Policy:

IMST 009 - Remote Working & Mobile Devices

Executive or Associate Director lead	Executive Director of Finance & SIRO
Policy author/ lead	Assistant Deputy Director of IMS&T (Informatics and Architecture)
Feedback on implementation to	Assistant Deputy Director of IMS&T (Informatics and Architecture)

Document type	Version 1.8
Date of initial draft	18/10/2019
Date of consultation	
Date of verification	11/11/2019
Date of ratification	21/11/2019
Ratified by	Executive Directors' Group (EDG)
Date of issue	26/11/2019
Date for review	30 May 2020

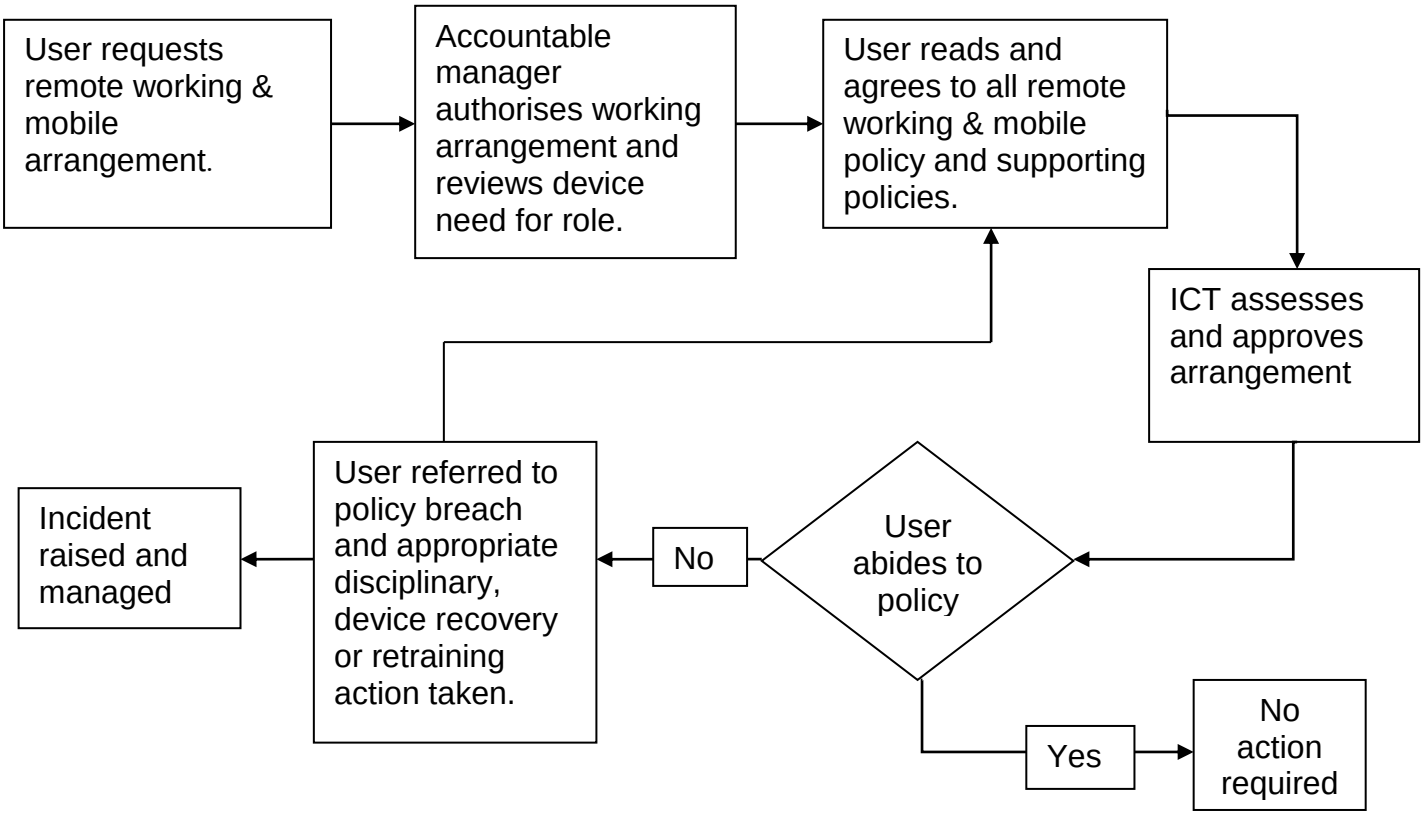
Target audience	SHSC staff and people authorised to access the SHSC network

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

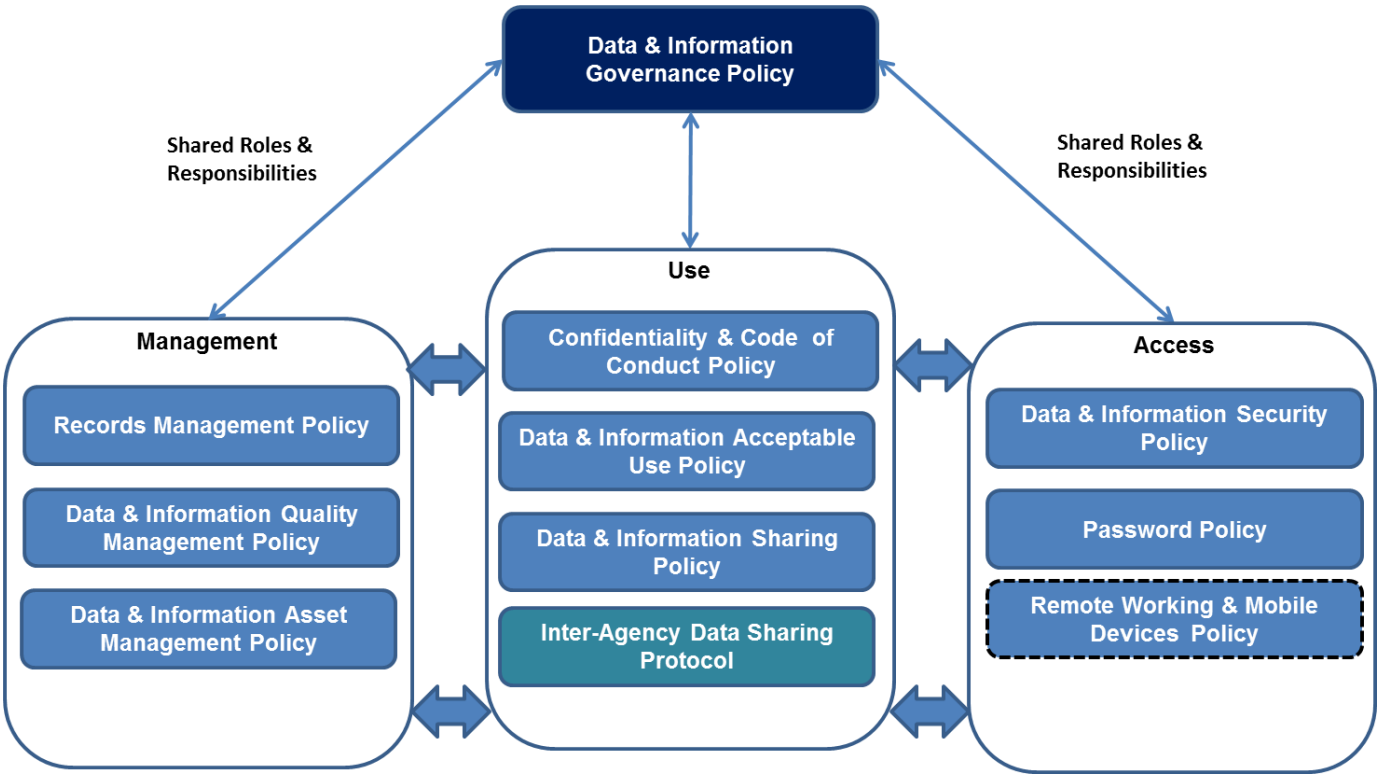
Policy Version and advice on document history, availability and storage
Update of existing 1.7 Remote Working & Mobile Devices policy. Also replaces Mobile Communication policy version 1.

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 or may need to occasionally work away from their normal base. 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 - presents their greatest 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 FT (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
- General Data Protection Regulation
- 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. Definitions

Remote Working
Mobile and remote working is the term used to describe working away from your usual workplace. 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, PC's, USB Memory devices and other forms of digital storage.

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

4. 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

5. 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
Chief Information Officer	CIO	Director IMST	Responsible for the Information Technology that supports the overarching strategies of the Trust.
Chief Clinical Information Officer	CCIO	Director Medical	Providing a vital voice for clinical strategy, allowing new IT and Data & Information products to help improve the provision of healthcare.
Senior Information Risk Owner	SIRO	Director Finance	Owns the Trust's information risk policy and risk assessment process.
Caldicott Guardian	CG	Director Nursing	Responsible for protecting the confidentiality of patient and service user information and enabling the appropriate level of information sharing.
Data Protection Officer	DPO		Supporting Trust -wide Data & Information governance in accordance to GDPR, NHS Digital & England and Data Security & Protection Toolkit.
Clinical Information Officer	CLIO		Supporting the Chief Clinical Information Officer and trust - wide clinical initiatives for increased data and information usage and opportunities, supported by data and information governance framework.
Cyber Security Officer	CSO		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.
Data & Information Asset Owners	DIAO	Directorate	Senior representatives of the directorates closely aligned to major stores of organisational data, information and systems.
Data & Information Asset Managers	DIAM	Service Managers	Primary administrative and management responsibilities for segments of data primarily associated with their functional area.
Data & Information Asset Supervisors	DIAS	Supervisors / Team Leaders	Supervisors have responsibility for the day-to-day maintenance and protection of data & information when they are affected by the processes that they manage.

Data & Information Asset Users	DIAU	All Users	Responsibility lies with all staff to make sure that all policies and security measures are adhered to.
Data & Information Asset Stewards	DIAS	IMST & Suppliers	Trust and third party IMST enabling and supporting secure & compliant data and information technical implementation, governance and guidance throughout the Trust and in accordance to trust policy, national guidelines and regulations.

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 (move line below to this line)
ones) plus other authorised users of systems are required to adhere to this policy.

6 Process

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. (move line below to this line)
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 laptops are physically secured to desks wherever possible using appropriate locking mechanisms, especially when left unattended.
- 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 your organisation's policy.
- Immediately report any actual or suspected loss, theft or unauthorised access/disclosure of devices, documents or information.

Don't

- Work with or discuss security classified 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.

6.1 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 be protected by 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.

6.2 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. A request for remote access can be made by completing the electronic Request for Remote Access form which is available via the Trust intranet.

6.3 Connection to non-NHS Networks

Trust equipment must not be connected to the internet via a commercial internet service provider without prior authorisation by the IT Department because of the risk to the security of the information held on them and the risk of introducing viruses onto the Trust network.

6.4 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 Help 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 telephone/device allows access to the intranet, such as a PDA or WAP telephone, any use of that facility is governed by the Trust Data & Information Acceptable Use and supporting policies.

The user should not ordinarily give their mobile telephone number to patients or carers. (Any patient 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.

Mobile phones should be switched off during meetings, lectures, seminars, training courses etc. other than in very exceptional circumstances where it is necessary to take an urgent call. In these circumstances it is courteous to alert colleagues to the fact than an urgent call is expected.

The mobile phone should be switched to silent/discreet mode when the user is with a patient/carer. The use of a mobile phone within NHS premises should be checked before use due to possible interference with electronic medical equipment.

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.

Many departments/buildings have local rules regarding the use of mobile phones and these must always be respected.

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. The user may be responsible for any loss or damage if reasonable precautions are not taken.

The user should be aware that calls from mobile telephones are expensive (including the use of text messaging) and therefore, discussion should be clear, succinct and to the point. The user should always use a landline where available in preference to their mobile phone.

Where appropriate mobile telephones will be used on a pool basis. A system and log for identifying users is required by the Department/Team.

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

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 Trust Director of IM&T 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 e-mail 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.

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

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

Information held on Personal mobile devices (BYOD)

Trust information must not be stored on non-Trust equipment, for example, home personal computers, laptops and PDAs 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.

6.5 Storage Devices Security

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, PDA 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 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 Help Desk.

6.6 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 for a “health check” at regular intervals as specified by the IT Department, or at their specific request.

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.

6.7 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. Should a virus be discovered the device must be disconnected immediately and the IT Help Desk informed.

6.8 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 Information Manager.

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.

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.

6.9 Use of Social Media

The Trust has a separate "Social Media Policy - Acceptable Use for Staff" which provides guidance on the use of social media, available via the SHSC intranet.

6.10 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 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 of local or national RA policy.
- Any unauthorised access of HSCIC applications.
- Any unauthorised alteration of patient data.

The Trust handles considerable amounts of patient data and this can be 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 Helpdesk & Data Protection Officer.

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

7. Dissemination, storage and archiving (Control)

This policy replaces version 1.5 Information Security Policy. The policy is to be made available on the Trust intranet and available to all staff.

8. 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.

[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 (robert.purseglove@nhs.net).

9. Audit, monitoring and review

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 the Internet and related systems	Review in light of any incidents, staff requests and suggestions	Information Manager; Head of Informatics and Information Systems; IT Dept.	Annual	Data & Information Governance Board	Information Manager; Head of Informatics and Information Systems; IT Dept.	Data & Information Governance Board

10. Implementation plan

Action / Task	**Responsible Person**	**Deadline**	**Progress update**
Upload to Intranet	Corporate Affairs	TBC	26/11/2019
Distribute communications	Corporate Affairs	TBC	05/12/2019
Provide training and awareness	IMST	TBC	
Review against progress and operational need	DIGB	TBC	

11. Links to other policies, standards and legislation (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:

- Common Law Duty of Confidentiality
- Data Protection Act/GDPR
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Copyright, Designs and Patents Act 1998
- NHS Code of Connection
- 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

12. Contact details

The document should give names, job titles and contact details for any staff who may need to be contacted in the course of using the policy (sample table layout below). This should also be a list of staff who could advise advice regarding policy implementation.

Title	***Name***	***Phone***	***Email***
Senior Information Risk Owner (SIRO)	Phillip Easthope	0114 3050765	Phillip.easthope@shsc.nhs.uk
Assistant Deputy Director of IMS&T	Ben Sewell	0114 2711144	Ben.sewell@shsc.nhs.uk
Information Manager	John Wolstenholme	0114 3050749	John.wolstenholme@shsc.nhs.uk

13. References

The document should include key references for the evidence base, and relevant legislation or government policy.

- The Data Protection Act (2018)
- General Data Protection Regulation
- The Freedom of Information Act (2000)
- Environmental Information Regulations (2004)
- European Directive 2003/4/EC
- Access to Health Records Act (1990)
- Human Rights Act (1998)

- Crime and Disorder Act (1998)
- Criminal Procedures and Investigations Act (1996)
- Regulatory and Investigatory Powers Act (2000)
- ICO Framework Code of Practice for Sharing Personal Information
- (2007)
- Children Act (2004)
- Working together to Safeguard Children (2006)
- NHS Act (2006)
- Multi-Agency Public Protection Arrangements (MAPPA)
- Mental Capacity Act 2005 and Code of Practice (2007)
- Information Sharing Guidance for Practitioners and Managers
- (2008)
- Confidentiality NHS Code of Practice (2003)
- Confidentiality Guidance for Doctors (GMC 2009)
- Confidentiality and Disclosure of Health Information Toolkit (BMA
- 2008)
- The NMC Code of Professional Conduct: Standards for Conduct,
- Performance and Ethics (NMC 2004)
- No Secrets: Guidance on developing and implementing multiagency policies and procedures to protect vulnerable adults from abuse.
- Data Protection and Sharing – Guidance for Emergency Planners and Responders (HMG 2007)
- Data Sharing Review Report (Thomas and Walport 2008)
- Health and Social Care Act (2001)
- Caldicott Guidance (2010)
- To Share or Not to Share – The Information Governance Review (2013)
- Computer Misuse Act 1990
- Department of Health, Records Management: NHS Code of Practice (2006)
- NHS Connecting for Health
- NHS Information Governance, Guidance on Legal and Professional Obligations (Department of Health, 2007)

Appendix A – Version Control and Amendment Log

Version No.	Type of Change	Date	Description of change(s)
1	Policy created	September 2007	Approved by the Information Governance Committee
	Revision	March 2008	Updated in light of national guidance on information security, data flows and encryption
	Revision	October 2010	Update and incorporation of comments from the Information Governance Steering Group
	Revision	February 2013	Minor amendments
	Revision	February 2014	Minor amendments
1.7	Revision	March 2018	Update as part of a wider review of Information Governance policies and incorporation of mobile communication policy
1.8	Revision	Apr – Oct 2019	Updates for legislative and monitoring changes and contact details.

Appendix B – Dissemination Record

Version	Date on website (intranet and internet)	Date of "all SHSC staff" email	Any other promotion/ dissemination (include dates)
1.7	August 2018		

Appendix C – Stage One Equality Impact Assessment Form

Equality Impact Assessment Process for Policies Developed Under the Policy on Policies

Stage 1 – Complete draft policy

Stage 2 – **Relevance** - Is the policy potentially relevant to equality i.e. will this policy potentially impact on staff, patients or the public? If **NO** – No further action required – please sign and date the following statement. If **YES –** proceed to stage 3

This policy does not impact on staff, patients or the public (insert name and date) No. J Wolstenholme, 21 Oct 2019

Stage 3 – **Policy Screening** - 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 on equality impact assessment for examples and detailed advice. This is available by logging-on to the Intranet first and then following this link https://nww.xct.nhs.uk/widget.php?wdg=wdg_general_info&page=464

	Does any aspect of this policy actually 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			

Stage 4 – **Policy Revision** - Make amendments to the policy or identify any remedial action required (action should be noted in the policy implementation plan section)
Please delete as appropriate: Policy Amended / Action Identified / no changes made.

Impact Assessment Completed by (insert name and date)

Appendix D - Human Rights Act Assessment Form and Flowchart

You need to be confident that no aspect of this policy breaches a person's Human Rights. You can assume that if a policy is directly based on a law or national policy it will not therefore breach Human Rights.

If the policy or any procedures in the policy, are based on a local decision which impact on individuals, then you will need to make sure their human rights are not breached. To do this, you will need to refer to the more detailed guidance that is available on the SHSC web site
http://www.justice.gov.uk/downloads/human-rights/act-studyguide.pdf
(relevant sections numbers are referenced in grey boxes on diagram) and work through the flow chart on the next page.

1. Is your policy based on and in line with the current law (including case law) or policy?

✓ **Yes. No further action needed.**

☐ **No. Work through the flow diagram over the page and then answer questions 2 and 3 below.**

2. On completion of flow diagram – is further action needed?

☐ **No, no further action needed.**

☐ **Yes, go to question 3**

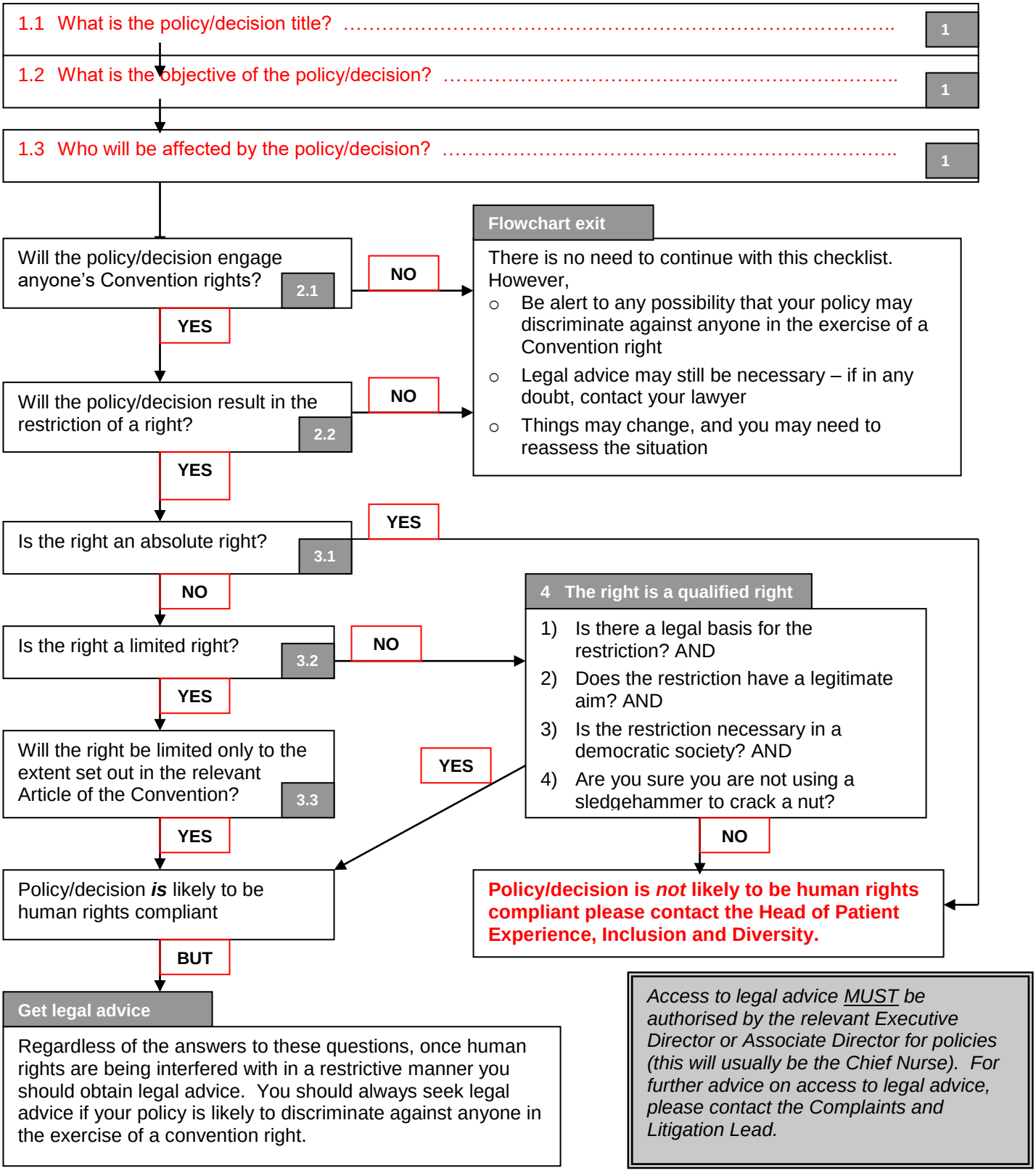
3. Complete the table below to provide details of the actions required

Action required	By what date	Responsible Person

Human Rights Assessment Flow Chart

Complete text answers in boxes 1.1 – 1.3 and highlight your path through the flowchart by filling the YES/NO boxes red (do this by clicking on the YES/NO text boxes and then from the Format menu on the toolbar, choose 'Format Text Box' and choose red from the Fill colour option).

Once the flowchart is completed, return to the previous page to complete the Human Rights Act Assessment Form.



Appendix E – Development, Consultation and Verification

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.

Appendix F –Policies Checklist

Please use this as a checklist for policy completion. The style and format of policies should follow the Policy template which can be downloaded on the intranet (also shown at Appendix G within the Policy).

1. Cover sheet ☒

All policies must have a cover sheet which includes:

- The Trust name and logo ☒
- The title of the policy (in large font size as detailed in the template) ☒
- Executive or Associate Director lead for the policy ☒
- The policy author and lead ☒
- The implementation lead (to receive feedback on the implementation) ☒
- Date of initial draft policy ☒
- Date of consultation ☒
- Date of verification ☒
- Date of ratification ☒
- Date of issue ☒
- Ratifying body ☒
- Date for review ☒
- Target audience ☒
- Document type ☒
- Document status ☒
- Keywords ☒
- Policy version and advice on availability and storage ☒

2. Contents page

3. Flowchart ☒

4. Introduction ☒

5. Scope ☒

6. Definitions ☒

7. Purpose ☒

8. Duties ☒

9. Process ☒

10. Dissemination, storage and archiving (control) ☒

11. Training and other resource implications ☒

12. Audit, monitoring and review ☒

This section should describe how the implementation and impact of the policy will be monitored and audited and when it will be reviewed. It should include timescales and frequency of audits. It must include the monitoring template as shown in the policy template (example below).

Monitoring Compliance Template						
Minimum Require-ment	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
A) Describe which aspect this is monitoring?	e.g. Review, audit	e.g. Education & Training Steering Group	e.g. Annual	e.g. Quality Assurance Committee	e.g. Education & Training Steering Group	e.g. Quality Assurance Committee

☒

13. Implementation plan

14. Links to other policies (associated documents) ☒

15. Contact details ☒

16. References ☒

17. Version control and amendment log (Appendix A) ☒

18. Dissemination Record (Appendix B) ☒

19. Equality Impact Assessment Form (Appendix C) ☒

20. Human Rights Act Assessment Checklist (Appendix D) ☒

21. Policy development and consultation process (Appendix E) ☒

22. Policy Checklist (Appendix F) ☒