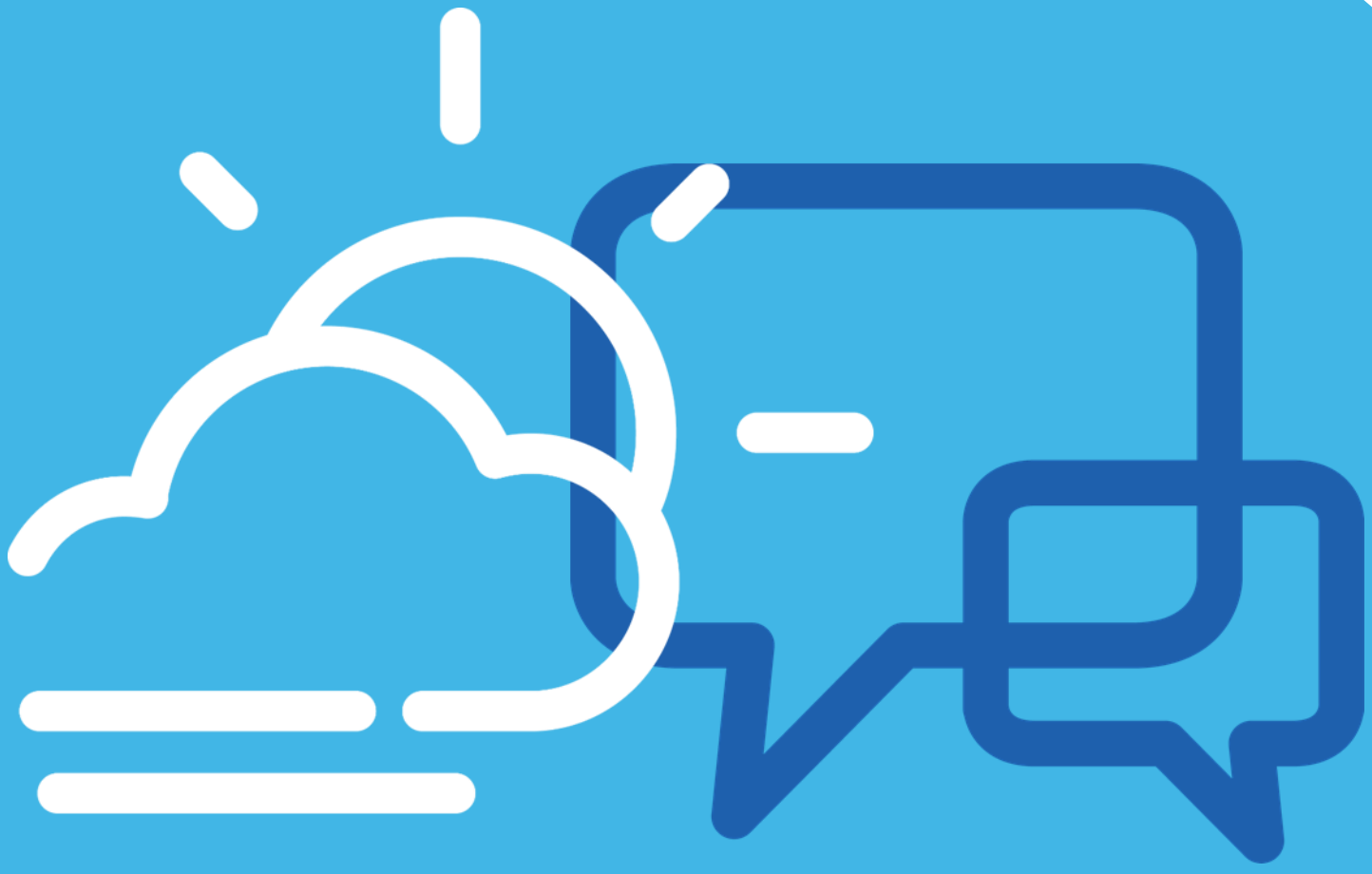
NHS
Greater Manchester Mental Health
NHS Foundation Trust

Mobile Media Security Policy

Greater Manchester Mental Health NHS Foundation Trust



Improving Lives

Document Name:	**Mobile Media Security Policy**
Executive Summary:	To ensure all mobile media is used securely. To ensure staff are provided with clear responsibilities about the secure use of mobile media.
Executive Lead:	Director of Finance, Capital and IM&T
Document Author:	Information Governance Manager, Deborah Tonkin
Document Purpose:	Policy
Target Audience:	All staff
Additional Circulation List:	All staff via intranet
Date Ratified:	15/01/19
Ratified by:	Information Governance Steering Group
Consultation:	Representatives from all directorates via membership of the IGSG.
Cross Reference:	Related trust policies including the Information Governance Policy (IG06) and the Incident, Accident and Near Miss Policy and Procedure (RM04) as well as the Information Security Management Code of Practice for NHS organisations and the Data Security and Protection Toolkit.
Superseded Docs	GMMH Mobile Media Security Policy (IG10) V1 Accessing and Using Mobile Technology Within GMMH Policy (IMT01) V1
Date of Equality Impact Assessment:	Pending
Board Objective Reference:	Objective 1 – To promote recovery by providing high quality care and delivering excellent outcomes Objective 3 – To engage in effective partnership working Objective 6 – To achieve sustainable financial strength and be well-governed
CQC Regulation Reference:	17 – Good Governance
Risk Register Reference:	N/A
Contact Details for further information	Information Governance Manager Deborah Tonkin Tel: 0161 358 1753 Email: Deborah.tonkin@gmmh.nhs.uk
Document Status	This is a controlled document. Whilst this document may be printed, the electronic version posted on the Trust intranet is the controlled copy.

Contents

1. Introduction 4

1.1. Purpose 4
1.2. Scope 4

2. Definitions 5

3. Duties 6

3.1. Board/Lead Committee 6
3.2. Chief Executive 6
3.3. Trust Caldicott Guardian 6
3.4. Director of HR & Corporate Services 6
3.5. Director of Nursing & Governance 6
3.6. Director of IM&T & Finance /SIRO 6
3.7. Data Protection Officer (DPO) 6
3.8. Head of Operations/ Business Managers/ Deputy & Associate Directors 6
3.9. Managers 7
3.10. IM&T Services 7
3.11. Employees 8

4. Processes and Procedures 8

4.1. Breach of Principles by Staff 8
4.2. Mobile working and use of portable IT equipment 8
4.3. User Related Policy Statement for the use of portable devices 13
4.4. Patient Recording of clinical sessions/consultations on mobile media 13
4.5. Usernames and passwords 13
4.6. Lost or Stolen IT Equipment and Data Security Breaches 14
4.7. Removable Media Devices 15
4.8. Work related downloading of documents & files 17
4.9. Virus Control 17
4.10. User Conduct 17

5. Training Requirements 18

6. Monitoring 18

7. Resource/Implementation Issues 18

8. Risk Issues 18

9. Requirements, Supporting Documents and References 18

9.1. Requirements 18
9.2. Supporting Documents 19
9.3. References 19

10. Subject Expert and Feedback 19

11. Review 19

1. Introduction

Technology is advancing at an unprecedented rate and at the same time the accessibility to it is becoming increasingly more diverse, easier and faster than could ever have been envisaged. A reliance on technology and the benefits it can bestow has understandably developed and it is recognised that removable media devices can be very useful in certain circumstances, provided they are used appropriately and do not pose any threat to the security of the Trust network or the confidentiality of individuals.

This policy aims to clarify the expectations and responsibilities of staff, including health and safety and information governance issues, for the appropriate use of mobile technology within and on behalf of the trust. It has been developed in accordance with related external requirements including:

- Using Mobile Phones in NHS Hospitals (Department of Health, 2009);
- The Human Rights Act 1998 - Article 8;
- Code of Practice to the Mental Health Act 1983 (Department of Health, 2008).

Due to the rate of advancements in technology it is proposed that this document will be reviewed annually and as and when new advancements are introduced. However, the principles within it are deemed to be generic enough to be applied to most developments not as yet made or anticipated.

1.1. Purpose

This document aims to clarify how and when mobile technology can be used. Specifically, it sets out:

- the criteria for access to, and conditions relating to use of, portable devices;
- employee responsibility and the rules of conduct for all members of staff using Trust provided portable devices;
- Trust's responsibilities for portable devices to maximise the benefits of using such equipment whilst minimising potential risks.

1.2. Scope

All staff, (including agency and bank staff), and contractors should be aware of and be fully compliant with this policy. They should feel confident to challenge the inappropriate use of technology or draw this to the attention of a senior manager within the Trust.

This policy covers the use of any and all electronic devices which have the capability to record sound and/or pictures in the format of photographs and/or videos, and commonly would include, but would not be limited to, mobile phones, smart watches, handheld computers, cameras with removable media and game consoles.

2. Definitions

General Data Protection Regulation – The General Data Protection Regulation (GDPR) applies across Europe from 25th May 2018. GDPR superseded the previous UK Data Protection Act 1998 (DPA). GDPR brings significant and wide-reaching changes in the way we deal with data protection. It expands the rights of individuals to control how their personal data is collected and processed, and places a range of new obligations on organisations to be more accountable for data protection.

Inappropriate Content/Material – Any information which is of a violent, sexual, discriminatory, inflammatory or disrespectful and offensive nature or sensitive data that is inappropriately disclosed and communicated. Any information that encourages and/or supports the following behaviours-gambling, alcohol consumption, substance abuse, self-harm, body dysmorphia, eating disorders, suicidal ideation and extreme political radicalisation.

Mobile Technology Device – Any electronic based piece of equipment, capable of transmitting sound, recording sound or pictures, or linking to a live feed via the internet and relates to equipment such as but not limited to laptops, net books/note books, iPads, iPhones, tablets and Smartphones .

Mobile working – The use of information technology and telecommunications to replace office based work. Mobile working allows employees to work at home or from a remote location using communication tools, such as such as phones, broadband or Wi-Fi, Internet, teleconferencing, e-mail or Instant Messaging.

Removable Media- includes but is not exhaustive:

- Floppy disks
- Data CDs or DVDs
- USB flash memory sticks/pens
- SD cards
- Smart Watches
- Zip drives and portable hard drives
- MP3 players e.g. iPODs
- PDA (or palm top computer)
- Mobile phones and digital cameras
- Tablets
- Smartphones and other smart devices
- Any Bluetooth device capable of storing data
- Digital Voice Recorders

Social Network Media – Any electronic based informal, social communication system including but not limited to Facebook, Twitter, About me, My space, You

Tube and WhatsApp.

3. Duties

3.1. Board/Lead Committee

The Information Governance Steering Group is responsible for ratification and monitoring of this policy.

3.2. Chief Executive

The CEO is responsible for ensuring that the Trust has clear policy and guidance on the expected standards when accessing and utilising technology within the Trust and when using devices and accessing information remotely.

3.3. Trust Caldicott Guardian

The Trust Caldicott Guardian has responsibility for reflecting service user interests regarding the use of their personal identifiable information and ensuring such data is shared and handled in an appropriate and secure manner.

3.4. Director of HR & Corporate Services

Responsible for the implementation of the policy Trust wide and providing HR support and guidance with compliance where appropriate.

3.5. Director of Nursing & Governance

Responsibility for the overall implementation of the policy in the clinical networks.

3.6. Director of IM&T & Finance /SIRO

Responsible for the implementation of the policy Trust wide and providing technical advice, support and guidance with practical application.

3.7. Data Protection Officer (DPO)

The data protection officer is responsible for overseeing data protection and Information Governance strategy and implementation to ensure compliance with GDPR requirements. The DPO will monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for all data subjects and the ICO.

3.8. Head of Operations/ Business Managers/ Deputy & Associate Directors

Responsibility for ensuring the implementation and adherence to the policy within Directorates.

3.9. Managers

All managers have a responsibility for:

- Ensuring day to day compliance with the policy.
- Challenging and taking appropriate action with anyone who does not respect and adhere to the fundamental principles of this policy and uses mobile technology in a negative manner likely to cause offence and/or the inappropriate exposure of another person.
- Reporting and acting upon any reported incidents where it is suspected that mobile technology may have been used inappropriate, without delay and via the Trust's recognised risk monitoring systems.

3.10. IM&T Services

IM&T Services are responsible for configuring Trust mobile equipment, (e.g. laptops), in such a way that authorised Trust users can remotely connect safely, securely and seamlessly to the Trust's network and information systems. A typical session will enable a user to work in much the same way as they do on a computer at a Trust site.

IM&T services will ensure that all Trust mobile equipment must be encrypted before any confidential information is processed on it. Approved encryption is installed on every Trust mobile device prior to issue.

IM&T Services are responsible for ensuring data on network drives is backed up on a regular basis.

The IT Department is responsible for ensuring that access to supplied equipment requires a username and password and that end point encryption and anti-virus software are installed as appropriate.

When equipment is returned, IM&T are responsible for: removing any data stored locally, ensuring the IT asset database is updated to reflect change of user and/or storage/decommissioning of the equipment. Before any equipment is put into storage, IT are responsible for ensuring that the equipment is wiped of all data and secured physically.

The equipment will then be reimaged/set up for a new user including appropriate encryption is installed prior to reissue. The asset register will be updated to reflect the new asset owner.

IM&T will undertake regular audits of remote/mobile working arrangements to ensure that all users are approved, assets can be accounted for, that secure remote access is used and any confidential / sensitive information is securely transported or stored in a remote location.

3.11. Employees

All employees are responsible for:

- ensuring that they comply with the requirements of this policy and use their mobile technology devices appropriately.
- ensuring the appropriate use and security of any information and IT equipment they use in accordance with their duties, e.g. computers, laptops, internet, removable devices, etc.

4. Processes and Procedures

4.1. Breach of Principles by Staff

Failure to comply with the requirements of this policy will be dealt with under the Trusts disciplinary procedures.

4.2. Mobile working and use of portable IT equipment

4.2.1 Mobile working rules

Staff must not remove Personal Identifiable Data (PID) **or** Business Critical Information (BCI)**,** information systems, or devices from the Trust without prior authorisation from their Line Manager or, (where necessary), Senior Management. *Note: The Caldicott Guardian is the Trust's 'ethical head' on the use of service user's data and has the final word in any arbitration regarding this.*

It is the expectation of the Trust that systems will be accessed remotely rather than data downloaded and stored on local devices, e.g. remote access in to Paris and the Trust network.

The use and storage of Personal Identifiable Data or Business Critical Information on staff owned equipment is strictly forbidden. Staff may only use Trust supplied equipment to access trust data and systems or to store data.

Staff must only use Trust provided encrypted devices when using Personal Data or Business Critical Information. They must inform the IT Service Desk if they believe that their equipment is not secure or has been compromised using the approved method.

Only authorised members of staff are allowed access to Trust information when used at home in any form, on any media. Unauthorised individuals, including family members must not be allowed to access Trust equipment or data. Use of any information at home must be for work purposes only.

Users are responsible for ensuring that unauthorised individuals are not able to see information or access systems.

Staff must ensure the security of the Trust provided mobile media device by ensuring it is locked in the boot of the car during transportation and then stored securely in the house at night. NO mobile media devices are to be left in the car overnight.

Access to any form of mobile device is restricted to the member of staff to whom it was issued. One device, one owner.

Under no circumstances should staff share their passwords and/or usernames or allow anyone else to use their account.

Users must be aware of the fact that carrying or using a laptop computer or other mobile device in a public place is likely to draw attention to them and will also increase the risk of both theft and the unauthorised disclosure of information on the screen.

The use of information assets in public areas should be kept to an absolute minimum due to the threats of 'overlooking', overhearing and theft. Any member of staff choosing to use information and/or mobile devices in these areas that results in any related information security incident will be required to state why the usage was required in that situation and the efforts they made to protect the information and any equipment.

Users must ensure personal responsibility and security for any Trust provided portable device in their care.

Any portable device that is owned by the Trust, which has internet connectivity, must be used in accordance with the Trust's Internet and Email Policy and the information security policy. Particular attention should be paid to the provisions relating to access to unsuitable material and activities which may compromise network security. This applies to wherever the equipment is used.

For prevention of viruses and related security risks staff may not connect any personally owned devices to the Trust network or IT hardware unless approved by IM&T.

Connection of Trust supplied equipment to home broadband networks for home working access is permitted.

SIM cards must not be transferred between different mobile devices; such as laptops, smartphones, tablets etc., as different tariffs may apply. Should there be a requirement to change the device with which the SIM card is associated, a change request should be submitted to the IT service desk.

Voice calls from a personal phone for business purposes are permitted.

Unless authorised by IM&T Services the use of personally-owned phones is prohibited for business use with regard to data transfer and storage. Staff are not permitted to synchronise their personal phone devices, (including iPhones, Smartphones and smart watches), with their business Outlook information.

4.2.2 Obligations for staff

Staff must not:

- disable Trust virus protection software on Trust equipment;

- download or load unauthorised software onto Trust equipment;
- save PID or BCI data directly to the local disk or desk top, (e.g. C:\ Drive), of a computer, laptop or device;
- install or connect any unauthorised hardware on any Trust device;
- connect mobile devices to unsecured public Wi-Fi networks;
- use any personal portable devices of any kind for trust business;
- use trust provided portable devices for personal use;
- use trust provided portable devices for the processing, storage or transfer of person identifiable data without sufficient encryption in place;
- use trust portable devices for bulk transfer of data off site without authorisation;
- use personal portable devices of any kind to connect to the trust's network infrastructure, apart from trust guest Wi-Fi;
- use trust provided portable devices as a permanent or indefinite storage mechanism; data must be transferred, as soon as possible to a secure networked drive and removed without hesitation from any trust provided portable device;
- use trust provided portable devices for any type of a commercial or profit-making nature, or for any other form of personal financial gain; or any use that conflicts with an employee's obligations to their employer; or any use considered to be against the organisation's rules, regulations, policies and procedures in particular this policy;
- allow any unauthorised persons to have access to or use the portable device provided.

Any staff member who removes information or equipment from GMMH premises is responsible for ensuring their safe transport and storage.

Information assets:

- must not be stored in places where a thief can easily steal them;
- must not be left visible in a car when travelling between locations;
- must not be left unattended in a public place;
- must not be placed in locations where they could easily be forgotten, e.g. overhead racks, taxi boots, train stations, exhibition halls etc.;
- must be password protected;
- must be transported in a secure, clean environment.

As a visitor you may be given permission to connect laptops or other devices to another organisation's network in order to acquire internet access at the discretion of that organisation. As a guest you must agree to use the connection in accordance with the aims and policies of that organisation and for no other purpose.

4.2.3 Organisational Obligations

The organisation will:

- have formal portable device request procedures, allocating such equipment where reasonable justification can be found;
- replace personal portable devices with trust issued equipment of this nature where reasonable justification can be found;
- ensure all trust provided portable devices come complete with appropriate encryption and security mechanisms;
- implement and maintain anti-virus software on servers and portable devices where appropriate;
- ask you to sign a receipt for a trust provided portable device and the data encrypted on it.

The organisation will not be held responsible for loss of portable devices or the recording of personal data of the user.

4.2.4 Mobile Working Agreement

Individual requests for mobile working will be reviewed on their own merits in accordance with existing HR procedures. Agreement to a specific request will depend on an objective assessment of whether the employee's work can be done remotely without any detriment to Trust services or service user relations.

When a mobile working agreement is possible, the purpose and terms and conditions should be formally reviewed and agreed by the mobile worker and their Head of Service. A reference copy of this agreement must be provided to the mobile worker. All such mobile working agreements should be reviewed periodically for their continued applicability.

The remote worker's proposed working environment(s) should be considered and where necessary surveyed for information risks. Any perceived information risks should be assessed to help inform mobile working options. The findings of this survey process and any associated risks should be documented, so that appropriate control measures may be reviewed.

For all mobile working/mobile working scenarios, consideration of risks must be made and should take account of the potential to:

- accidentally breach service user confidentiality;
- disclose sensitive data of the organisation to unauthorised individuals;
- lose or damage critical business data;
- damage the organisation's infrastructure and e-services through spread of a malicious code such as viruses;
- create a hacking opportunity through an unauthorised internet access point;
- misuse data through uncontrolled use of removable media such as digital memory sticks and other media;
- cause other operational or reputational damage.

Steps should then be taken to define, agree and implement the environmental

security controls deemed necessary. The Trust should maintain records of all such assessments, surveys, related decisions, agreements and implementation plans.

It is the responsibility of the mobile worker to maintain their mobile working environment and security in conformance with the organisation policies and agreement permitting their mobile working. Where a mobile worker requires clarification or guidance they should consult the Trust.

The mobile worker should be made fully aware of their information governance responsibilities to the organisation. Training should be provided to mobile workers for any additional or special tools or functions that underpin the security of their mobile working, such facilities and the training in their use are the responsibility of the Trust. This may for example include guidance on the deletion of cached information from internet browsers used to access web-based services.

Any staff members defined as mobile workers are responsible for ensuring that their remote work conditions comply with health and safety regulations and Trust policies and procedures. Staff must undertake a health and safety and display screen equipment risk assessment and a copy of this assessment must be retained on their personnel file. Staff are responsible for ensuring that the assessment is reviewed following any change in their remote working environment.

Mobile workers must ensure they have adequate insurance cover for any Trust equipment on their premises. Cover is normally available within the mobile workers home contents insurance for the loss of any equipment provided by the Trust. Where this policy has been breached and results in the loss, theft or damage of equipment the Trust reserves the right to claim any expenses incurred from the person in breach.

It is the responsibility of the Trust to ensure that the organisations infrastructure is maintained in a technically secure manner that would reasonably prevent a security breach arising from a remote worker’s location.

The Trust is responsible for the safety testing of supplied equipment and annual electrical safety Portable Appliance Testing (PAT) of this equipment. Staff who use the equipment are responsible for ensuring that these checks are undertaken.

A request for the necessary equipment with authorisation from the Head of Service should be made via IM&T Support Central.

Once all necessary steps have been satisfied the mobile working arrangements may be made operational. Please note that other NHS IG codes of practice and good practice guidance for information governance, information security management, the use of data encryption tools and security of permitted removable media remain applicable and should be followed.

Failure by staff to observe and maintain their mobile working agreement, including all associated IG policies, may result in their mobile working facility being withdrawn.

The Trust may undertake audit checks to ensure this mobile working policy is

complied with. Any compliance issues will be reported to the line managers concerned and may be handled through HR processes or contractual arrangements.

All incidents involving the use of mobile working facilities must be reported to immediately to the IG Manager and IT Manager and a Datix completed.

4.3. User Related Policy Statement for the use of portable devices

Appropriate/Inappropriate Usage
The need to use removable media devices is negated by a number of network tools that the Trust has put in place, (e.g. shared network drives), which allow users to work in such a manner that will improve the quality of work and productivity. As a result the use of removable media devices in the Trust **is not permitted**, except in certain circumstances where an agreement to use such equipment has been reached with the Trust's IT Department and in some instances with the permission of the Trust's Caldicott Guardian.

The use of Trust supplied portable devices is not taken lightly by the Trust due the risks associated with the secure storage of data. Consequently, all staff who believe they have a business need to use such equipment must provide reasonable justification to the Trust in support of any application for the supply and or acquisition of such equipment.

The use of portable devices supplied by a user is **NOT** acceptable under any circumstances. In the event that such equipment is being used in such a manner it should stop immediately and an application with supporting justification be made to the Trust for the provision of such equipment.

4.4. Patient Recording of clinical sessions/consultations on mobile media

4.4.1 Patient Recording of clinical sessions/consultations on mobile media

Under GDPR and DPA 2018 clients are permitted to record their clinical consultations if they so wish. These recordings must only capture information relating to them and not capture details of any third parties. Medical staff are encouraged to follow their ethical codes of practice.

4.4.2 Staff recording of clinical sessions/consultations on mobile media

Staff who wish to record clinical sessions on mobile media must submit a DPIA to the IG team prior to ensure that all legal and ethical areas have been addressed prior to the capturing of these sessions for example for training purposes.

4.4.3 Usage of communication applications, e.g. WhatsApp, Messenger, etc.

The use of communications applications such as Messenger, WhatsApp etc. is not permitted for business use or to discuss details relating to your employment and or service users.

4.5. Usernames and passwords

4.5.1 Usernames & passwords

The use of Trust provided portable devices is aligned to the creation and ongoing

usage of a Trust network account. Therefore:

- You are responsible for maintaining the security of your individual username and password.
- You must not share your unique username and password. Unauthorised access, modification (or the intent to access/modify) are criminal offences under the Computer Misuse Act 1990.
- If a breach of security is recorded under your login the burden of proof will be with you to show that you are not responsible for the breach.

The Trust's Email, Internet Usage, and IT Security policies should be read in conjunction with this policy.

4.5.2 Temporary Staff usernames & passwords

Please refer to the Clinical Systems Access Policy.

4.6. Lost or Stolen IT Equipment and Data Security Breaches

4.6.1 Lost or Stolen Equipment

All staff are responsible for reporting suspected or known breaches of information security, or identified weaknesses within information systems they may use to the appropriate nominated manager.

All staff are required to report immediately to the Trust the loss or theft of any of the following:

- Laptop or notebook, Memory Stick, flash pens, CDs, DVDs, external hard drives, Palmtop Computer, blackberry device, mobile phone, iPad. IPhone, Dictaphone, digital or other such mobile IT device.
- Papers or files containing personal information such as:- patient, carer or staff information.

The above should be reported if the equipment or data belongs to the Trust or relates to anyone connected with the Trust e.g. staff, patient or carer. This also applies in instances where your own property is lost or stolen and it contains such information.

Loss or theft of any of the above items should be reported immediately to the:

- Line Manager
- Trust Security Officer
- Information Governance Manager
- IT Manager
- Police

The Lost or Stolen IT Equipment and Data incident must also be reported via the Trust Incident Reporting System, Datix.

4.6.2 Security Breaches

Recording security breaches enables management to improve the quality of service to patients and staff; you must report incidents for this purpose.

Any security breaches e.g. unauthorised sharing of usernames and passwords (or suspected breach) must be reported immediately either directly to IT via IM&T Support Central or through your line manager.

Security breaches must also be reported via the Trust incident reporting process.

If warranted the findings will be subsequently reported to the SIRO, IG Steering Group and the ICO. The ICO will take the decision to refer to the Criminal Investigations Team in view of prosecuting under Section 55 of the Computer Misuse Act.

4.7. Removable Media Devices

4.7.1 User Responsibilities

Users must:

- Use personally provided removable media devices only by agreement of the Trust IT department who in turn have to be satisfied that the device is encrypted to a secure enough standard and represents no risk or threat to data integrity and confidentiality and that there is a legitimate business reason for the transportation of this data by this mechanism.
- Ensure personal responsibility and security for any Trust provided removable media device in his/her care.
- Return all removable digital media devices to the IT Department.

Users must not:

- Use any removable media devices unless you have been specifically authorised to do so from the IM&T department.
- Use Trust provided removable media devices for the transfer or storage of person identifiable data in bulk form or otherwise unless that device has been encrypted.
- Use removable media for bulk transfer of data off site without the completion of a Bulk Transfer pro-forma and explicit consent of the Trust's Caldicott Guardian and IT Department.
- Use any personally provided removable media devices without Trust standard encryption in place and without the authorisation of IM&T.
- Use personal removable media for the transfer or storage of person identifiable data.
- Use Trust provided removable media devices as a permanent or indefinite storage mechanism. Data must be transferred, as soon as possible to a secure networked drive and removed without hesitation from any Trust provided device.

- Use removable media devices to introduce viruses onto the Trust network.
- Store portable devices in an insecure manner when not in use either on or off site.
- Use Trust provided removable media devices for any type of a commercial or profit-making nature, or for any other form of personal financial gain. Or any use that conflicts with an employee's obligations to their employer. Or any use considered to be against the organisation's rules, regulations, policies and procedures in particular this policy.

4.7.2 Overview of organisational responsibilities

The organisation will:

- Provide staff with a removable media device provided there is a legitimate business reason for the transportation of this data by this mechanism.
- Provide staff with removable media devices that are encrypted to the latest industry standards as dictated by NHS Digital.
- By default, disable all USB and or CD/DVD drives granting access to them on a case by case basis where is agreed there is a legitimate business reason for their usage.
- Ask you to sign a receipt for a Trust provided removable media device and the data encrypted on it.
- Will keep a record of the removable media device that has been signed for and the nature of the data that was put on the device.
- Provide appropriate network tools e.g. roaming profiles and shared network drives to assist the user with the transportation of data within the Trust's network.

The organisation will not:

- Transfer data to removable media device unless there is a legitimate business reason to do so.
- Support users in acquisition and usage of their own removable media device.
- Advocate the use of removable media devices as the norm.
- Be held responsible for loss of removable media devices.

4.7.3 Appropriate/Non Appropriate Usage of removable media devices

The use of Trust supplied removable media device is not taken lightly by the Trust due the risks associated with the secure storage of data. Consequently, reasonable justification has to be provided to the IT department that there is an absolute business need for the use of such a device. This is especially apparent when Person Identifiable Data (PID) or commercially sensitive data is to be placed on such a device.

Before any removable media is issued by the Trust it will be encrypted with the latest

technology which will ensure the safety and integrity of the data to be placed on the device.

4.8. Work related downloading of documents & files

Staff are not permitted to download and install any software without gaining the authorisation of the IM&T Department first. Staff may encounter occasions where they are asked to download software that they were not expecting. In these instances contact must be made with IM&T for guidance and assistance.

The intentional downloading of software, in the knowledge its operation will lead to malicious damage to the Trust's operation, will lead to disciplinary action and potential prosecution under the Computer Misuse Act 1990, (this includes but is not limited to known viruses and 'malware').

Staff should not download files that will breach the owner's copyright, nor take any action on downloaded files (further distribution) that may also be in breach of copyright.

4.9. Virus Control

Use of a Trust provided portable device may permit access to the Internet. Users should be aware the internet is a major source of computer viruses, the effects of which can range from a minor irritant to a major disaster.

Although the IT network has background antivirus defences, which are updated in line with software supplier recommendations, it is still essential for users to specifically check files and mail prior to opening. In the event that a user suspects a virus infestation they must stop using that portable device and contact IM&T.

4.10. User Conduct

Staff are bound by the legal duty of confidence, the General Data Protection Regulation, Caldicott Principles and other related legislation concerning the information you come across/use in the course of their work.

Staff may not disclose information relating to any identifiable individual, either patient or staff using removable media unless you have the necessary authorisation to do so.

Users should also not undertake the unauthorised transmission to a third party of confidential material concerning the activities of the Trust.

Personal/Patient Identifiable data – Person identifiable information or other organisational confidential information must not be stored on Trust provided removable media without it first being encrypted with NHS approved software. Any such storage should be considered temporary and at the first possible opportunity such data should be transferred to a Trust networked drive, i.e. M: or N:. Thereafter without hesitation such data should be removed from any portable device.

Bulk Transfers of Data (approx. 51+ records) – removable media should not be used for the Bulk Transfer of data without authorisation. Users must also ensure the completion of 'Bulk Data Transfer' proforma and have the explicit consent of the Trust's Caldicott Guardian. In the event that a bulk transfer of data using removable media is permissible, data must be protected with encryption and password security. In the event of such data being sent electronically all information must be protected with encryption and password security. In instances of hard copy transfers a record should be made of the type of date being sent, the intended recipient and the intended usage. This record will be held by the Information Governance Manager.

5. Training Requirements

In line with the Trust Mandatory Training policy, the Trust will ensure that all users of Trust information systems and assets are provided with the necessary information security guidance, awareness and training as appropriate to discharge their security responsibilities based on the outcome of the training needs analysis undertaken by the Learning and Development Department.

6. Monitoring

Minimum Requirement	Frequency	Process for monitoring	Evidence	Responsible Individual(s)	Response Committee(s)
The trust has an up to date policy for mobile media security	Annually	Routine review of policy	Policy document Consultation records Meeting minutes at which policy discussed	Head of IM&T Service Delivery	Information Governance Steering Group
	Ad hoc as changes in circumstance arise	Urgent review of policy and related requirements		Author	

7. Resource/Implementation Issues

Not applicable for this document.

8. Risk Issues

All risks to be assessed locally and on an individual basis as outlined within the body of this document.

9. Requirements, Supporting Documents and References

9.1. Requirements

Board Objective Reference:	Objective 1 – To promote recovery by providing high quality care and delivering excellent outcomes Objective 3 – To engage in effective partnership working Objective 6 – To achieve sustainable financial strength and be well-governed

CQC Regulation Reference:	17 – Good Governance
Other requirements:	Using Mobile Phones in NHS Hospitals (Department of Health, 2009); The Human Rights Act 1998- Article 8; Code of Practice to the Mental Health Act 1983 (Department of Health, 2008). Data Security and Protection Toolkit

9.2. Supporting Documents

- Using Mobile Phones in NHS Hospitals (Department of Health,2009)
- The Human Rights Act 1998- Article 8
- Code of Practice to the Mental Health Act 1983 (Department of Health, 2008)

9.3. References

- NHS Code of Practice for Information Security DoH
- NHS Digital, Data Security and Protection Toolkit: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit

10. Subject Expert and Feedback

All queries should be directed to the author.

11. Review

Trust policy for review is every five years, however, this policy will be reviewed annually in line with the Data Security and Protection Toolkit, or sooner in the light of organisational, legislative or other changes.