOP- IT14 (S1) Remote working