Policy:

IMST 009 - Remote Working & Mobile Devices

Executive Director Lead	Executive Director of Finance & SIRO
Policy Owner	Head of Informatics
Policy Author	Data Protection Officer

Document Type	Policy
Document Version Number	Version 2.0
Date of Approval By PGG	05/2024
Date of Ratification	July 2024
Ratified By	ARC
Date of Issue	May 2024
Date for Review	04/2027

Summary of policy

This policy provides guidance on the use of mobile devices and software which enable Trust staff and other people working on behalf of the Trust to work away from Trust bases.

Target audience	SHSC staff and people authorised to access the SHSC network

Keywords	BYOD, Mobile, Wifi, Govroam, remote working, devices

Storage & Version Control

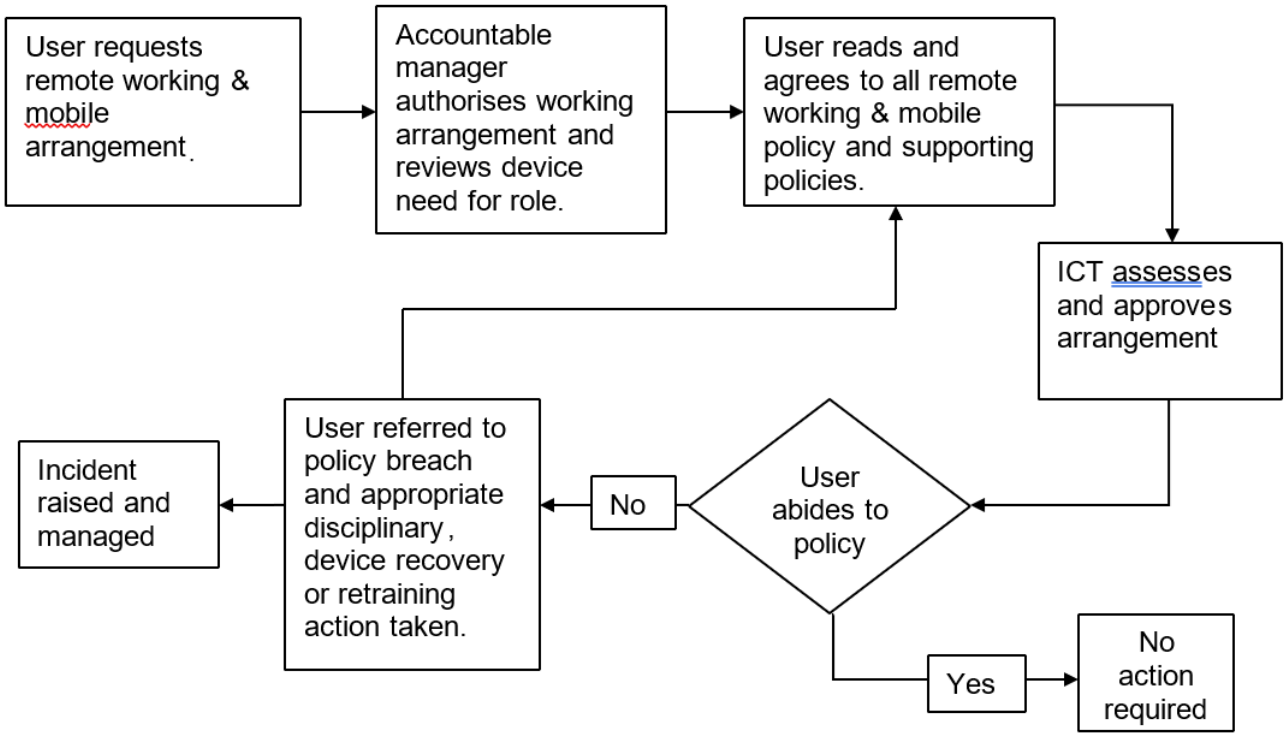
Version 2.0 of this policy is stored and available through the SHSC intranet/internet.. This version of the policy supersedes the previous version (V1.9 11/2022). Any copies of the previous policy held separately should be destroyed and replaced with this version.

Version Control and Amendment Log

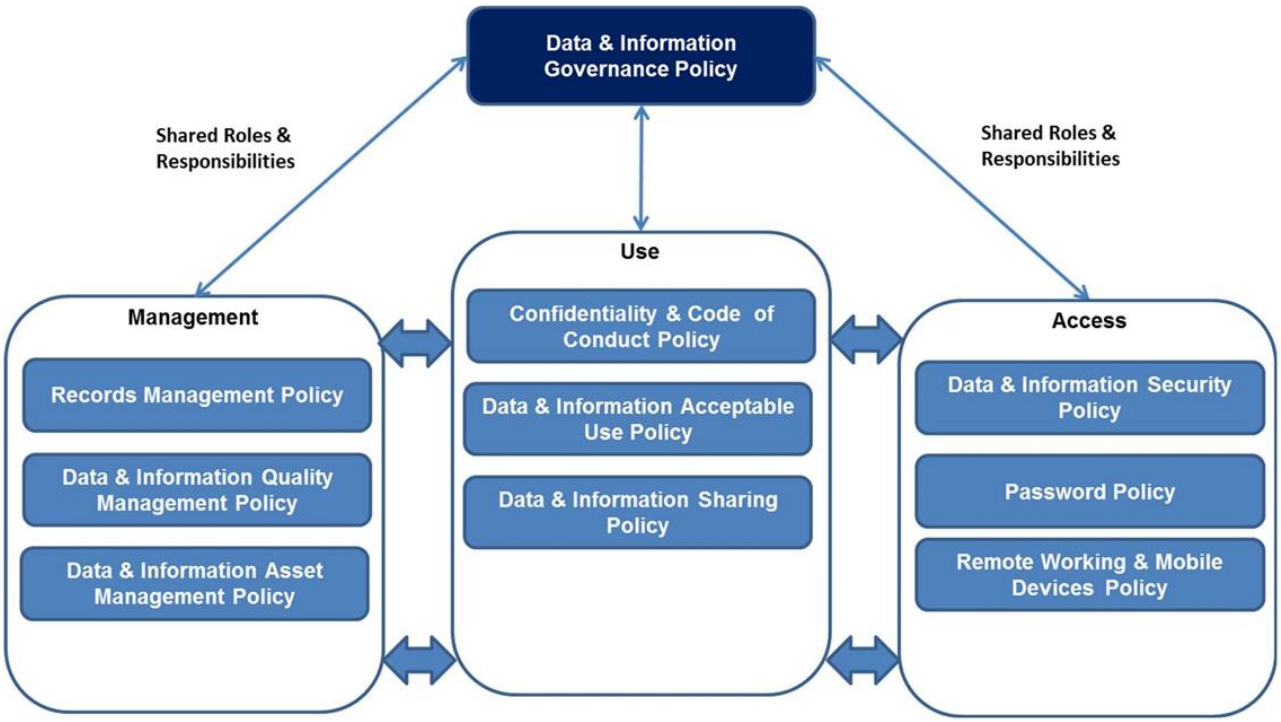
Version No.	Type of Change	Date	Description of change(s)
1	Policy created	09/2007	Approved by the Information Governance Committee
	Revision	03/2008	Updated in light of national guidance on information security, data flows and encryption
	Revision	10/2010	Update and incorporation of comments from the Information Governance Steering Group
	Revision	02/2013	Minor amendments
	Revision	02/2014	Minor amendments
1.7	Revision	03/2018	Update as part of a wider review of Information Governance policies and incorporation of mobile communication policy
1.8	Revision	10/2019	Updates for legislative and monitoring changes and contact details.
1.9	Revision	04/2022	Updates to match Data & Information Security Policy, updates of group names, addition of arrangements for remotely-based staff.
2.0	Revision	05/2024	Addition of sections on mobile phones and WhatsApp/instant messaging

Contents

Flowchart



The Data & Information Governance Policy provides the overarching shared roles and responsibilities needed to satisfy complete Trust Data, Information and System ownership and management.



1 Introduction

Current working practice within Health and Social Care is such that individuals may not have a static work base, may need to work away from their normal base or work from home. In the course of their work such individuals may need to access the Trust network or to take Trust information away from their base. At the same time, developments in technology are such that it is now possible to process information on various types of portable/mobile electronic devices.

While these changes to working practices and developments in technology bring many benefits they also introduce risks to the organisation, individual staff members and the security of Trust information. Information is no longer retained in the work base where it can be automatically backed up but is moving about the city, region or country on a variety of devices. The convenience of these devices - their small size and capacity to hold large amounts of information – also increases the risk. They can easily be lost, mislaid or stolen. It is important that information, whether stored on mobile devices or accessed or worked on remotely, is protected by proper security.

This policy is also concerned with the removal of hard-copies of confidential information from Trust premises where necessary so that it is transported, stored and used securely and returned to Trust premises in a timely manner.

2 Scope

The scope of this document is to outline the Trust's policy for Remote Working & Mobile Devices for all data, information and system management and protection.

This policy applies to all staff and services within the Sheffield Health & Social Care (SHSC), including private contractors, volunteers and temporary staff and to those organisations where we provide commissioned services.

Shared governance and compliance areas for data and information include:

- NHS Digital & England Guidance
- Data Security & Protection Toolkit
- Cyber-Security Best Practices
- Information Technology Service Management
- UK General Data Protection Regulation/Data Protection Act
- Caldicott Principles
- Data & Information Quality Management
- ISO27001 Information Security Management Systems

The policy supports the Trusts needs to continually improve, protect and manage all digital, data and information assets according to legislation and best practice through a collaborative approach.

Systems

All manual and electronic information systems owned, operated or managed by the Trust, including networks and application systems, whether or not such systems are installed or used on Trust premises.

Other systems brought onto Trust premises including, but not limited to, those of contractors and third party suppliers, which are used for Trust business.

Users
All users of Trust information and/or systems including Trust employees and non-Trust employees who have been authorised to access and use such information and/or systems.

Data & Information
All information collected or accessed in relation to any Trust activity whether by Trust employees or individuals and organisations under a contractual relationship with the Trust.

All information stored on facilities owned or managed by the Trust or on behalf of the Trust.

All such data & information belongs to the Trust unless proven otherwise.

3 Purpose

Mobile computing can bring many benefits to the Trust. It allows for information to be available whilst working on the move and in remote or home-working situations. It can improve the patient care experience and can contribute to the improvement of working lives.

The purpose of this Policy is to set out the process to be used to enable staff to use portable devices and information assets in a responsible and appropriate way, including:-

- Understanding their responsibilities when accessing the network
- Understanding the possible implications and risk of information misuse
- Connection to the Trust network – remotely and with mobile devices
- The processing of Trust information away from Trust premises
- The processing of Trust information on mobile devices
- The secure transfer of information
- The security of mobile devices and information
- The use of home computers and personal mobile devices

4 Definitions

Remote Working
Mobile and remote working is the term used to describe working away from a Trust site or office, including working from home. New technology has made this easier. Within the context of the Trust, mobile computing is a term used to describe the use of mobile devices that process Trust data. Typically, this will include items such as laptops, tablets (such as iPads) and mobile telephones (smart phones) where these are capable of storing data.

Portable Equipment
Includes, but is not limited to, laptops, mobile phones and smart phones, tablet devices, PCs, USB Memory devices and other forms of digital storage.

Technology continues to evolve and thus this is not intended to be an exhaustive list. However, it includes all battery-powered and mains-adapted personal computing and storage devices.

5 Detail of the policy

This policy provides guidance on the use of mobile devices and software which enable Trust staff and other people working on behalf of the Trust to work away from Trust bases. It clarifies the responsibilities for support of people working away from Trust bases and the return of devices to Trust premises for update and repair.

6 Duties

The strategy combines traditional Information Asset (IAO / IAA), data governance, data quality and (ITSM) system management roles and responsibilities into a single accountable shared Business Information Management framework.

Role		Responsibility	Description
Senior Information Risk Owner	SIRO	Director Finance	Owns the Trust's information risk policy and risk assessment process.
Chief Information Officer	CIO	Chief Digital Information Officer	Responsible for the Information Technology that supports the overarching strategies of the Trust.
Chief Clinical Information Officer	CCIO	CCIO	Providing a vital voice for clinical strategy, allowing new IT and Data & Information products to help improve the provision of healthcare.
Caldicott Guardian	CG	Director Medical	Responsible for protecting the confidentiality of patient and service user information and enabling the appropriate level of information sharing.
Data Protection Officer	DPO	DPO	Supporting Trust -wide Data & Information governance in accordance with GDPR, NHS Digital & England and Data Security & Protection Toolkit.
Cyber Security Officer	CSO	Assistant Deputy Directors IMST	Supporting the Trust to continuously assess, implement and manage Trust wide cyber-security, and removing identified vulnerabilities with support from all technical and business managers and users.
Information Asset Owners	IAO	Directorate	Senior representatives of the directorates closely aligned to major stores of organisational data, information and systems.
Information Asset Managers	IAM	System/Service Managers	Primary administrative and management responsibilities for segments of data primarily associated with their functional area.

Each Data and Information role has clear responsibilities for data, information and system management within their respective service domains and role accountability, supported by natural hierarchy escalation and incident management.

All staff who use Trust information systems (including manual systems as well as electronic ones) plus other authorised users of systems are required to adhere to this policy.

7 Procedure

It would be counterproductive to ban or reduce the use of mobile devices simply because there is a risk. To do so would prevent the benefits of using these devices being realised.

You should follow the principles given within this policy and associated Data & Information governance polices.

There are some basic controls that should be in place as a matter of course to secure mobile devices and the information that is on them or that is sent to and from them. In order to reduce the risk of loss or theft you should, as a minimum:

Do

- Read and understand your organisation's data and information security policies and procedures.
- Ensure that these devices and documents are kept with you or locked away when not in use, and make sure that they are out of sight while you're travelling.
- Consider using carry cases/bags which are not obvious laptop bags, e.g. without manufacturers' logos.
- Apply the same level of security that you would normally have in your place of work if you are storing equipment or documents at home, in hotels or other sites.
- Minimise the amount of data that you hold on your device or in hard copy form.
- Ensure this is limited to what you require to do your job and that it is backed up in accordance with Trust policy.
- Immediately report any actual or suspected loss, theft or unauthorised access/disclosure of devices, documents or information.

Don't

- Work with or discuss confidential or sensitive information in areas where your conversation can be overheard or your device screen and documents can be viewed by unauthorised persons.
- Leave your device or documents visible in an unattended vehicle, even for a short time.
- Store or carry any tokens or passwords used for accessing your device or systems in the same bag as your device. If you lose one, you will lose both.
- Hold more information than is necessary to carry out your tasks.

It is important to remember that these measures are not just for the protection of the equipment and the information on it - they are also there to protect you. Don't make yourself a target.

7.1 Direct Connection to the Trust Network

All electronic processing devices connecting directly to the Trust network (that is, connected to a network point or via a Wi-Fi connection on NHS premises) must have the latest operating system updates applied and run up-to-date anti-virus and firewall software. Where the device does not update automatically, it is the responsibility of the

user to ensure that the anti-virus software is up-to-date and that the firewall is switched on.

Personal devices (that is, devices that are not provided by your employer for use in your work) such as home personal computers, laptops, netbooks, media players (such as i-pods) and personal digital assistants, must not be connected directly to the Trust network unless authorised by the IT Department in line with Trust Bring Your Own Devices (BYOD) arrangements. The BYOD electronic application form is available via the SHSC intranet.

7.2 Remote Connection to the Trust Network

Connection to the Trust network remotely (that is, via web services or remote services) requires authorisation by the IT Department and will be subject to authentication procedures specified by them.

As technology has evolved, and in response to external factors, many Trust staff now spend more time working away from SHSC premises. This may be when staff who are usually based on SHSC premises opt to work at home but there are also instances where staff spend little or no time working within SHSC premises, sometimes at a considerable distance away.

Where staff are based at distant locations, the following arrangements will apply:

The work location will be agreed with and approved by the line manager.

Remotely-based staff will be expected to collect SHSC equipment (laptops, phones etc) from Trust bases. Where this is not practical, it will be the responsibility of the employing team to arrange carriage of the equipment to and from their staff. Similarly, in the event that equipment needs to be returned to SHSC premises for repair or upgrade, the employing team will be responsible for this and the IT Department will not provide loan-devices whilst the original equipment is not available. The employing team will also be responsible for retrieving any Trust equipment when remotely-based staff leave Trust employment.

SHSC equipment may be used within the United Kingdom. If staff normally based within the United Kingdom have a need to use SHSC equipment outside the United Kingdom for a limited period of time due to exceptional circumstances, such requests should be directed to their line manager in the first instance and if agreed, will be considered on a case-by-case basis by the Assistant Deputy Director of IMST (Operations & Services) in consultation with the SIRO.

Staff or sub-contractors who are based permanently overseas will not be provided with SHSC equipment and other arrangements must be made with the IT Department for access to the SHSC network.

Requests for access from remotely-based staff will be processed by the IT Department subject to sufficient notice, with a target of 10 working days for turn-around.

The IT Service Desk will support remotely-based staff during normal working hours only. It is the responsibility of staff who require support to contact Service Desk within those hours – out-of-hours arrangements should not be used to request routine support where the user's working hours differ from normal SHSC hours.

7.3 Connection to non-NHS Networks

Trust equipment may be connected to the internet via non-Trust services including home connections and services provided by partner organisations providing that it is protected by up-to-date anti-virus software and the connection is made via the Trust's approved VPN solution.

7.4 Mobile Phones

Trust Mobile Phones:

All users are instructed to read the operating manual for the mobile telephone before use.

All mobile phones are provided with an international bar in place. To have the bar removed, authorisation from the Service Director must be passed to the IMST Service Desk giving dates for the duration the bar is to be lifted.

Mobile telephones issued by the Trust need only be switched on when the member of staff is on duty or on call.

Where a mobile phone allows access to the internet, any such access is governed by the Trust Data & Information Acceptable Use and supporting policies.

The user should not ordinarily give their mobile telephone number to service users or carers unless this is part of an approved business process (any service user or carer who may require advice or assistance should be encouraged to channel their request through the existing landline telephone systems e.g. administrative support, Community Team base). Staff should also use the phone settings to withhold the telephone number.

The mobile phone should be switched to silent/discreet mode when the user is with a service user/carer.

Many departments/buildings have local rules regarding the use of mobile phones and these must always be respected. The local policy on use of mobile phones within NHS premises should be checked before use due to possible interference with electronic medical equipment.

Most medical equipment within the trust has not had issues of interference caused by mobile phones. Medical equipment that may encounter interference is within controlled wards which no mobile device is permitted to enter.

This Trust prohibits the use of mobile phones of any type, hand-held or hands free, whilst driving and requires that the phone is switched to voice mail and the calls retrieved when it is safe and practical to stop the vehicle.

As mentioned in section 7.2, SHSC equipment may normally only be used within the United Kingdom. If for some reason staff based in the United Kingdom need to use SHSC equipment abroad they should be directed to their line manager. The Trust does not currently support the use of mobile phones overseas and has bars on international calls and data roaming.

Users must ensure that all mobile telephones/devices security devices, if fitted, are enabled. This may be in the form of a PIN (personal identification number) code or password.

The user should take all reasonable steps to prevent damage or loss to their mobile telephone. This includes not leaving it in view in unattended vehicles and storing it securely when not in use. Lost or stolen trust-provided mobile phones must be reported immediately to the IT department and the line manager.

Trust mobile phones will be assigned to specific personnel who should review this policy before use. This will ensure a controlled and responsible approach to mobile phone usage within the premises. Where mobile telephones are used on a pool basis, a system and log for identifying users should be maintained.

Mobile phones, whether trust-provided or personal, should not be used to capture or share confidential patient information. Staff members are reminded to always uphold patient privacy and confidentiality.

When going on home visits it is permissible for staff to keep their trust mobile phones with them. This is to ensure the safety of the staff member.

The provided mobile telephone is at all times the property of the Trust.

There are also ward telephones which are used in case staff need to be contacted, for example, regarding a family emergency.

Personal Mobile Phones:

The use of personal mobile phones by staff in an inpatient environment is prohibited. Personal mobile phones should be stored away in lockers that are provided and are only to be used at designated break times.

Community staff can keep their mobile phones on them but they must not be used in front of service users. They should only be used on breaks.

In addition, ringtones or music played via mobile phones could disturb patients who are trying to recuperate, and noise created from the use of mobile phones could be disruptive to those patients wishing to rest. Loud ring tones and alarms on mobile phones can also be confused with alarms or medical equipment. Mobile phones should be kept on vibrate or silent when in inpatient areas.

Staff must be mindful of moderation of tone, volume and language when using mobile phones on Trust premises.

During 1-1 observations, staff are expected to refrain from using their phones to ensure active interaction with service users.

Staff must not access illegal or explicit internet sites or sites with adult-only content whilst on Trust premises.

Staff personal mobile phones are their own responsibility when on Trust property.

All staff are empowered to challenge the misuse of mobiles on site. Any signs of device misuse should be reported to a manager.

Use of camera on phone:

Service users should not feel uneasy about potential recording. Staff members are reminded that taking photos or recordings of service users with personal mobile phones is not allowed, and any such incidents should be reported immediately.

Integrated cameras/document management functions within any form of personal mobile communication should never be used for clinical purposes. Cameras are provided for official use.

Managers may use trust devices for capturing photos required for identification purposes. This is for staff photos only.

Where you are using a Trust device to take images of a patient or their relative/carer, you must obtain their consent before the image is taken and inform them of the purposes for which the images will be used.

Exemptions:

There are some special circumstances where it is acceptable for mobile phones to be used where normally forbidden within this Policy. These are considered to be:

- Senior on-call clinicians and managers who may need to be urgently contacted whilst in a patient area.
- Where there is a clinical imperative that negates the use of all other means of communication.
- Phones should only be visible in front of service users in emergency cases. For example, safety reasons.
- To enable staff to operate a buddy system so they can share information on staff whereabouts.
- To engage and interact with service users where appropriate.
- When a major incident is declared.
- Phones can be used for mobile hotspot if there is no access to Wi-Fi.

7.5 Information held on Trust mobile devices

Confidential Trust information may only be stored on Trust mobile devices with the permission of the relevant Director or Head of Department and the Chief Digital Information Officer or Caldicott Guardian.

Where confidential information is approved for storage on a mobile device, only the minimum amount of personal information necessary for the specific business purpose must be used.

Information must not be stored permanently on mobile devices. If it is necessary to work away from the Trust, information should be transferred back to the Trust server and deleted from the mobile device as soon as possible.

Unauthorised software must not be installed onto Trust mobile devices.

Information must be virus checked before transferring onto Trust computers. This will be done automatically for non-confidential information that is sent via email. (Confidential information may only be sent outside the Trust if it is encrypted using an approved method in line with the SHSC Data & Information Sharing policy).

Confidential information may only be saved to USB sticks where those devices are encrypted to nationally required standards. Any such devices for use within the Trust must be purchased via the IT department who will register them for use on the Trust network. Should it be necessary to use USB devices with equivalent levels of security from partner organisations these must be registered with and approved by the SHSC IT Department.

Any other USB storage devices will be restricted to read-only operation on Trust equipment.

CD/DVD drives connected to Trust PCs will be prevented from writing to disc unless specifically approved by the SHSC IT department.

7.6 Information held on Personal mobile devices (BYOD)

Trust information must not be stored on non-Trust equipment, for example, home personal computers or laptops unless this has been approved as part of the SHSC Bring Your Own Device (BYOD) arrangements.

Only personal devices that have been authorised by ICT Operations and the respective line manager shall be authorised for use.

All devices authorised shall be configured and operated in accordance with and supporting data and information governance policies.

7.7 Security of Storage Devices

Information stored on any mobile devices must be protected by adequate security including regular back up procedures and up to date anti-virus software. It is the responsibility of the individual to virus-check portable storage devices such as memory sticks. Backup copies of confidential information held on mobile devices should be made to a secure Trust server – if this is not possible, the user must make sure that any backup information is kept secure.

Any confidential data to be stored on a PC or other removable device in a non-secure area or on a portable device such as a laptop, tablet or mobile phone must be

encrypted using an encryption solution authorised by the IT department which meets national requirements.

When using encrypted devices, users are responsible for managing their own passwords or phrases. These should be kept securely but users should be aware that if they are forgotten, the IT Department will not be able to retrieve them and it will not be possible to decrypt. Passwords must not be kept with the device (such as on Post-It notes or labels attached to the device) or written down in an easily accessible place.

Passwords should not be shared with other people and you should change your password if you suspect that it has become known to another person.

The installation and configuration of laptop and mobile device security functionality, including access control, encryption and tamper-resistance must be undertaken by appropriately trained IT Department staff. Access controls will be in line with national guidance and subject to encryption solutions which conform to national requirements.

Users will be instructed in the use of encryption software when it is installed on their mobile device or a new device is issued to them. Advice on encryption can be sought from the IT Service Desk.

7.8 The security of mobile devices and information

Mobile devices and confidential information, whether hard-copy or electronic, must be protected by adequate security, for example, they must be:

- Kept out of sight - for example in the locked boot of the car when being transported.
- Not left unattended - for example, not left in the car boot overnight.
- Locked away when not being used.
- Kept secure and guarded from theft, unauthorised access and adverse environmental events particularly when taken home.
- Encrypted (in the case of electronic devices).

Trust equipment must be returned to the IT Department when requested by the IT Department.

Data stored on NHS laptops or other mobile devices must be securely erased by the IT Department before the laptop is reassigned for another purpose or disposed of when redundant. Failure to securely erase data may result in that data being available to a subsequent user of the laptop/mobile device.

7.9 Use of portable media by external visitors to the Trust

External visitors, for example lecturers, contractors, company representatives, patients or their representatives, must not connect any device, including USB sticks and laptops, or insert any media into any equipment belonging to the Trust without authorisation from a member of Trust staff. Any such device must be virus-scanned by up to date anti-virus software provided by the Trust before any files contained within the device may be opened or copied. Should a virus be discovered the device must be disconnected immediately and the IT Service Desk informed.

7.10 Assessment of Risk when taking confidential information off-site

Confidential information must not be taken off Trust premises unless it is absolutely necessary for the performance of Trust business and it must be returned to secure Trust premises as soon as it is practical to do so.

Where it is necessary to take confidential information off Trust premises then the responsible manager must undertake an assessment of the risks involved and take appropriate action to minimise those risks.

The relevant Information Asset Owner must be informed of and approve the removal of confidential information from Trust premises. For routine processes where confidential information is taken off Trust premises the risk assessment must be documented and notified to the Trust Data Protection Officer.

Where possible, the information should be in electronic form and stored on a device encrypted to national standards as described elsewhere in this policy. If information is in the form of hard-copy documents special care must be taken to ensure that these are not left unattended in surroundings which are not secure from unauthorised access – for instance they must not be left in view in a public place or in an unlocked vehicle or left in any place where they could be accessed by other people such as members of the family within the home.

Staff are not permitted to take SHSC printers for use away from SHSC premises and they may not print work documents to home printers.

Hard-copy confidential information which is taken off Trust premises or is produced away from Trust premises and is no longer needed must be returned to Trust premises for secure destruction. It must not be disposed in normal household waste. Where staff are remotely-based and do not usually visit Trust premises, arrangements for secure destruction of hard-copy confidential information must be agreed with the line manager and documented as part of the Agile Working Agreement Form.

If any confidential information is lost or subject to unauthorised access whilst away from Trust premises this must be reported as soon as possible using the Trust's incident reporting procedures.

7.11 Use of Social Media

The Trust has a separate Social Media Policy which provides guidance on the use of social media, available via the SHSC intranet (JARVIS).

7.12 WhatsApp and other Instant Messaging Services

WhatsApp and similar messaging services (Signal, Telegram, TikTok and others) offer an easy way to share information between a group of users.

Whilst it may offer secure transmission of messages to members of the group, NHS trusts and other public services have been reprimanded by the ICO for unauthorised and uncontrolled use of WhatsApp by staff to transfer confidential service user information. Information has been shared with groups that include members outside the organisation and where information is shared outside official channels, there is a danger that relevant information is missing from the official record.

Within SHSC, the use of WhatsApp and similar instant messaging services for the transfer of confidential service user information is not permitted.

WhatsApp and similar instant messaging services should not be used by staff to communicate with service users.

WhatsApp may be used for communication of organisational (non-personal) information between groups of SHSC-staff for specific work-related purposes, for instance emergency planning and incident management groups.

Any such groups operating within the Trust must have a nominated administrator who is responsible for keeping group membership up to date and for ensuring that any information shared within the group is transcribed into official corporate records as appropriate.

The administrator is responsible for checking the terms and conditions of use for the service and ensuring that these are appropriate for the group. Members of the group should set passcodes on their phones, disable message notifications on the lock screen to avoid inadvertent disclosure of information, and enable remote-wipe in case of theft.

WhatsApp and similar services must never be used to avoid scrutiny of work messages and decision making. Any messages sent for work purposes may be disclosable under Freedom of Information (FOI) regulations and the group administrator is responsible for identifying any information within messages which is relevant to FOI requests and providing it within the specified timescales.

7.13 Reporting Incidents and Weaknesses

An Information Incident is an event that could compromise the confidentiality of information (if it is lost or could be viewed by or given to unauthorised persons), the integrity of the data (if it could be inaccurate or content could have been changed) or the availability of the information (access).

Examples of information incidents are:

- Potential and suspected disclosure of NHS information to unauthorised individuals.
- Loss or theft (attempted or actual) of paper records, data or IT equipment on which data is stored.
- Disruption to systems and business processes.
- Attempts to gain unauthorised access to computer systems, e.g. hacking.
- Records altered or deleted without authorisation by the data “owner”.
- Virus or other malicious malware attacks (suspected or actual).
- “Blagging” offence where information is obtained by deception.
- Breaches of physical security e.g. forcing of doors or windows into secure rooms or filing cabinets containing NHS sensitive or other UK Government information left unlocked in an accessible area.
- Leaving a desktop or laptop unattended when logged-in to a user account without locking the screen to stop others accessing information.
- Human error such as emailing data to the wrong recipient by mistake.
- Covert or unauthorised recording of meetings and presentations.
- Damage or loss of information and information processing equipment due to theft, fires, floods, failure of equipment or power surges.
- Deliberate leaking of information.
- Insider fraud.[1]
- Smartcard or application misuse.
- Smartcard theft.
- Non-compliance with local or national RA policy.
- Any unauthorised access of NHS Digital applications.
- Any unauthorised alteration of patient data.

[1] Where any incidents involving suspected fraud are identified, the Trust’s Fraud, Bribery and Corruption Policy should be followed and advice sought from the Local Counter Fraud Specialist.

The Trust handles considerable amounts of patient data, much of which is sensitive. An information incident involving sensitive data, especially patient confidential information, is considered to be a data/information breach and must be reported.

All information management and technology security incidents and weaknesses must be reported via Trust incident reporting procedures (see Trust Incident Reporting Policy).

Incidents that present an immediate risk to the Trust should be escalated through local supervisor & manager, IT Service Desk and the Data Protection Officer.

Where Trust equipment containing confidential information is reported lost or stolen, the IT Service Desk will follow the standard procedure to remotely wipe or disable the missing equipment.

SIRO & Digital Assurance Group Reporting (DAG)
The Data Protection Officer will keep SIRO & DAG informed of the information incidents status by means of regular reports and immediate alerts where an immediate risk is identified.

8 Development, Consultation and Approval

This policy was originally developed by the city-wide Information Governance Group (SCT and PCTs).

It was tabled at the SCT Information Governance Committee.

It was sent, along with other IG policies to JCF in June 2007 (in light of the heavy workload due to the Foundation Trust application, the policies were considered outside the meeting by staff side).

Following consultation with staff side, the policies were agreed by the Information Governance Committee in September 2007.

The policies were re-formatted in line with revised Trust requirements.

This policy was augmented in light of national guidance on information security, data flows and encryption in March 2008.

The policies in new format were approved by the Information Governance Committee on 10 March 2008.

The policies were approved by the Performance Information Group on 18 March 2008.

This policy was revised and submitted to the Information Governance Steering Group in October 2010

Further amendments made following submission to the Information Governance Steering Group, then submitted to the Performance Information Group.

This policy was revised and minor amendments made in February 2013.

This policy was revised and minor amendments made in February 2014.

This policy was revised as part of a major review of Information Governance policies in 2018 to meet the requirements of legislative change (introduction of the General Data Protection Regulation (GDPR) and Data Protection Act 2018) and the migration from the Information Governance Toolkit to the Data Security & Protection Toolkit which takes account of the National Data Guardian's data security standards.

The policies were approved by the Data & Information Governance Board in May 2018.

This policy was updated in October 2018 to update references and contact details for submission to the November 2019 Data & Information Governance Board.

The policy was revised in April 2022 to account for changes in working practices and technology. It was submitted to the September 2022 Data & Information Governance Group.

The policy was revised in April 2024 to include further guidance on the use of mobile phones and the addition of a section covering WhatsApp and other instance messaging services.

9 Audit, Monitoring and Review

This section should describe how the implementation and impact of the policy will be monitored and audited. It should include timescales and frequency of audits.

If the policy is required to meet a particular standard, it must say how and when compliance with the standard will be audited.

Monitoring Compliance Template						
Minimum Requirement	Process for Monitoring	Responsible Individual/ group/committee	Frequency of Monitoring	Review of Results process (e.g. who does this?)	Responsible Individual/group/ committee for action plan development	Responsible Individual/group/ committee for action plan monitoring and implementation
Compliance with this policy in terms of use of mobile devices and associated software	Review in light of any incidents, staff requests and suggestions	Information Governance Manager; Head of Informatics; Head of Service Delivery & Infrastructure; IT Dept.	Annual	Digital Assurance Group	Information Governance Manager; Deputy Directors of Digital; IT Dept.	Digital Assurance Group

Policy documents should be reviewed every three years or earlier where legislation dictates or practices change. The policy review date should be written here – 03/2024

10 Implementation Plan

Action / Task	Responsible Person	Deadline	Progress update
Upload to Intranet	Communications Dept.	07/2024	
Distribute communications	Communications Dept.	07/2024	
Provide training and awareness	IMST	Ongoing	
Review against progress and operational need	DAG	06/2025	

11 Dissemination, Storage and Archiving (Control)

Version	Date added to intranet	Date added to internet	Date of inclusion in Connect	Any other promotion/ dissemination (include dates)
1.7	08/2018	08/2018		
1.8	11/2019	11/2019		
1.9	11/2022	11/2022		
2.0	07/2024	07/2024		

12 Training and Other Resource Implications

Information Governance training is mandatory for all staff on induction and on a yearly basis.

The Information Governance Team will work with the Learning Development team and managers to ensure that appropriate additional training is available to support staff.

The Information Governance team will work the Senior Information Risk Owner, Data & Information Managers and other appropriate managers and teams to maintain continued awareness of confidentiality and security issues to both the organisation and staff through staff emails, newsletters, intranet etc.

13 Links to Other Policies, Standards (Associated Documents)

The Trust and its employees, including non-Trust employees authorised to access Trust Information and systems, are obliged to comply with the following legislation and requirements:

- SHSC Data & Information Sharing Policy
- SHSC Social Media Policy
- SHSC Agile Working Policy
- Common Law Duty of Confidentiality
- Data Protection Act/UK GDPR
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Confidentiality: NHS Code of Practice
- Records Management: NHS Code of Practice
- Fraud, Bribery and Corruption Policy

And any relevant guidance related to the following:

- Information Quality Assurance
- Information Security
- Information Governance Management

14 Contact Details

Title	*Name*	*Phone*	*Email*
Senior Information Risk Owner (SIRO)	Phillip Easthope	0114 3050765	phillip.easthope@shsc.nhs.uk
Chief Digital Information Officer	Chris Reynolds	0114 2664960	chris.reynolds@shsc.nhs.uk
Head of Service Delivery & Infrastructure	Adam Handley	0114 3050770	adam.handley@shsc.nhs.uk
Information Governance Manager	Katie Hunter	0114 2716723	katie.hunter@shsc.nhs.uk
Data Protection Officer	John Wolstenholme	0114 3050749	john.wolstenholme@shsc.nhs.uk

Appendix A

Equality Impact Assessment Process and Record for Written Policies

Stage 1 – **Relevance** - Is the policy potentially relevant to equality i.e. will this policy potentially impact on staff, patients or the public? This should be considered as part of the Case of Need for new policies.

NO – No further action is required – please sign and date the following statement. **I confirm that this policy does not impact on staff, patients or the public.**	***I confirm that this policy does not impact on staff, patients or the public.*** Name/Date: J Wolstenholme, 09 April 2024	**YES,** Go to **Stage 2**

Stage 2 Policy Screening and Drafting Policy - Public authorities are legally required to have 'due regard' to eliminating discrimination, advancing equal opportunity and fostering good relations in relation to people who share certain 'protected characteristics' and those that do not. The following table should be used to consider this and inform changes to the policy (indicate yes/no/ don't know and note reasons). Please see the SHSC Guidance and Flow Chart.

Stage 3 – **Policy Revision** - Make amendments to the policy or identify any remedial action required and record any action planned in the policy implementation plan section

SCREENING RECORD	Does any aspect of this policy or potentially discriminate against this group?	Can equality of opportunity for this group be improved through this policy or changes to this policy?	Can this policy be amended so that it works to enhance relations between people in this group and people not in this group?
Age			
Disability			
Gender Reassignment			
Pregnancy and Maternity			

Race			
Religion or Belief			
Sex			
Sexual Orientation			
Marriage or Civil Partnership			

Please delete as appropriate: - Policy Amended / Action Identified (see Implementation Plan) / no changes made.

Impact Assessment Completed by:
Name /Date

Appendix B

Review/New Policy Checklist

This checklist to be used as part of the development or review of a policy and presented to the Policy Governance Group (PGG) with the revised policy.

		Tick to confirm
	Engagement	
1.	Is the Executive Lead sighted on the development/review of the policy?	✓
2.	Is the local Policy Champion member sighted on the development/review of the policy?	✓
	Development and Consultation	
3.	If the policy is a new policy, has the development of the policy been approved through the Case for Need approval process?	N/A
4.	Is there evidence of consultation with all relevant services, partners and other relevant bodies?	✓
5.	Has the policy been discussed and agreed by the local governance groups?	✓
6.	Have any relevant recommendations from Internal Audit or other relevant bodies been taken into account in preparing the policy?	✓
	Template Compliance	
7.	Has the version control/storage section been updated?	✓
8.	Is the policy title clear and unambiguous?	✓
9.	Is the policy in Arial font 12?	✓
10.	Have page numbers been inserted?	✓
11.	Has the policy been quality checked for spelling errors, links, accuracy?	✓
	Policy Content	
12.	Is the purpose of the policy clear?	✓
13.	Does the policy comply with requirements of the CQC or other relevant bodies? (where appropriate)	✓
14.	Does the policy reflect changes as a result of lessons identified from incidents, complaints, near misses, etc.?	✓
15.	Where appropriate, does the policy contain a list of definitions of terms used?	✓
16.	Does the policy include any references to other associated policies and key documents?	✓
17.	Has the EIA Form been completed (Appendix 1)?	✓
	Dissemination, Implementation, Review and Audit Compliance	
18.	Does the dissemination plan identify how the policy will be implemented?	✓
19.	Does the dissemination plan include the necessary training/support to ensure compliance?	✓
20.	Is there a plan to i. review ii. audit compliance with the document?	✓
21.	Is the review date identified, and is it appropriate and justifiable?	✓