Policy:

IMST 005 Data, Information & System Asset Management

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	Final Draft
Document status	Version 1.1
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	31/03/2023 (Extended from 30/11/2022)

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

Keywords	Asset, Information, Data, Governance

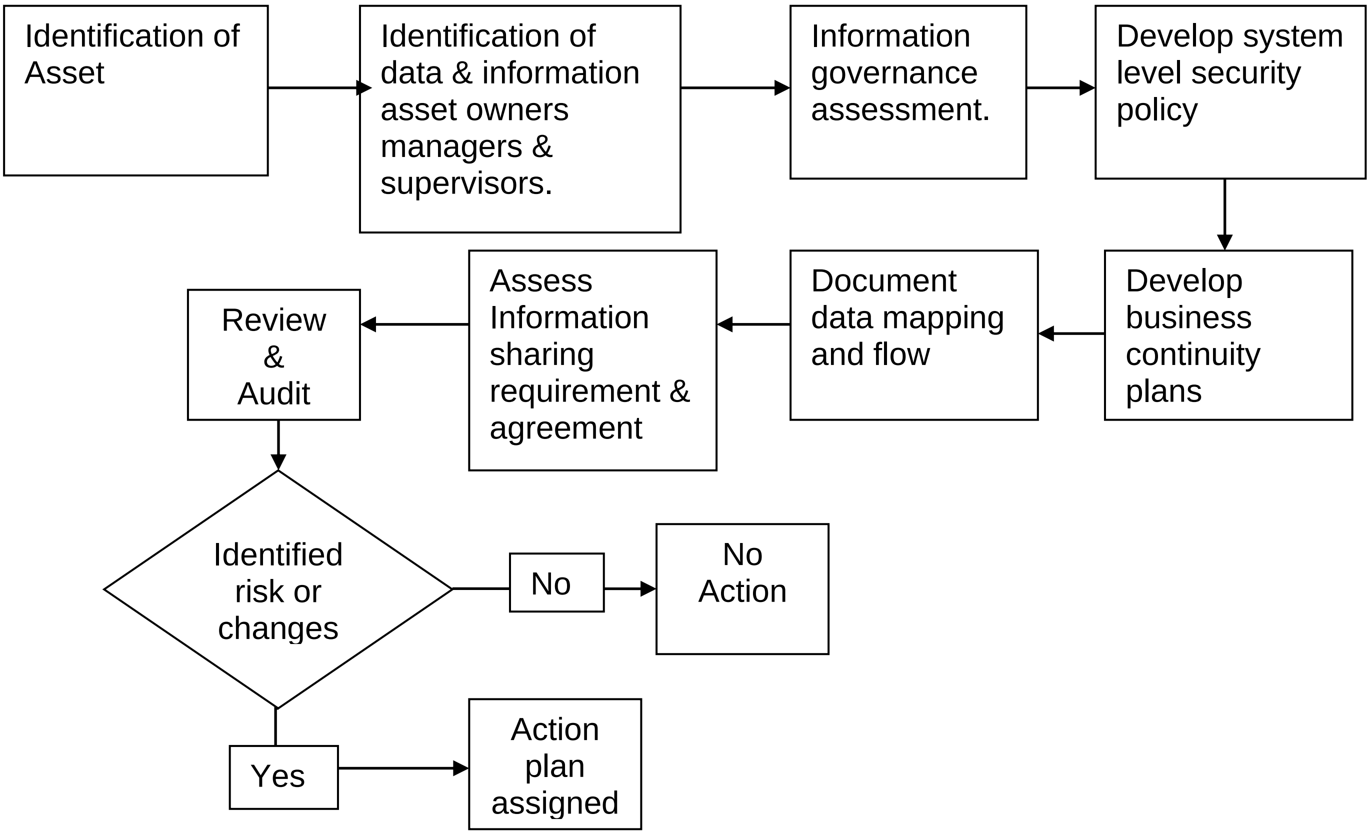
Policy Version and advice on document history, availability and storage

New Policy aligning to Data & Information Governance and supporting policies.

Revised October 2019

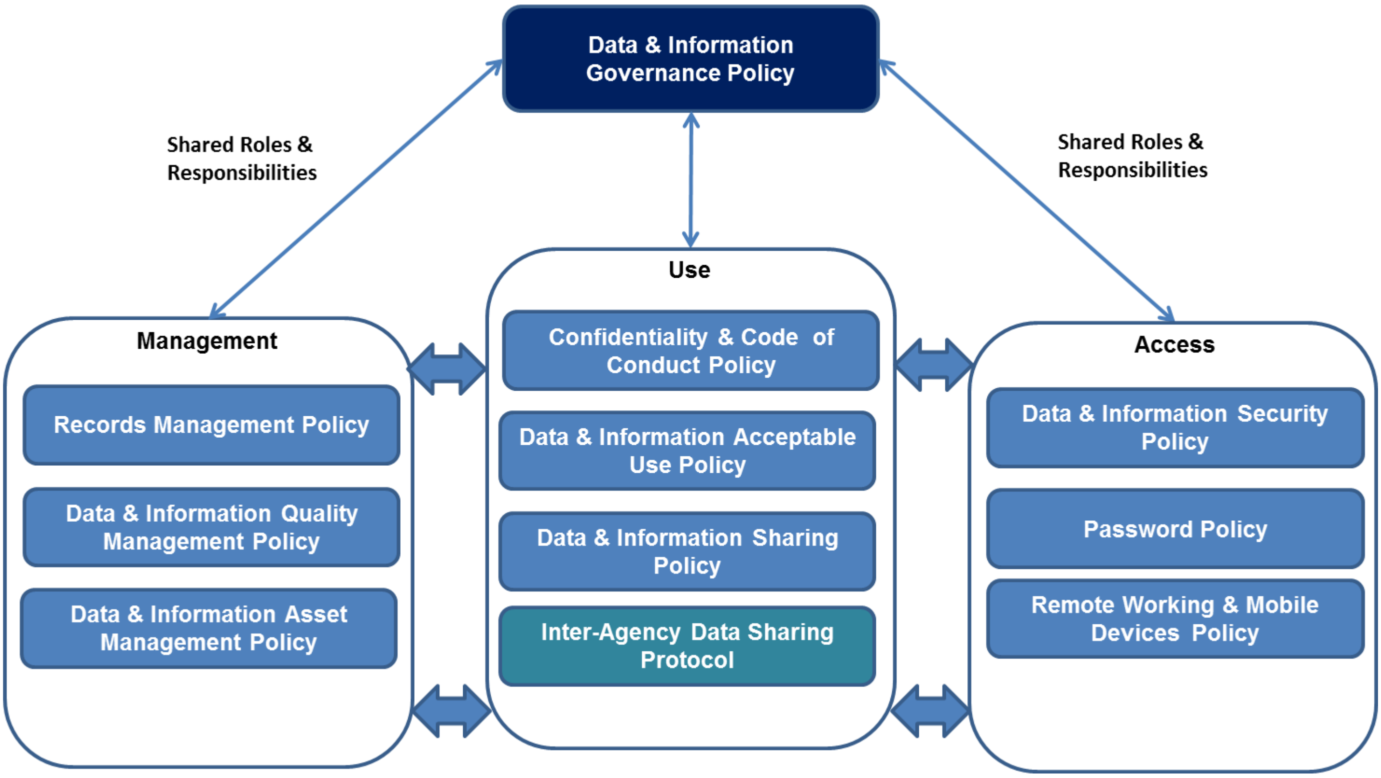
Contents

Flow Chart



Identification of Asset
Identification of data & information asset owners managers & supervisors.
Information governance assessment.
Develop system level security policy
Develop business continuity plans
Document data mapping and flow
Assess Information sharing requirement & agreement
Review & Audit
Identified risk or changes
No
No Action
Yes
Action plan assigned

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



Data & Information Governance Policy
Shared Roles & Responsibilities
Shared Roles & Responsibilities
Management
Records Management Policy
Data & Information Quality Management Policy
Data & Information Asset Management Policy
Use
Confidentiality & Code of Conduct Policy
Data & Information Acceptable Use Policy
Data & Information Sharing Policy
Inter-Agency Data Sharing Protocol
Access
Data & Information Security Policy
Password Policy
Remote Working & Mobile Devices Policy

1. Introduction

Trust Data & Information Asset Management policy for identifying, managing and controlling key data and information assets in accordance to National Guidelines, and supporting required GDPR / DPA practices and processes.

2. Scope

The scope of this document is to outline the Trust's policy for Data & Information Security 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

Data & Information Asset

An information asset can be defined as a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.

The Data Security & Protection Toolkit categorise an information asset as:

Information: Databases, system documents and procedures, archive, media/data, paper records.

- Software: Application programs, system development tools and utilities.
- Physical: Infrastructure, equipment, furniture and accommodation used for data processing.

- Services: Computing and communications, heating, lighting, power, air conditioning used for data processing.
- People: Their qualifications, skills and experience in the use of information systems.
- Intangibles: For example, public confidence in the organisation’s ability to ensure the Confidentiality, Integrity and Availability of personal data.

An asset can be a single significant document or a set of related data, documents or files. It can be shared or be confined to a specified purpose or organisational unit. It will have recognisable and manageable value, risk, content and lifecycle. The Trust has hundreds of such systems, both electronic and paper-based, that hold information relating to service users and staff.

Critical Information Asset

A critical information asset is one which the organisation is reliant on and cannot operate without. The result of the critical information asset being unavailable for up to 24 hours will disrupt and effect patient care, quality of service and the operations of the organisation.

System Level Security Policy (SLSP)

Demonstrates understanding of information governance risks and commitment to address the security and confidentiality needs of a particular system.

4. Purpose

Provides a clear policy for Trust Data & Information Asset management practices for all Data and Information Governance roles and responsibilities.

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	CCIO	Director Medical	Providing a vital voice for clinical strategy, allowing new IT, Data &

Officer			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 plus other authorised users of systems are required to adhere to this policy.

6 Process

To assess whether a body of information should be considered a data and information asset the questions below should be asked:

- Does it have a value to the organisation?
- Does it have a specific content?
- Does it have a manageable lifecycle?
- Is there a risk associated?
- Does it have a purpose?
- Does it have a disposal schedule?

All critical assets must have a SLSP and business continuity plan in place.

The Data & and Information implementation process is managed by the Informatics and Information Systems team within the trust, with the support of identified Data and Information Asset Managers, Supervisors and the Trust SharePoint Data and Information asset register.

In order to give assurance that an asset is not going to be a major risk for the Trust a process of accreditation has been developed in line with national requirements to ensure that assurance can be given that as a Trust we are ensuring the highest level of security and mitigating risk as much as is possible.

6.1 Identification of Asset

The first stage in the process is the identification of the assets and the need for them to be accredited for use. The Informatics and Information Systems team will register the assets in the Data and Governance SharePoint Asset Register; this is the current register for all Trust assets.

Identification of information assets and moving forward as a Trust with the accreditation process will continue to help reduce the risks within the Trust and provide a mechanism for effectively identifying, mitigating and managing risks in relation to identified information assets.

6.2 DIAM/DIAS Identification

When an asset needs a review of its accreditation or a new asset is to be accredited the Informatics and Information Systems Team will assign a lead to help with the process. The first stage is the identification of responsibility and the assignment of a Data and Information Asset Manager and a Data and Information Asset Supervisor. (DIAM/DIAS).

6.3 IG Assessment

The Privacy Impact Assessment (PIA) is a form of risk assessment required for new or changed systems dealing with personal identifiable / sensitive data. A PIA is mandatory on all Information Assets or project processes that involve personal data, but the level of PIA can be proportionate.

Patient Safety Assessment - A form of risk assessment required for assets dealing with service information. DIAM / DIAS are required to consider and answer a set of questions to ensure the asset is not a risk to the safety of patient's and the data we hold and/or process about them. A Patient Safety Assessment is only for clinical systems that hold patient information.

Contractor Requirements - It is essential to ensure that when an asset is accredited for use that the correct checks are carried out on any contractors to reduce the risk to the Trust by ensuring the contractor is fit for purpose and can meet statutory and regulatory standards. The IG team will work to ensure the contractors meet the required IG standards. The checks are:

- ICO register for data controllers
- Data Security & Protection Toolkit for compliance with policy and standards

6.4 System Level Security Policy

In order to further reduce and / or be able to manage risk within the accreditation process a System Level Security Policy is completed to ensure that all aspects of security are considered.

A risk assessment is also carried out with links to the information recorded via the SLSP – each aspect of security is considered and if issues arise they are recorded as part of the risk assessment and all are presented to the SIRO to ensure the risks are acceptable risks for the Trust.

6.5 Business Continuity

Each DIM is required to provide a Business Continuity Plan, which helps the accreditation process to mitigate risks within the Trust. We can be confident that a service has thought about future service provision if a system becomes unavailable.

Business continuity is a core component of corporate risk management and emergency planning. Its purpose is to counteract or minimise interruptions to an organisation's business activities from the effects of major failures or disruption to its Information Assets (e.g. data, data processing facilities and communications).

Approved Business Continuity Plans must be in place for all critical Assets and all staff must be aware of their roles and responsibilities.

DIM have implemented approved procedures and controls for their assets and have effectively informed all relevant staff.

Business continuity plans, system specific procedures and control measures are regularly reviewed, and where necessary tested, to assess their ability to meet their business objectives.

All business continuity plans are to be completed by the DIM and signed off for approval by the SIRO.

6.6 Data Mapping

Within the NHS, numerous urgent and routine transfers of patient and staff information take place each day for the purposes of healthcare and administration of healthcare

services e.g. communications to patients, e-mails to job candidates, patient notes made during a home visit, moving case notes.
It has long been recognised that this information is more vulnerable to loss or compromise when outside the organisation i.e. being carried around or sent / copied from one location to another.
Information mapping is essential as it will help individuals to understand how data is transferred to and from the organisation, and give assurance that measures are in place to ensure data is secure in transit and that it reaches its destination promptly and safely.

6.7 Information Sharing Agreements

The information sharing gateway provides a tool for IG professionals to work electronically with the ability to register recipient organisations and provides a level of assurance against their compliance (i.e. DSPT, PSN etc.). It also signs the organisations up to a common information sharing agreement framework.

The solution then allows data mapping to take place capturing the frequency of data transfer and why, when and how it's being transferred. This enables a risk assessment rating to be generated, so that as a Data Controller we can confirm that flows are lawfully and fairly processed.

This information sharing gateway provides details on where flows of data are coming from (i.e. which asset) and complements the work being done on information asset management. Any information sharing agreements in place should be signed and logged on the portal.

6.8 Review/Audit

The IG team will undertake yearly reviews of assets. The critical assets will be a priority.

The IG team will conduct regular audits and spot checks on the Trust's assets to ensure compliance. The IG team use the ICO Guide to Data Protection Audits as a guide.

The focus of the audit approach will be to determine whether the organisation policies and procedures are being followed operationally with staff in order to reinforce and educate, and to regulate the processing of personal data; also to ensure that processing is carried out in accordance with such policies and procedures. When an organisation complies with its requirements, it is effectively identifying and controlling risks to prevent breaching the GDPR/ DPA.

An audit will typically assess the organisation's procedures, systems, records and activities in order to:

- Ensure the appropriate policies and procedures are in place;
- Verify that those policies and procedures are being followed;
- Test the adequacy controls in place;
- Detect breaches or potential breaches of compliance; and
- Recommend any indicated changes in control, policy and procedure.

6.9 Reporting Incidents and Weaknesses

An Information Security 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 security 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 security 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
The Data Protection Officer will keep SIRO & DIGB informed of the information security status of the Trust by means of regular reports and immediate alerts where an immediate risk is identified.

[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).

7. Dissemination, storage and archiving (Control)

This is a new 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.

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 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

Policy documents should be reviewed every three years or earlier where legislation dictates or practices change. The policy review date should be written here – 30/11/2020.

10. Implementation plan

The implementation plan should be presented as an action plan and include clear actions, lead roles, resources needed and timescales. The Director of Corporate Governance team can provide advice on formats for action plans however; an example layout for the plan is shown below:

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 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)
0.1	Draft policy created	March 2018	New policy created aligning to the Data & Information Governance Strategy
1.0	Amended and approved	May 2018	Minor amendments and approval by Data & Information Governance Board (DIGB)
1.1	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	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**

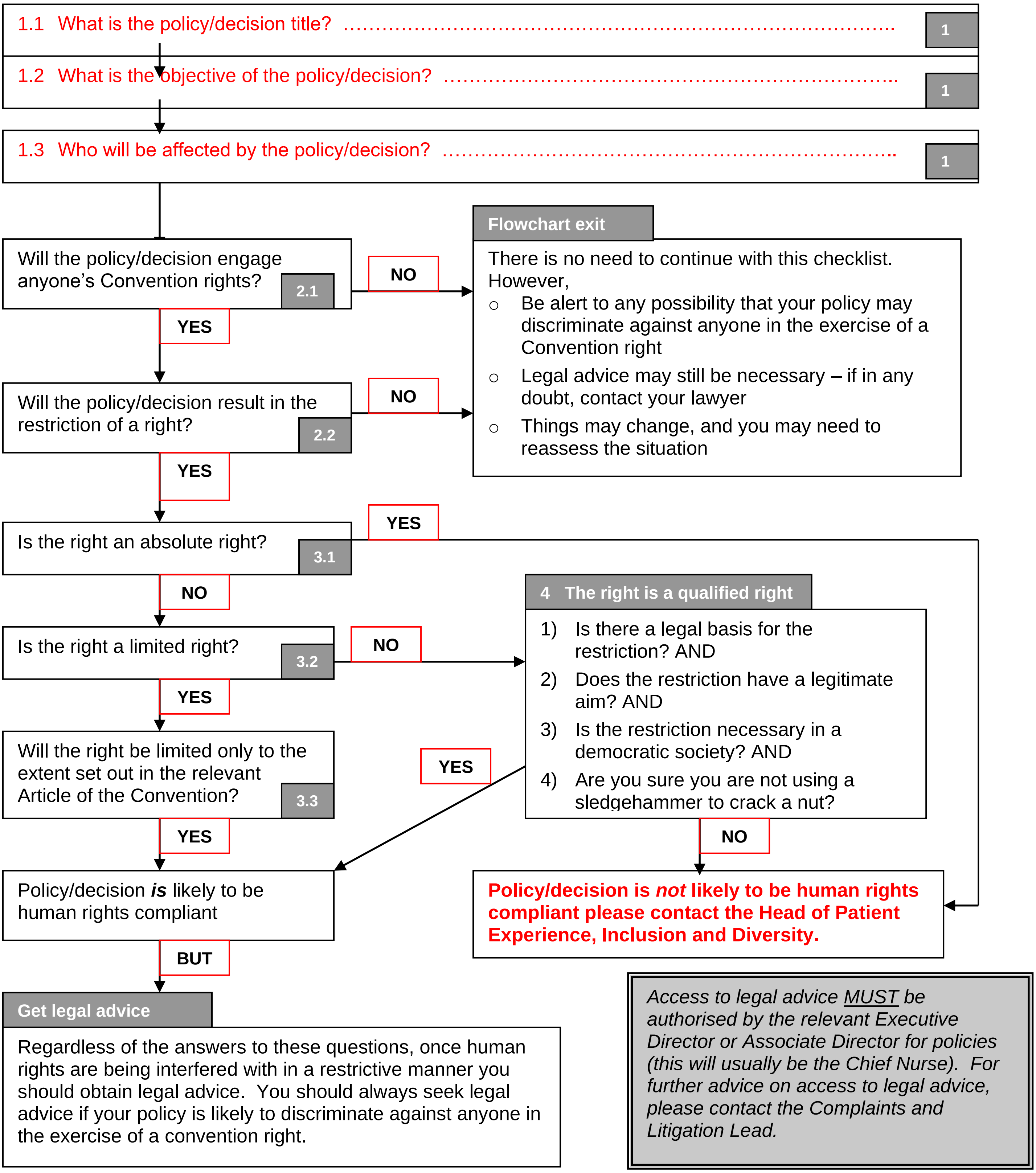
3. **Complete the table below to provide details of the actions required**

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.



1.1 What is the policy/decision title? ……………………………………………………………………..

1.2 What is the objective of the policy/decision? ……………………………………………………………..

1.3 Who will be affected by the policy/decision? ……………………………………………………………..

2.1 Will the policy/decision engage anyone's Convention rights?

2.2 Will the policy/decision result in the restriction of a right?

Flowchart exit

There is no need to continue with this checklist. However,

- Be alert to any possibility that your policy may discriminate against anyone in the exercise of a Convention right
- Legal advice may still be necessary – if in any doubt, contact your lawyer
- Things may change, and you may need to reassess the situation

3.1 Is the right an absolute right?

3.2 Is the right a limited right?

3.3 Will the right be limited only to the extent set out in the relevant Article of the Convention?

4 The right is a qualified right

1) Is there a legal basis for the restriction? AND
2) Does the restriction have a legitimate aim? AND
3) Is the restriction necessary in a democratic society? AND
4) Are you sure you are not using a sledgehammer to crack a nut?

Policy/decision ***is*** likely to be human rights compliant

Policy/decision is *not* likely to be human rights compliant please contact the Head of Patient Experience, Inclusion and Diversity.

Get legal advice

Regardless of the answers to these questions, once human rights are being interfered with in a restrictive manner you should obtain legal advice. You should always seek legal advice if your policy is likely to discriminate against anyone in the exercise of a convention right.

Access to legal advice MUST be authorised by the relevant Executive Director or Associate Director for policies (this will usually be the Chief Nurse). For further advice on access to legal advice, please contact the Complaints and Litigation Lead.

Appendix E – Development, Consultation and Verification

This policy was developed 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) ☒