Policy:

IMST008 Records Management

Executive Director lead for Care Records Executive Director lead for Corporate /Business Records	Executive Director of Operations
Policy author/ lead	Information Manager
Feedback on implementation to	Information Manager

Document type	Version 3.1
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	30/11/2022 (updated from 31/03/2021 by PGG 09/03/2020)

Target audience	All people working on Trust business

Keywords	Records Management, Care Records, Corporate Records, Retention, Disposal

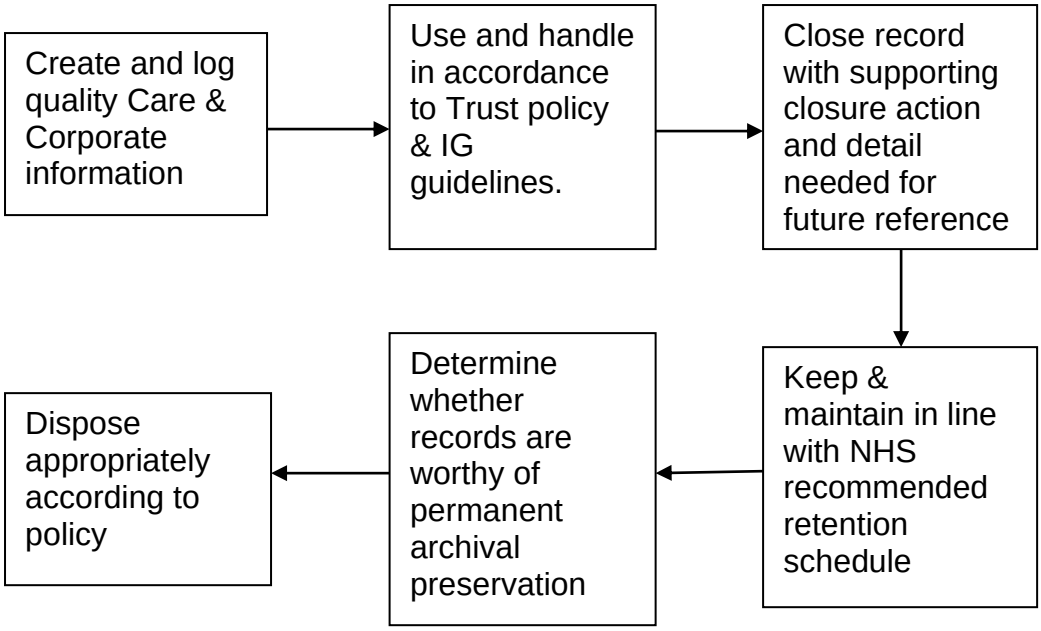
Policy Version and advice on document history, availability and storage
This is version 3.1 of this policy and replaces version 3.

This policy will be available to all staff via the Sheffield Health & Social Care NHS Foundation Trust Intranet and on the Trust's website. The previous version will be removed from the Intranet and Trust website and archived

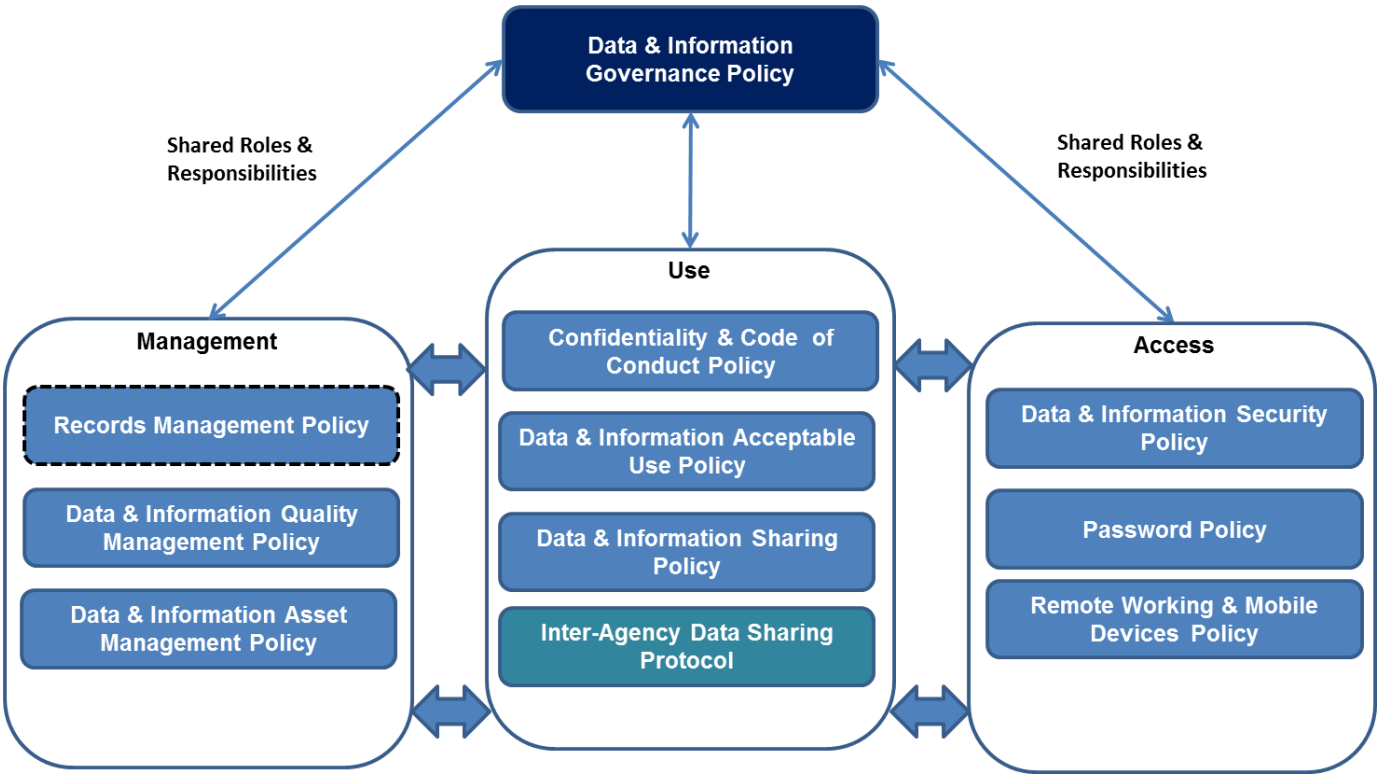
Any printed copies of the previous version should be destroyed and if a hard copy is required, it should be replaced with this version.

Contents

Flow Chart



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

Records Management is the process by which an organisation manages all the aspects of records of their creation, all the way through their lifecycle to eventual disposal. It covers all records whether internally or externally generated and in any format or type of media.

Records Management, through the proper control of the content, maintenance and volume of records, reduces vulnerability to legal challenge or financial loss, supports compliance with legislation and standards, improves control of valuable information resources and promotes best value in terms of human and space resources.

Within the overall context of Records Management care records have a fundamental role in the provision of safe, effective, high quality, evidence- based treatment and care to service users. Accurate and comprehensive recording of information is essential for service user care and continuity of communication between practitioners.

There are legal obligations that apply to the management of records and the Trust will take action as necessary to comply with these obligations. In particular, all NHS records are Public Records under the Public Records Acts. This Trust, in common with all NHS organisations, has a duty under the Public Records Act 1958 to make arrangements for the safe keeping and eventual disposal of all types of its records. In addition it needs robust records management procedures to meet its obligations, particularly under Data Protection legislation, the Access to Health Records Act 1990, the Common Law Duty of Confidentiality, Article 8 of the Human Rights Act 1998 and the Freedom of Information Act 2000. Further information about legal obligations is provided in section 11 of this policy.

This policy aligns to the Information Governance Alliance “Records Management Code of Practice for Health and Social Care” for best practice and statutory obligations.

2. Scope

The scope of this document is to outline the Trust’s policy for Records Management 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 and information belongs to the Trust unless proven otherwise.

3. Definitions

Records
Defined as recorded information, in any form, created or received and maintained by the Trust in the course of its business, providing evidence of its functions, activities and transactions.

Records Management
Discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the Trust and preserving an appropriate historical record. The key components of Records
Management are-

- Record creation;
- Record keeping;
- Record maintenance (including tracking of record movements);
- Access and disclosure;
- Closure and transfer;
- Appraisal;
- Archiving; and
- Disposal.

Record Lifecycle
Describes the life of a record from its creation or receipt through the period of its active use, then into a period of inactive retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or preservation in an archive.

Data & Information Governance
Overarching policy of requirements for handling data, information and systems in a secure and confidential manner according to the best legal, ethical and quality standards detailed in the Data & Information Governance Policy.

4. Purpose

This policy defines a structure for the Trust to ensure adequate records are created and that they are managed in a systematic and planned way from the moment they are created through to their ultimate disposal. It ensures that the Trust can control both the quality and the quantity of the information it generates, that it can maintain the information in a manner that effectively serves its needs, the needs of its service users and the needs of others to whom it is accountable or are affected by or have an interest in its actions and decisions; and that it can dispose of the information efficiently when it is no longer required.

Records Management is a key component of the Information Governance framework for the NHS. The Trust will ensure that the way it manages its records is fully integrated with other Information Governance work areas.

This policy is intended to be complementary to the good record keeping practice set out in various professional codes of conduct.

5. Duties

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, Data & Information products to help improve the provision of healthcare.
Senior Information Risk Owner	SIRO	Director Finance	Owns the Trusts 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 ones) plus other authorised users of systems are required to adhere to this policy.

6. Process

All care and corporate records have a fundamental role to play in the provision of safe, effective, high quality, evidence-based clinical care and effective corporate decision making and personnel management.

Information contained within all records must be recorded accurately, be current, contemporaneous, comprehensive and concise, support effective future action, evidence and legal document requirements.

Must ensure that, where manual records remain in existence, they have the complete record, both manual and electronic, available to them, when it is needed.

Whether manual or electronic, the responsibility for the contents and care of records lies with all Trust staff that handle, write and maintain them.

Set out below are the policy aims for effective management of SHSC's records in order to ensure that:

- Records are available when needed
- Records can be accessed (located and displayed) when needed
- Records can be interpreted
- Records can be trusted
- Records can be maintained and accessed over time despite any changes in format
- Records are secure from unauthorised access, alteration or destruction
- Records are retained and disposed of appropriately

You should use your judgement to decide what is relevant and what should be recorded however, all entries should be complete and adequate for the purpose.

Record facts clearly and where the facts lead to a deduction or opinion make it clear that the statement is an opinion.

Beware of writing judgemental statements, where you are not in a position to judge**.**

Events should be recorded as soon as is practicable after they occur and all entries should be completed within the same working day. If there is a delay the time of the event and the delay should be recorded – electronic records will record the date and time they were made as well as the date they refer to.

All entries must be written in a clear and unambiguous style

Records should not include jargon, meaningless phrases (e.g. comfortable night), irrelevant speculation or offensive subjective statements. All statements must be factual.

Always remember that your record keeping is open to scrutiny by the service user, your peers, your professional body and the courts.

It is a fundamental requirement that all of the Trust's records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the Trust's functions.

In cases of doubt about retention periods or about retention and disposal arrangements please contact the appropriate Records Management Lead for guidance. (See section 12 for contact details)

The Trust creates joint Health and Social Care and Corporate records. In cases where a record is covered by different retention periods the record should be retained for the longest period for that type of record.

The Trust will follow the minimum retention periods set out in the Information Governance Alliance "**Records Management Code of Practice for Health and**

Social Care" which provides detailed guidance on minimum retention periods for a range of NHS record types.

6.1 Care Records

Care records are a means of communication between practitioners and between practitioners and the service users. They are sometimes called in evidence before a court during legal proceedings.

Care records should contain the relevant findings in the health and care of the person receiving treatment or care and should provide clear evidence of the care planned, the decisions made, the care delivered and the information shared.

6.2 Corporate Records

Corporate records are a means of logging, communicating and managing corporate trust action and supporting services for all staff

Corporate information refers to information generated and received by a service other than clinical / care (i.e. service user) information. The term describes the records generated by an organisation's business activities, and therefore will include records from the following (and other) areas of the organisation:

- IMST
- HR & Finance
- Corporate Governance
- Training

6.3 Training

All staff and others working on Trust business are made aware of their responsibilities for record keeping and record management through generic and specific training programmes and guidance. Further information on training and awareness is contained in section 8 below.

6.4 Accessible Information Standard

From 31 July 2016 Health and Social Care organisations are required to meet the Accessible Information Standard which is a legally enforceable standard to support service users and carers with a disability, impairment or sensory loss.

The standard has been introduced to make sure that disabled people have access to understandable information and relevant communication support.

The standard requires organisations to:

- IDENTIFY that someone has a NEED linked to a disability
- RECORD information about the NEED
- MEET this NEED
- SHARE information about this NEED

The Insight system has been updated so that NEEDS can be recorded and so that information that a person has a NEED recorded is flagged when the system is accessed.

Further information about the standard is provided on the Trust Intranet as a separate Accessible Information Standard section or 'widget' within the General Information section of the Homepage.

6.5 Further Guidance

Detailed guidance to support the above policy aims with regard to the creation and maintenance of Care Records can be found in the document "Guidelines for the Structure, Format and Management of Care Records" which is attached to this policy at Appendix G. Practitioners must create and manage care records in accordance with the guidance, which forms part of the framework of standards, procedures and guidance supporting implementation of this policy.

Detailed guidance to support the above policy aims with regard to Corporate / Business Records is being developed and will be made available in the Policies section of the Trust's intranet.

6.6 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.

[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).

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 is version 3 of this policy and replaces version 2 (October 2016). 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

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
Duties	Local induction, PDR, Supervision	Line Managers	At least annually	Directorates	DIGB	DIGB
Legal obligations that apply to records	Supervision PDR	Line Managers	Annual	Directorates	DIGB	DIGB
How a new Record is created	Clinical Records Audit	Directorates	Annual	Clinical Audit	DIGB	DIGB
How health records are tracked when in current use	Electronic records stored centrally and subject to audit trail	CRG	Ongoing	Directorates	DIGB	DIGB
How health records are retrieved from storage	Supervision PDR	Line Manager	Annual	DIGB	DIGB	DIGB
Process for retention, disposal and destruction of records	Retention & Disposal Schedule	CRG	Annual	DIGB	DIGB	DIGB

Basic Records keeping standards which must be used by all staff	Clinical Records Audit	Directorates	Annual	Clinical Audit	QAC	QAC
Process for making sure a contemporaneous record of care is completed	Clinical Records Audit	CRG	Annual	Clinical Audit	QAC	QAC
How the organisation trains staff in line with the TNA	Supervision PDR Training records	Directorates ETD	Annual	DIGB	DIGB	DIGB

The Trust will ensure that an audit of records management practices will be regularly included in the Internal Audit work programme and that reports and recommendations for corrective action are fed back to the Audit and Assurance Committee.

The Data & Information Governance Board (DIGB) will ensure arrangements are established to test compliance of records management procedures and practices with the provisions of this policy and with associated standards, including NHS Litigation Authority Risk Management Standards and Data Security & Protection Toolkit Requirements, to identify areas requiring attention in future work programmes.

With regard to care records, record keeping standards for all professional groups will be periodically audited through the clinical audit process.

All audits involving physical records must be undertaken at the location where the records are held. Records must not be taken off the premises, including photocopies and print-outs of scanned documents etc.

The Data & Information Governance Board will oversee and sign off the content of annual work programmes to support implementation of the policy, and will monitor actual progress with the programmes.

Issues and progress on records management covering all records will be fed back to the Data & Information Governance Board, who in turn will feedback to the Trust Board, through providing the necessary assurances to the Quality Assurance Committee.

This policy will be reviewed three years after ratification, or sooner if major changes occur in legislation, guidance or in other policies which have an impact on Records Management.

10. Implementation plan

The table below sets out the outline implementation strategy for this policy. The implementation strategy will be progressed through annual work programmes which will be developed by the Records Management Leads. Resource implications of implementing the strategy will be subject to justification and prioritisation as detailed plans are developed in the annual work programmes

Action / Task	Responsible Person	Deadline	Progress update
Dissemination			
Post on Trust intranet.	RM leads	Within 7 days of ratification	
Ensure all staff in directorate teams are aware of this policy and their responsibilities under it.	Heads of directorates		
Review and update organisational arrangements.	Board level RM leads	At each policy review	
Review and update Lead roles for Records Management.	Board level RM leads		
Training & Development			
Ensure Records Management is covered in Corporate Induction.	Training Dept.	Ongoing	
Ensure Records Management is covered in Local Induction.	All Managers	Ongoing	
Ensure Records Management training needs are identified in Personal Development Plans.	All Managers	Ongoing	
Ensure appropriate staff undertake	All Managers	Ongoing	

relevant Records Management modules of the IGT Training Tool. Ensure specialist RM training is provided to staff where necessary. Review effectiveness of IG Training provided. Identify unmet training needs for inclusion in the annual work programmes.	 All Managers RM Leads RM Leads	 Ongoing Annually Annually	
Develop, review, update supporting policies, procedures and guidance, as necessary, to ensure :- • Creation and keeping of records which are adequate, consistent, and necessary for statutory, legal and business requirements. • Systematic, orderly and consistent creation, appraisal, retention and disposal arrangements for records during their lifecycle. • Provision of systems which maintain appropriate confidentiality, security and integrity for records in their storage and use. • Provision of clear and efficient access for staff and others who have a legitimate right of access to Trust records, and compliance with current Data Protection and Freedom of	RM Leads working through the Information Sharing and Care Records Group and Data & Information Governance Board	Ongoing	

Information legislation			
Undertake a records audit to create an inventory of Corporate records in both manual and electronic format. Establish arrangements to maintain the inventory.	Corporate Records Lead	March 2019	
Review progress with implementation of the Electronic Records Plan to ensure consistency with the Records Management Policy and supporting work programmes	RM Leads working through the Information Sharing and Care Records Group	Ongoing	
Ensure audit of RM practices is included in Internal Audit work programmes and act on agreed recommendations. Test compliance of records management procedures and practices with the provisions of this policy and with associated standards. Ensure record keeping standards for care records for all professional groups are periodically audited through the clinical audit process. Complete the RM component of the Data Security & Protection Toolkit. Ensure areas identified as requiring attention in audits and compliance checks are addressed in work programmes or action	RM Leads Data & Information Governance Board Data & Information Governance Board Data & Information Governance Board Data & Information Governance Board	Annually Annually Annually Annually Annually	

plans. Monitor actual progress with work programmes or action plans. Feedback issues and progress to the Quality Assurance Committee	Data & Information Governance Board Data & Information Governance Board	Ongoing As necessary	
Review and update the RM policy	RM Leads	3 years after ratification or sooner if circumstances require	

The annual work programmes developed to deliver the implementation strategy will be agreed and signed off by the Data & Information Governance Board.

11. Links to other policies, standards and legislation (associated documents)

Further information about Records Management requirements is contained in the Information Governance Alliance "Records Management Code of Practice for Health and Social Care. This Code of Practice is a guide to the standards of practice in the management of records for those who work within or under contract to NHS organisations. It is based on current legal requirements and best professional practice.

It underpins this policy.

The Code of Practice is available alongside this policy on the Trust's Intranet.

Attention is drawn to the following legislation which has significant implications for Records Management:

Data Protection Legislation

A key driver for compliance with records management principles is the Data Protection Act 2018 which enacts the General Data Protection Regulation into UK law. These acts regulate the processing of personal data, held both manually and on computer. Personal data is data relating to a living individual that enable him/her to be identified from that data alone or from that data in conjunction with other available information. Processing of personal data includes everything done with that information, for example, obtaining, holding, recording, using, disclosing and sharing it.

Access to Health Records Act 1990

This Act remains in force only in respect of the health records of deceased patients. It applies only to records created since 1 November 1991. This Act provides rights of access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased's estate. In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements.

Freedom of Information Act 2000

Good records management is also a pre-requisite for compliance with the Freedom of Information Act 2000. The Freedom of Information Act, which applies to all public authorities, gives individuals a general right of access to all types of recorded information held by the Trust unless they are covered by an exemption. This right of access to information is additional to other rights such as access to personal information under the Data Protection Act. Good quality records management procedures and practice are necessary to enable the Trust to respond in a timely manner to any requests for information it may receive so that appropriate records can be located, retrieved and evaluated.

Common Law Duty of Confidentiality

Common Law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges; hence it is also referred to as case law. The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent. In practice this means that all service user information, whether held on paper or

electronically, or held in the memory of a practitioner, must not normally be disclosed without the consent of the service user. Three circumstances making disclosure of information lawful are:

- where the individual to whom the information relates has consented;
- where disclosure is in the public interest; and
- where there is a legal duty to do so, e.g. a court order.

All staff involved in the management of records must be aware of their responsibility for maintaining confidentiality of records. If in doubt seek help.

Human Rights Act 1998

The Act became part of UK law on 2 October 2000. Article 8 provides that each individual has a right to respect for his/her private life, and that right may only be interfered with in accordance with law and to the extent that it is necessary in a democratic society in the interests of national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals or the protection of the rights and freedoms of others. The European Court has held that the individual's private life protected by Article 8 includes his/her medical records and that respect for their confidentiality is a fundamental human right. It was held that the protection of patient confidentiality is vital both to an individual's own sense of protection of his/her private life and to the preservation of public confidence in the medical profession and health services in general.

Current understanding is that if Trusts comply with the provisions of the Common Law Duty of Confidentiality and Data Protection legislation they will meet the requirements of Article 8.

More information on the application of Data Protection legislation, the Access to Health Records Act, the Common Law Duty of Confidentiality, the Human Rights Act and the Freedom of Information Act and on the records management implications of other legal and professional obligations can be found in Information Governance Alliance "Records Management Code of Practice for Health and Social Care".

To support effective implementation of this Records Management Policy the Trust is developing a framework of related policies, standards, procedures and guidelines. These will be available alongside this policy on the Trust's Intranet.

12. Contact details

Further information about the content and status of this policy can be obtained from the Trust Records Management Leads.

Title	***Name***	***Phone***	***Email***
Trust Records Management Lead for Care Records	Clive Clarke, Deputy Chief Executive & Executive Director of Operations	271 8758	Clive.Clarke@shsc.nhs.uk
Trust Records Management Lead for	Margaret Saunders	305 0727	Margaret.Saunders@shsc.nhs.uk

Corporate / Business Records	Director of Corporate Governance (Board Secretary)		
Board level Director for Records Management – Care Records	Liz Lightbown, Executive Director of Nursing, Professions and Care Standards	271 6395	Liz.Lightbown@shsc.nhs.uk
Board level Director for Records Management - Corporate / Business Records	Clive Clarke, Deputy Chief Executive & Executive Director of Operations	271 8758	Clive.Clarke@shsc.nhs.uk
Caldicott Guardian	Clive Clarke, Deputy Chief Executive & Executive Director of Operations	271 8758	Clive.Clarke@shsc.nhs.uk
Mental Health Act Administrator	Mike Haywood	271 8102	Mike.haywood@shsc.nhs.uk
Clinical Audit Facilitator	Philip Jonas	271 8950	Philip.jonas@shsc.nhs.uk
CIO & Director of Information Management Services & Technology	TBA		
Trust Data Protection Officer	John Wolstenholme, Information Manager	305 0749	John.Wolstenholme@shsc.nhs.uk
Board level Lead for Freedom of Information	Clive Clarke, Deputy Chief Executive	271 8758	Clive.Clarke@shsc.nhs.uk
Trust Freedom of Information Lead	TBA		
Education, Training and Development Lead	Karen Dickinson	226 3116	Karen.Dickinson@shsc.nhs.uk

13. References

All records created in the course of the business of the Trust are Public Records under the Public Records Acts 1958 and 1967. The Trust will take actions as necessary to comply with its obligations set out in the following statutory requirements, NHS Standards and other guidance :-

- Public Records Acts 1958 and 1967;
- Data Protection Act (2018) /GDPR;
- Access to Health Records Act 1990;

- Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality;
- The Human Rights Act 1998;
- Professional Codes of Conduct;
- NHS Information Governance Requirements, Standards and Best Practice;
- Caldicott Review of Patient Identifiable Information 1997;
- National Data Guardian for Health and Care: Review of Data Security, Consent and Opt-Outs;
- Department of Health: Your Data: Better Choice, Better Care;
- Information Governance Alliance: Records Management Code of Practice for Health and Social Care;
- Confidentiality: NHS Code of Practice;
- NHS Litigation Authority Risk Management Standards;
- Department of Health Standards;
- Care Quality Commission Standards;
- Information Governance Alliance guidance;
- Information: To share or not to share? The Information Governance Review (2013);
- The Health and Social Care (Safety and Quality) Act 2015;
- The Lord Chancellor's Code of Practice under Section 46 of the Freedom of Information Act 2000;
- The National Archives Model Action Plan for Developing Records Management Compliant with The Lord Chancellor's Code of Practice under Section 46 of the Freedom of Information Act 2000;
- SCCI1605 Accessible Information – the 'Accessible Information Standard'
- Any new legislation, standards and guidance affecting records management as it arises.

Appendix A – Version Control and Amendment Log

Draft Step to Final V3	Type of Change	Date	Description of change(s)
1	Policy ratified by EDG	January 2009	
2	Revisions submitted to Care Records Group	January 2011	
3	Revisions requested by Information Governance Steering Group	January 2011	
4	Revisions requested by Performance Information Group	January 2011	
5.9	Revised policy ratified by EDG	February 2013	
6.0	Updated version submitted to Information Governance Steering Group	March 2016	Updated for electronic records – detailed guidance for manual records formats removed
6.1	Updated for organisational changes and reformatted	October/ November 2016	Organisational changes – governance groups and responsibilities, addition of retention & disposal appendix to replace separate Retention, Disposal and Destruction of Care Records Policy; addition of reference to Accessible Information Standard and Appendix on Copy Letters to Service Users
7.0	Ratification / issue	November 2016	Ratification, finalisation and issue
7.1	Revisions requested by DIGB	August 2017	Addition of guidance for recording of gender change on Insight and access to records held by Sheffield Archives
7.2	Further revisions to update and streamline the policy	February 2018	Included in wider revision of Information Governance policies
3	Re-numbered	August 2018	Re-numbered version
3.1	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)
3	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 October 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 can be found at http://www.shsc.nhs.uk/about-us/equality--human-rights

	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? N/A as no flow diagram in this Policy.

☐ **No, no further action needed.**

☐ **Yes, go to question 3**

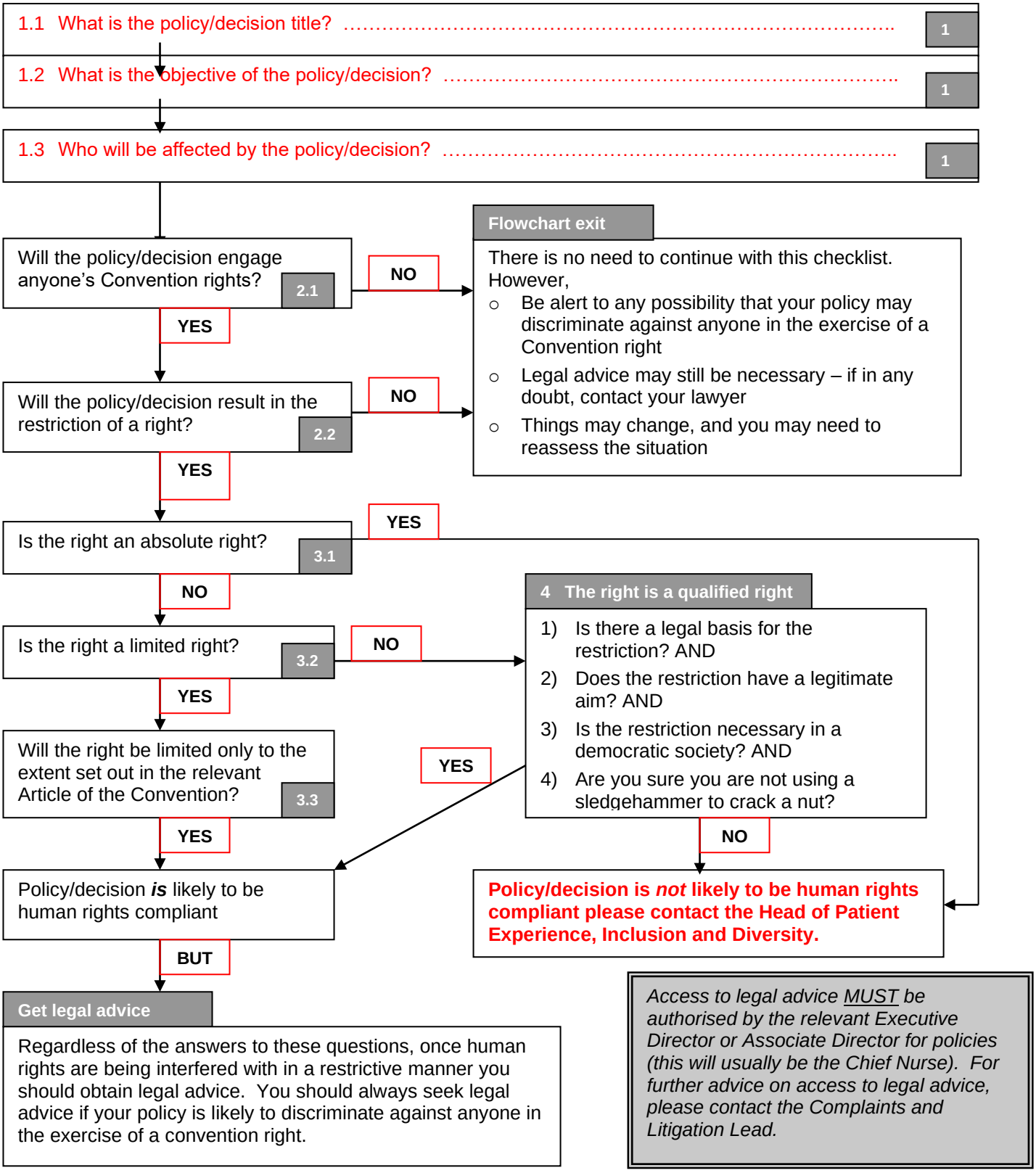
3. Complete the table below to provide details of the actions required

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

Previous versions of the policy were developed under the Care Records Group, Information Governance Steering Group and Performance Information Group.

The review leading to this version of the policy was commissioned by the Information Governance Steering Group in March 2016 with further amendments under the authority of the Data & Information Governance Board in October 2016.

It incorporates recommendations from the Information Governance Toolkit Audit for 2015/16.

The policy was revised to include guidance for recording of gender change on Insight and access to records held by Sheffield Archives in February 2017.

This policy was reviewed 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 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
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) ✓

Appendix G – Care Records Standards

1. All Care Records - paper or electronic

You should use your judgement to decide what is relevant and what should be recorded however, all entries should be complete and adequate for the purpose.

Record facts clearly and where the facts lead to a deduction or opinion make it clear that the statement is an opinion.

Beware of writing judgemental statements, where you are not in a position to judge.

Record any discussion or disagreement with the service user, which is relevant to their care.

Details of any assessments and reviews undertaken and clear evidence of the arrangements made for future ongoing care should be recorded.

Care records should identify any risks or problems that have arisen and show the action taken to deal with them.

In circumstances where practitioners have recorded and kept separate their own detailed process notes, the existence of these notes must be referenced in the single service user care record.

Events should be recorded as soon as is practicable after they occur and all entries should be completed within the same working day. If there is a delay the time of the event and the delay should be recorded – electronic records will record the date and time they were made as well as the date they refer to.

All entries must be written in a clear and unambiguous style

Records should be written in a style that the service user can understand wherever possible, however, it is recognised that the care record is a professional document and the use of technical language may be unavoidable.

Records should not include jargon, meaningless phrases (e.g. comfortable night), irrelevant speculation or offensive subjective statements. All statements must be factual.

Avoid using abbreviations if possible. Abbreviations may be acceptable if:
- the abbreviation is more widely understood than writing in full (e.g. GP, NHS)
- writing in full would not aid either clinical or patient understanding
- abbreviations may be used if the term is written in full followed by the abbreviation at least once in the record

A registered practitioner must countersign entries by unregistered staff and students.

The care record should not contain information about complaints made by the service user about their care.

Advance directives and consent and resuscitation status statements must be clearly recorded in the care record.

Always remember that your record keeping is open to scrutiny by the service user, your peers, your professional body and the courts.

2. Confidentiality and Storage

The contents of all care records must be treated as confidential.

Information should be shared with other agencies only when it is relevant for them to know, and must be done in accordance with the Trust's Information Sharing policies and protocols.

Care records must be kept securely at all times. When not in use any paper care records must be kept in a locked area, e.g. drawer, cabinet, room. For added security for electronic care records all work stations should be locked when not in use to prevent unauthorised access to the electronic care record. When in use care must be taken to maintain the confidentiality of the care record.

Any incidents of unauthorised access must be reported using the Trust's incident reporting procedures. The Data & Information Governance Board will review and monitor all such incidents in order to ensure appropriate reporting, assessment and follow up of remedial action.

3. Transporting Care Records between Trust Sites

Where any manual care records have to be transported between sites this must be done in a secure manner to ensure service user confidentiality at all times. Hard copy care records should be transported either in designated medical records bags or in secure sealed envelopes.

Any staff taking confidential information away from Trust premises must comply with the arrangements set out in the Trust's Remote Working and Mobile Devices Policy.

The main points to note when taking physical care records away from Trust premises are: -

- Physical copies of 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 physical copies of 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.
- Where possible, the information should be in electronic form and stored on a device encrypted to national standards as described in the Remote Working and Mobile Devices Policy or accessed remotely. If information is in the form of manual care records special care must be taken to ensure these are not left unattended in surroundings which are not secure from unauthorised access.

Confidential information, whether manual or electronic, must be protected by adequate security, for example they must be:-

- Kept out of sight, for example, in the locked boot of a car when transported;
- Not left unattended, for example, not left in a car boot overnight or when the car is parked up and left during visits etc.;
- Locked away when not being used;
- Kept secure and guarded from theft, unauthorised access and adverse environmental events when taken home;
- Properly encrypted to national standards when stored on electronic devices.

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.

4. Care Records sent out of SHSC NHS Foundation Trust

If it is necessary to send care records out of the Trust to other individuals or organisations then the provisions of the Trust's Procedure for Sending Care Records out of Sheffield Health & Social Care NHS Foundation Trust must be followed. A copy of the procedure is included with this guidance at Appendix C.

5. Duplication of Care Records

In the event that duplicated client records are identified their existence must be notified promptly to the Information Department using the electronic 'Insight Issues and Change Requests' form available via the SHSC Intranet. The Information Manager is responsible for ensuring the appropriate corrective action is taken.

The number of duplicated client records identified will be reported periodically, depending on volume, to the Care Records Group.

6. Misfiling of Care Records

Where documents or notes are identified as having been stored against the wrong service user, the person identifying the misfile will report the incident using the Trust's incident reporting procedures and notify the Information Department using the electronic 'Insight Issues and Change Requests' form available via the SHSC Intranet.

Insight support staff will ensure that the misfiled records are moved to the correct person.

Where the misfile results in the inappropriate disclosure of confidential information this must be reported as a data breach.

7. Missing Care Records

In the event of being unable to locate any physical care record this must be reported as an incident in accordance with the Trust's Incident Management Policy.

8. Disposing of Care Records

Practitioners must never dispose of care records. Decisions on disposal of care records will be taken by the Data & Information Governance Board.

Detailed arrangements governing the retention and disposal of Trust care records can be found elsewhere in this policy.

9. Auditing and Monitoring

An annual audit of care records across all professions must be completed using the Trust- wide Records Audit Tool. Audit forms and guidance will be made available by the Clinical Effectiveness team.

Any audits involving physical care records must be undertaken in the department where the records are stored. Care records must not be taken off the premises, including photocopies and print-outs of scanned documents etc.

References:

- Sheffield Health and Social Care NHS Foundation Trust Remote Working and Mobile Devices Policy
- Setting the Records Straight, Audit Commission (1999)
- Guidelines for Records and Record Keeping, Nursing & Midwifery Council, (2007)
- Record Keeping – Guidance for nurses and midwifes, Nursing & Midwifery Council (2010)
- Guidelines on Confidentiality and Record Keeping, Division of Counselling Psychology (May 2002)
- Record Keeping: Guidance on Good Practice – Division of Clinical Psychology, The British Psychological Society (2008)
- Basic Specialist Training Handbook, Royal College of Psychiatrists January 2003
- Generic medical record-keeping standards prepared by the Health Informatics Unit of the Royal College of Physicians. (2007)
- College of Occupational Therapists (2006) Records Keeping, College of Occupational Therapist guidance 2. London:COT
- NHSLA Risk Management Standards
- Clinical Information Assurance – Mental Health Trust Guidance

Appendix H – Procedure for sending Manual Care Records out of Sheffield Health & Social Care NHS Foundation Trust

This procedure is to ensure that Care Records that are sent out of the Trust are done so in a safe and secure manner.

This procedure describes how the notes should be sent and by whom. This procedure does not cover who has the right to request access to the care records held by Sheffield Health and Social Care NHS Foundation Trust.

In most cases for anyone other than the service user to have copies of the notes authorisation must be given by the service user; however, authorisation is not always required when a Health Professional who is currently looking after the service user makes the request.

Requests by Health Professionals not belonging to the Sheffield Health & Social Care NHS Trust should be made to the Corporate Affairs Department

Where the records are stored on Insight the Corporate Affairs Department will then locate the appropriate records, seek authorisation from the appropriate professional and dispatch the records via encrypted CD. Departments using SystmOne may process their own requests adhering to the same principles.

For requests that are not processed by the Corporate Affairs Department the following procedure must be followed.

Any request must be made in writing

The request must state the records required and the reasons the records are needed. Authorisation to send the records must by sought from the appropriate Health Professional.

Where possible, records should be provided in electronic format on media encrypted to national standards.

If records are to be sent via e-mail the e-mail must be encrypted – either between addresses which both belong to approved public sector domains (such as NHSmail) or using the SHSC encryption facility – see the e-mail policy for further details. Ordinary SHSC e-mail addresses are not sufficient without the message being specifically encrypted.

If paper copies are to be provided these must be sent by Special Delivery (signed for).

Appendix I – Retention, Disposal & Destruction of Records

1. Retention Periods

The Trust will adhere to the retention periods specified within the Information Governance Alliance Records Management Code of Practice for Health and Social Care (available via the SHSC Intranet).

This lists minimum recommended retention periods for various types of records including care records and corporate records.

Where records are held by the Trust for both Health and Social Care purposes and the retention periods for Health records differ from those for Social Care records, the Trust will adhere to the longer of the relevant retention periods.

Since the introduction of the Care Records Mandate, all care records should be electronic but where physical records (including paper and microfilm/microfiche) remain they will be governed by the same retention periods.

Where records have passed their minimum retention period they will be considered for archiving or disposal but records which may be relevant to the Independent Inquiry into Child Sexual Abuse (IICSA) must not be destroyed.

Requests to destroy records before they have reached their minimum retention period must be submitted to the Data and Information Governance Board.

2. Electronic Care Records

The major retention periods for care records used within the Trust are as follows:

- For GP patient records the retention period is 10 years after death.
- For mental health records the current retention period is 20 years after the date of last contact between the service user and any heath/care professional employed by the mental health provider, or 8 years after the death of the service user if sooner.

Other periods may be relevant depending on the specific type of record so in cases of doubt the guidance document must be consulted before destroying any care records. Where the appropriate retention period can still not be identified the matter should be referred to the Information Manager.

Records held on SystmOne will follow national procedures in relation to retention and disposal. Retention and disposal of electronic records held on the Insight system will be subject to the following process:

The minimum retention period should be calculated from the beginning of the year following the date of the last contact with the service user or the year in which the service user died.

The dates used in calculating the minimum retention period will be the date of death as recorded on Insight for deceased people or the latest of the last recorded activity, the last date of discharge from an inpatient or residential setting, or the last recorded note or document recorded for service users with no date of death (in the case or notes or documents the date used will be the date the note or document refers to, not the date it was made or scanned).

For client records transferred from an earlier system or other clients with no activity or notes recorded on the system and no date of death, the minimum retention period will be calculated from the date the client record was created.

Once records held on Insight have reached their minimum retention period they will be removed from the system unless they are still in use. Such records will initially be moved to a secure archive storage area and may be deleted at a later date subject to the approval of the Data & Information Governance Board

3. Physical Care Records

Where physical care records still exist they should be scanned onto the appropriate electronic patient information system which will hold the definitive care record. Once paper records have been scanned and the electronic copy verified the electronic record becomes the definitive record and the original physical documents may be securely destroyed before the minimum retention period has been reached.

If physical care records are the only copy of the care record and they are not to be scanned then they must be retained for the appropriate retention period and destroyed securely when no longer needed.

4. Documentation of Archived/Destroyed Records

When care records of any format are archived or destroyed a record must be kept listing:

- the records destroyed, including destruction dates
- the name and designation of the senior manager authorising the destruction
- evidence of destruction e.g. a certificate of destruction from an external contractor, or details of method and place of destruction together with name and designation of Trust staff carrying out the destruction

5. Transfer of Records to Archives

The Trust has previously transferred a selection of service user records considered to be of archival value to the Sheffield Archives as the Approved Place of Deposit.

The Trust retains control of who can access those records already transferred to the archives. Requests for access to detailed records will not normally be granted until 100 years after the date of the record. In the case of requests for genealogical purposes the Trust will normally agree to confirm the dates of treatment and provide a copy of a photograph of the service user to family members if one is held.

Other requests for access to records held by the archives will be considered on their merits. The Caldicott Guardian will be the final arbiter for these requests.

At present there are no arrangements for the transfer of electronic care records to the archives.

6. Corporate/Organisational Records

Retention and disposal or organisational records will be managed subject to the same guidance as care records and under the overall authority of the Director of Corporate Governance (Board Secretary).

Appendix J – Providing Copy Letters to Service Users

Service users have a right to receive copies of any letters that help their understanding of their health and the care they are receiving should be copied to them as of a right.

A letter includes communications between different health professionals, including:

- Letters or forms of referral from primary health care health professionals to other NHS services
- Letters from NHS health professionals to other agencies (e.g. social services)
- Letters to primary care from hospital consultants or other healthcare professionals following discharge or following an outpatient consultation or episode of treatment.

This policy does not relate to Care Plans which are covered by separate arrangements

Other documents, for example, single test results or Mental Health Act reports, should not normally be sent to service users. In due course, the outcome of such tests should be included in a letter that is copied to the service user.

Reports written to Mental Health Review Tribunals and Manager's Hearings should adhere to the guidance set out in the Mental Health Act.

Where there is frequent communication, the service user may choose not to have a copy of every letter.

Content of Letters - 'No surprises'
The contents of copied letters should reflect the discussion in the consultation with the healthcare professional sending the communication. There should be no new information in the letter which might surprise or distress the service user. All significant issues that have been discussed should be included in the letter.

Exclusions
There may be occasions where it would not be appropriate to copy letters to the service user, for example::

- Where it has been established that the service user does not want a copy
- Where the healthcare professional feels that it may cause harm to the service user
- Where the letter includes information about a third party who has not given consent
- Where special safeguards for confidentiality may be needed

Where the letter is written at the request of an outside agency, other factors apply in addition to whether the letter should be copied to the service user, for instance, compliance with data protection.

Harm to the service user
Sharing difficult or sensitive information is not in itself enough to justify not copying a letter even if the healthcare professionals is anxious to protect the feelings of the service user. It is the service user's choice as to whether they wish to receive a copy of the letter unless the health professional's judgement is that it would be likely to cause serious harm to the service user or some other person.

Third party information

It will not be appropriate to copy a letter which contains information about a third party (other than members of staff involved in the care of the service user), who has not given permission to disclose the information, unless the information was originally provided by the service user or is already known to them.

Consent to receive letters
It is for each service user to decide whether they wish to receive copies of letters written about them by health professionals. Service users should be routinely asked and their decision recorded – this may be noted in the Alerts/Warnings box on Insight.

It will be sufficient to seek consent once rather than each time a letter is written as long as it is explained at the start of an episode that copies of letters will be sent routinely to the service user unless they decide to opt out of receiving them, which can be done at any time.

The person responsible for generating the letter is responsible for ensuring that the service user's consent to receive copies is sought and for making and sending copies. This does not mean that this person is necessarily the person who carries out these activities.

Mental capacity
There will be no 'blanket' assumptions about mental capacity.

Whilst a person may lack capacity for one purpose, they may have sufficient capacity for another. These judgements will be made on an case by case basis.

Some people may not have mental capacity to make a decision about whether they would like a copy of their letter, for instance because they have a learning disability or dementia.

It should already be recorded on a service user's health record if they have someone to act on their behalf or to represent their views, for instance a carer, advocate etc. However, there is no formal legal provision underpinning such arrangements. Health professionals must use advice from their professional bodies and the DoH Good Practice in Consent Implementation Guide to ensure that arrangements are in the best interests of service users.

Copying letters to carers
Some service users have carers, for instance partners, friends or family members, who are actively involved in their care.

As carers, they need information and support from professionals supporting the person they care for, and they have a right to an assessment of their own needs. Service users may want to have information shared with their carers. With the service user's consent, a copy of letters can be sent to the carers. Occasionally the service user may not want a letter copied or shown to the carers. Both the service user and carer have the right to expect that information that either provides to the health service will not be shared with other people without their consent. In such circumstances, unless there is an over-riding reason to breach confidentiality, the wishes of the service user must be respected.

Children and young people
People over the age of 16 are able to make health care decisions for themselves, and should therefore, be asked for their agreement to receive copies of letters about them. It is

up to healthcare professionals to assess the competence of younger children to understand and make a decision.

Letters written by non NHS agencies
Letters from non-NHS agencies may be written to healthcare professionals and not copied to service users. The healthcare professional may consider it is important to show the letter or give a copy to the service user. However, it is not the responsibility of the healthcare professional who receives the letter to send a copy to the service user.

Service users with a disability, impairment or sensory loss may require communications in specific formats – see the section on the Accessible Information Standard on the SHSC Intranet for further details.

Appendix K – Recording of Gender Change on Insight

Background

Once a person has been granted a Gender Recognition Certificate, information about their application for a certificate and about their previous gender becomes "protected information". It is an offence for a person who has acquired protected information in an official capacity to disclose the information to any other person, unless the subject of the protected information has agreed to the disclosure.

It is not an offence to disclose the 'protected information' referred to under the Gender Recognition Act 2004 if:

- the disclosure is made for medical purposes to a health professional; and
- the person making the disclosure reasonably believes that the subject has given consent to the disclosure or cannot give such consent.

'Medical purposes' includes the purposes of preventative medicine, medical diagnosis and the provision of care and treatment.

The Information Governance Alliance (IGA) Records Management Code of Practice for Health and Social Care states:

A patient can request that their gender be changed in a record by a statutory declaration, but this does not give them the same rights as those that can be made by the Gender Recognition Act 2004. The formal legal process (as defined in the Gender Recognition Act 2004) is that a Gender Reassignment Certificate is issued by a Gender Reassignment Panel. At this time a new NHS number can be issued and a new record can be created, if it is the wish of the patient. It is important to discuss with the patient what records are moved into the new record and to discuss how to link any records held in any other institutions with the new record.

Process for recording change of gender on Insight

Where a service user decides that they wish to identify as a different gender but does not have a Gender Recognition Certificate their electronic record will be updated with the new details and the old details stored in history without creating a new record.

Where a service user is formally granted a Gender Recognition Certificate they will be informed by the treating service of their right to have a new record created under their new identity and the old one closed. The risks to their continuity of care of not maintaining a link with the original record will be explained to the service user and their decision sought.

Where the service user opts to maintain a single, continuous record their name, gender and other details will be updated as appropriate on the Insight record and the old name will be stored in name history.

Where the service user opts for a new record the following process will be followed:

The treating service will inform the Information Department to ensure that the name of the existing Insight client record is changed to an alias and any current episodes are closed.

A new Insight record will be created under the new service user details including the NHS number corresponding to these details. Where the service user has retained their original NHS number this will be recorded under the new record and removed from the old record. Where a new number has been issued the old number can be retained on the old client record but no link between the two will be maintained. Where the new record begins with the original NHS number but a new one is subsequently issued the Insight record will be updated with the new NHS number.

Any SHSC services currently involved in the service user's care will be informed to access the new record and NHS number by the person creating the new record. New referrals/episodes will be created for current services against the new client record. Records, notes etc will not be transferred from the old record to the new one without the service user's agreement.

A warning will be entered on Insight against the old record along the lines of:

"These records are protected under law and are actively audited. Do not access them without contacting the Information Manager."

Appendix L – Access to Records held by Sheffield Archives

Some old patient records, including those from the West Riding Mental Hospital (later Middlewood Hospital), have been transferred to the Sheffield Archives for permanent preservation, having been judged to be of historical interest.

No further patient records will be transferred to Sheffield Archives.

Patient confidentiality still applies to the records held by Sheffield Archives and Sheffield Health & Social Care is still the data controller in respect of these records.

Access to records of deceased people is governed by the Access to Health Records Act 1990 – requests may be made by the appointed representative of the deceased or people who have a claim arising out of the death.

For other people who wish to access patient records held by Sheffield Archives, access to detailed patient information will not normally be granted until 100 years have passed since the date of the record.

The Trust will allow confirmation of the dates the patient was treated and where a photograph of the patient is held a copy may be provided to family members.

Requests for other information will be referred to the Trust.