Shropshire Community Health
NHS Trust

Records and Document Management Policy

Controlled document
This document is uncontrolled when downloaded or printed

Author(s) Owner(s)	Author: Gill Richards (Head of Information Governance) and David Shelton (Records Management Lead) Owner: Shelley Ramtuhul, Corporate Secretary/Director of Governance/Senior Information Risk Owner (SIRO)
Version No.	Version 2.3
Approval Date	June 2023
Review Date	June 2026

Document details	
Title	**Records and Document Management Policy**
Trust Ref No	1348-47170
Local Ref (optional)	2.3
Main points the document covers	This policy explains how the records and document management arrangements will be delivered and adhere to the national Code of Practice.
Who is the document aimed at?	All staff (including employees, contractors, temporary staff, secondments, student placements)
Owner	Corporate Secretary/Director of Governance/Senior Information Risk Owner (SIRO)
Approval process	
Who has been consulted in the development of this policy?	A selection of Managers/staff
Approved by (Committee/Director)	Data Security and Protection Assurance Group Director of Finance/SIRO
Approval Date	16 June 2023
Initial Equality Impact Screening	Yes
Full Equality Impact Assessment	No
Lead Director	Director of Finance/SIRO
Category	General
Subcategory	Information Governance
Review date	16 June 2026
Distribution	
Who the policy will be distributed to	All staff (including non-employed workers)
Method	Website and email
Keywords	Records management, records, record keeping, archive, archiving, disposal, retention, retention schedule, corporate, clinical, filing, archiving, storage, data protection, freedom of information, information governance, NHS number.
Document Links	
Required by CQC	Yes – Well Led
Other	Data Security and Protection Toolkit (DSPT)

Amendments History		
No	Date	Amendment
1.	May 2012	Policy reviewed and updated to reflect changes within the Trust's organisational structure and latest guidance and standards
2.	Aug 2013	Changes to contact details for the Information Governance and Data Protection Lead
3.	Nov 2014	Review and minor amendments to reflect current organisational structure and links to reference information
4.	Mar 2017	Review and minor amendments to reflect current organisational structure and links to reference information
5.	Oct 2018	Review and update to take into account new Data Protection legislation – DPA and GDPR Combine the previous separate Records Retention Archiving and Disposal Policy into this policy
6.	Dec 2021	Templar Executive Consultancy and IG Manager. The whole document was reviewed by a consultancy and finalised by the IG Manager.
7.	Jan 2022	Updated to reflect the transfer of the Records Management role into IG. Processes have been extracted into a new SOP.
8.	July 2022	Update IT Service Manager description
9.	October 2022	Update Owner - Corporate Secretary/Director of Governance/Senior Information Risk Owner (SIRO)
10.	March 2023	Amended 'Information Governance Manager' to 'Head of Information Governance'. Updated Safe Haven role to function. Updated IAO role (detailed moved to new Appendix 2). Updated role of Information Risk Manager to include assigned to Head of IG. Added 'Records of historical value'. Updated references 'Records Management Group'. Naming conventions advice updated - 11.1,(d)(f).

Contents

1 Introduction

1.1 The Records Management Code of Practice 2021 states that, *"All health and care employees are responsible for managing records appropriately and must manage them in accordance with the law. The Public Records Acts 1958-1967 are the principal legislations relating to public records. Records of NHS organisations are public records in accordance with Schedule 1 of the 1958 Act. This means that employees are responsible for any records that they create or use in the course of their duties. This includes records controlled by NHS organisations under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations."*

1.2 Our patients, staff and stakeholders place trust in us to manage their records effectively. Shropshire Community Health NHS Trust (SCHT) recognises the importance of sound records management arrangements for both clinical and corporate records produced in support of the Trust's purpose to improve the health and well-being of our communities; working collaboratively across the NHS and allied organisations to deliver high quality services appropriate to the changing needs of the population.

1.3 The Trust's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the Trust and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

1.4 The Trust Board has adopted this Records Management Policy and is committed to ongoing improvement of its records management functions to deliver:

- Compliance with legislation and regulatory standards
- Better use of staff time
- Accurate, up to date and accessible patient, staff and organisational records
- Improved control of valuable information resources
- Better use of physical, network servers and cloud storage space
- Reduced costs

1.5 This document was written in accordance with the Records Management Code of Practice 2021 and explains the Trust's processes for ensuring that all records are:

- Created when required
- Properly controlled
- Readily accessible, and eventually
- Archived or otherwise disposed of appropriately

1.6 The Trust recognises that good record keeping is also important to achieve compliance with the following legislation and regulatory requirements:

- The Data Protection Act 2018 (DPA)
- UK General Data Protection Regulation
- The Freedom of Information Act 2000 (FOI)v
- The Access to Health Records Act 1990
- The Public Records Act 1958 and 1967
- Care Quality Commission (CQC) Fundamental Standards
- Data Security and Protection Toolkit

- Mental Capacity Act 2005
- Accessibility Information Standard 2016 (AIS)

See Appendix 1 for a brief summary of the items listed above.

2.1 The Records Management Code of Practice 2021 has been published by NHSX and provides guidance on how to keep records, including how long to keep different types of records. The Code provides a framework for consistent and effective records management based on established standards. It includes guidelines on topics such as legal, professional, organisational and individual responsibilities when managing records.

2 Purpose

2.2 This policy explains the document and records management arrangements adopted within Shropshire Community Health NHS Trust. It covers records prepared and maintained in all media, including paper and electronic records, for the benefit of all of Trust's stakeholders.

2.3 It references the Trust's processes developed to achieve best working practices in the creation, use, security, storage, retention and destruction of all records produced within the organisation.

2.4 The aim of this policy is to promote a records management culture that ensures:

- **Records are available when needed:** from which the Trust is able to form a reconstruction of activities or events that have taken place
- **Records can be accessed:** records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist (clear version control process)
- **Records can be interpreted:** the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records
- **Records can be trusted:** the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated
- **Records can be maintained through time:** the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format
- **Records are secure:** from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled, and audit trails will track all use and changes.
- **Records are held in a robust format**; which remains readable for as long as records are required
- **Records are retained and disposed of appropriately:** using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value

2.5 Staff are trained appropriately so that they are made aware of their responsibilities for record keeping and record management

3 Duties

3.1 The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

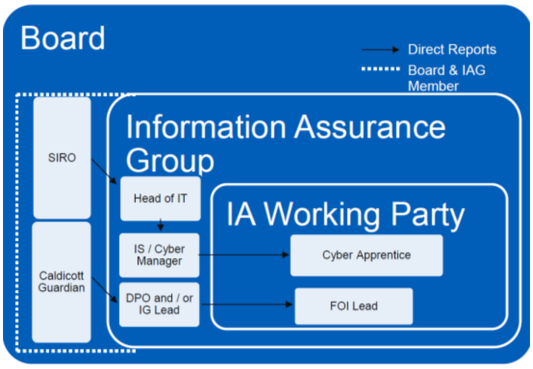
3.2 The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

3.3 The **Board** provides leadership on the management of risk and ensures the approach to risk management is consistently applied as well as determining the information risk appetite for the Trust. The Board is also responsible for setting the Trust's Risk Appetite regarding information security.

3.4 The **Senior Information Risk Owner (SIRO)** is the Board's executive level delegate responsible for risk management including oversight of data protection and other aspects of information governance. The role of the SIRO is to understand how the strategic business goals of the organisation may be impacted by information risks. The SIRO will act as an advocate for information risk on the Board, including internal discussions, and will provide written advice to the Accountable Officer on the content of the annual Statement of Internal Control (SIC) with regards to information risk. The SIRO will advise the Chief Executive and the Board on information risk management strategies, provide periodic reports and briefing on risk management assurance and ensure that key risks are appropriately logged on the corporate risk register.

3.5 The **Chief Executive** is the Accountable Officer and has overall responsibility for ensuring our compliance with this policy and with Data Protection legislation. They have overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.

The organisation will set out a line of accountability, responsibility and direction in accordance with the guidance set out in the Data Security and Protection Toolkit (DSPT) Standard 1 Personal Confidential Data, example diagram



3.6 The **Chief Information Officer (CIO)** is an executive within the organisation that oversees the operation of the information technology department and consults with other personnel on technology-related needs and purchasing decisions. The CIO is the Head of Digital Services.

3.7 The **Caldicott Guardian (CG)** has responsibility for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. For any patient confidentiality issues the first point of contact should be the CG.

The CG is also the designated **Privacy Officer**.

3.8 The **Chief Clinical Information Officer (CCIO)** is an executive within the organisation who is involved in change management, ensuring clinical adoption and engagement in the use of technology, supporting clinical process redesign in a digital world, providing clinical focus to ICT projects that will ensure the needs of the business are met with regards to patient care. The CCIO is the Medical Director/Caldicott Guardian.

3.9 **Directors, Deputy Directors, Divisional and Service Delivery Group Managers** of services and business functions within the Trust have overall responsibility for the management of records generated by their activities, i.e. for ensuring that records controlled within their service are managed in a way which meets the aims of the Trust's records management policies.

3.10 The **Data Protection Officer (DPO)** has day-to-day responsibility for monitoring compliance with this policy, advising the organisation on data protection matters and for receiving reports of personal data incidents for escalation as appropriate. The DPO is responsible for challenging and advising the Board on data protection to ensure that the Trust remains compliant.

3.11 The role of the **Information Asset Owner (IAO)** will be assigned to staff that hold the position of Deputy/Associate Director, Head of Department, Service Delivery Group Manager. The IAOs will be accountable to the Senior Information Risk Owner (SIRO); and will have delegated responsibility from the SIRO to oversee and support the information risk management framework within their respective areas. The role will support the SIRO in fostering a culture that values, protects and uses information for the benefit of patients, service users, employees and the Trust as whole. Full responsibilities listed in Appendix 2.

3.12 The **Information Asset Owner** may nominate an Information Asset Administrator (IAA) and delegate the day-to-day responsibility of the information asset. The Information Asset Owner will nominate an appropriate person to undertake the role of Data Protection Liaison Officer (DPLO).

3.13 **Data Protection Liaison Officers (DPLOs)** are responsible for providing administrative support to staff within the respective services/departments in the disclosure of personal data under the Data Protection legislation.

3.14 The **Head of Information Governance** is responsible for the day-to-day operational monitoring of information governance and information handling.

3.15 The **IT Service Manager** is responsible for the day-to-day management and operation of the corporate network infrastructure including the secure operation of the network, devices, connections, monitoring, protection and controls.

3.16 A **Safe Haven function** will be established in all services, teams and departments across the Trust. The IAOs will be responsible for identifying the safe haven(s) location and setting up the function in their respective areas; and the IAAs will be responsible for the day-to-day management and operation of safe-haven procedures. The safe haven environment will cover an agreed set of administrative procedures for the safe and secure handling of personal confidential information; such as reporting, handling Freedom of information and Subject access requests, dealing with requests from commissioners; and ensuring pseudonymisation and anonymisation is appropriately applied. The term "Safe Haven" means both a physical location within the organisation e.g. Trust premises or a virtual location e.g. MS Teams; where confidential information is both received and stored in a secure manner. A Register of Safe Havens will be held by the Head of Information Governance.

3.17 The **Information Risk Manager** is responsible for providing support to staff and managers who are responsible for information assets. They will provide support to the relevant groups and committees, including risk registers and monitoring service delivery risks. The role of the Information Risk Manager will be undertaken by the Head of Information Governance.

3.18 The **Freedom of Information Manager** to ensure that the Trust complies with the Freedom of Information Act 2000 in processing Freedom of Information requests and the maintenance of a Publication Scheme. This role will manage the need to carefully balance the case for transparency and openness under the Freedom of Information Act against the data subject's right to privacy under the data protection legislation. Advising the organisation with regards to deciding whether the information can be released without infringing the UK GDPR and DPA 2018 data protection principles.

3.19 **All Line Managers** are responsible for ensuring that staff with responsibilities set out in this policy can undertake the role sufficiently, including training, to meet the organisation's obligations under the Data Protection legislation.

3.20 The **Trust/Corporate Risk Manager** is responsible for providing support to staff and managers who are responsible for information assets. They will provide support to the relevant groups and committees, including risk registers and monitoring service delivery risks.

3.21 The **Records Manager** is responsible for:

- Assisting directorates and services to achieve good record keeping and compliance with the relevant standards, legislation, policies and procedures relating to the management of records
- Ensuring that records management audits are conducted by directorates and services
- Providing a Caldicott support function to ensure that the records management activities are in line with national and local guidance and protocols on confidentiality
- Liaising with, and supporting the Corporate Risk Manager in records management related incidents investigations and follow up actions
- Advising and supporting the activities of Local Records Management Coordinators
- Developing appropriate training material and methods of delivery for Trust staff and promoting best practice.
- Ensuring compliance and consistency across the Trust

3.22 The **Records Management Lead** supports the Head of Information Governance in their role as Records Manager and is responsible for:

- the Records Management Policy
- the overall development and maintenance of the Records Management Framework and for ensuring this policy complies with legal and regulatory edicts.
- providing learning and development with key learning points from this policy and for monitoring compliance with the policy to assess its overall effectiveness.
- developing and supporting a culture of high-quality records management practice across the Trust to deliver associated organisational benefits.
- knowing what records the Trust holds and where they are, by conducting regular audits of records working closely with the IG Assurance team
- ensuring that records created by the Trust are stored securely and that access to them is controlled

3.23 **Records and Document Management Co-ordinators** will be nominated to represent services, teams and department; or the Local Team Leader will be assume this responsibility.

3.24 **Records and Document Management Co-ordinators**[1] are responsible for:

- Championing good records and management
- Act as a first point of contact for records management queries
- Advise their team to ensure access control is in place for their restricted content
- Creation and use of accurate records process
- Records registration and tracking systems
- Systems for the safe use and storage of records to minimise loss
- Records are archived in appropriate, secure areas
- Directing staff to the retention periods as defined in the Records Management Code of Practice 2021.
- A mechanism for identifying records which must be permanently kept
- Identify areas of concern in the management of records and, when necessary, bring these topics for discussion by the relevant Network Group
- Conduct/support relevant audits of local records management practices/procedures
- Advising on the training requirements of their staff, including local induction training

3.25 Under the Public Records Act 1958 the responsibility of the Chief Executive and senior managers for the safe keeping of records is extended to all staff for all records they either create, use or handle.

3.26 All staff who come into contact with patient or personal information are subject to a Common Law Duty of Confidentiality. This duty of confidentiality continues beyond the death of a patient or after an employee has left the NHS.

3.27 This responsibility will be reflected in all job descriptions and assessed as part of staff appraisals.

3.28 The Data Security and Protection Assurance Group (DSPAG) will act as the forum for ensuring that compliance is achieved with the relevant legislative and regulatory standards and will report to the Digital Programme Group (DPG) Relevant risks and issues will be escalated to the Quality and Safety Committee and/or the Resource and Performance Committee.

3.29 **All staff** are responsible for upholding Data Protection requirements, including identifying and managing risk, and understanding/complying with relevant policies and procedures for handling personal data appropriate to their role. Staff must immediately report any event or breach affecting personal data held by the organisation to their Line Manager.

[1] Were know as ‘Local Records Managers’

4 Records Management

4.1 As stated in the Records Management Code of Practice 2021:

> *"Records of NHS organisations are public records in accordance with Schedule 1 of the Public Records Act 1958. This includes records controlled by NHS organisations under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations. This applies regardless of the records format."*

4.2 Examples of records that should be managed using the guidelines are listed below. This list gives examples of functional areas as well as the format of the records:

- health and care records
- registers - for example, birth, death, Accident and Emergency, theatre, minor operations
- administrative records, for example, personnel, estates, financial and accounting records, notes associated with complaint-handling
- X-ray and imaging reports, output and images
- secondary uses records (such as records that relate to uses beyond individual care), for example, records used for service management, planning, research

4.3 Examples of records that should be managed using the guidelines are listed below. This list gives examples of functional areas as well as the format of the records:

- health and care records
- registers - for example, birth, death, Accident and Emergency, theatre, minor operations
- administrative records, for example, personnel, estates, financial and accounting records, notes associated with complaint-handling
- X-ray and imaging reports, output and images
- secondary uses records (such as records that relate to uses beyond individual care), for example, records used for service management, planning, research

4.4 Examples of record formats that should be managed using the guidelines are listed below:

- Digital and paper
- Photographs, slides, and other images
- Physical records (records made of physical material such as plaster, gypsum and alginate moulds)
- Microform (i.e. microfiche/microfilm)
- Audio and video tapes, cassettes, CD-ROM etc.
- E-mails
- Computerised records
- Scanned records
- Text messages (SMS) and social media (both outgoing from the NHS and incoming responses from the patient) such as Twitter and Skype
- Websites and intranet sites that provide key information to patients and staff.
- Manual Records (such as case notes)

- Electronic Records (such as patient administration systems)
- Pictures and videos (Dicom[2] images, ultrasound recordings)

4.5 Records are legal documents and everyone working for the NHS has a common law duty of confidence to clients, staff and their employer. This duty of confidence continues after the death of a patient and after an employee has left the NHS.

4.6 Good information is essential to the effective delivery of high quality evidence based health care, it is anticipated that the robust implementation of this policy will help the Trust to achieve the following objectives:

- To support patient care and continuity of care
- To support evidence-based clinical practice
- Meet legal and regulatory requirements, including requests from patients under access to health records (under the Data Protection Act, Subject Access Requests) and requests for information from the general public (under Freedom of Information legislation)
- To support patient choice and control over treatment and services designed around patients
- To assist clinical and other types of audits
- To support improvements in clinical effectiveness through research and also to support archival functions by taking account of the historical importance of material and the needs of future research
- To support day-to-day business which underpins the delivery of care
- To support sound administrative and managerial decision-making, as part of the knowledge-base for NHS services

Note: The *Clinical Record Keeping Policy* gives more in-depth detailed guidance specific to health records and clinical record keeping requirements.

5 Records Life Cycle

5.1 The term “Records Life Cycle” describes the life of a record from its creation/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 confidential disposal or permanent preservation as being of historical or research interest. The key components of records management are:

- **Creation:** create and log quality information
- **Using:** use/handle
- **Retention:** keep/maintain in line with NHS recommended retention schedule
- **Appraisal:** determine whether records are worthy of Archival Preservation. Further use may be identified at this stage.
- **Disposal:** dispose appropriately according to Trust guidelines

It is imperative that records are closely monitored and managed throughout their lifecycle.

[2] Digital Imaging and Communications in Medicine - X-ray, MRI, CT, etc

6 Characteristics of Authoritative Records

6.1 **Authentic**

- It is what it claims to be
- To have been created or sent by the person claimed to have created or sent it and
- To have been created or sent at the time claimed

6.2 **Reliable**

- Full and accurate record of the transaction/activity or fact
- Created close to the time of transaction/activity
- Created by individuals with direct knowledge of the facts or by instruments routinely involved in the transaction /activity

6.3 **Integrity**

- Complete and unaltered
- Protected against unauthorised alteration
- Alterations after creation can be identified as can the persons making the changes

6.4 **Useable**

- Located, retrieved, presented and interpreted
- The context can be established through links to other records in the transaction/activity

7 Records Creation and Registration

7.2 Records are created throughout the Trust to ensure that information is available for the purposes defined in the introduction of this policy.

7.3 Directorates and services will ensure accurate record keeping by the use of standardised documentation and locally agreed processes and procedures for the creation and filing of records. The information contained in records is only usable if it is accurate, legible, is kept up to date and is easily accessible. Documented local procedures are important in ensuring a high standard of data quality for both manual and electronic records.

8 Use of Abbreviations

8.1 It is recognised that the use of abbreviations saves time when writing documents but excessive use of abbreviations can make it hard to understand or follow the flow of the content of a document. Best practice is to only use abbreviations where necessary and to include the full term the first time it is used within that document with the abbreviation in brackets e.g. Care Quality Commission (CQC). This is of particular importance in minutes of meetings as these are evidence of topics discussed and decisions made and may be referred to by someone who does not have the knowledge and background of those who attended that meeting. In meeting minutes, it is also important to have a key for any abbreviations used for those attending.

8.2 Additionally when using abbreviations in business or Trust documents, it is also advisable to include a glossary at the end of the document listing all abbreviations or terms used. In Health records this would be an agreed Abbreviation List where applicable.

9 Record Registration

9.1 To ensure records can be identified and retrieved when needed, it is good practice to maintain a register and to allocate a registration system to a set of records.

9.2 Registration is the act of giving a record a unique identifier (number or alphabetical prefix) on its entry into a record-keeping system which records that sequentially in a register or index.

9.3 All electronic records systems used by the Trust require unique identifiers, e.g. all clinical systems must use the patient's **NHS Number** to register their records.

9.4 Determining which records require registering is a decision that should be made by staff with advice from the Records Manager and Local Records Manager and, when relevant, the Caldicott Guardian.

9.5 The kinds of records, which are most likely to be placed on a register, include, but are not limited to:

- Care/clinical records
- Personnel records
- Corporate documents
- Policies and procedural documents
- Policy papers (reports, correspondence, etc.)
- Minutes, circulated papers, etc. of meetings
- Financial papers
- Contracts and Service Level Agreements (SLAs)
- Estates papers
- Performance monitoring
- Incident Reporting
- Papers relating to the preparation of legislation
- Freedom of Information requests
- Data Protection Subject Access Requests - SARs
- Complaints and claims papers and correspondence
- Research and development papers

9.6 Registration will depend on the Trust's business need to maintain accountable records of particular activities, its information needs, how many records there are on that particular topic or in that series and the obligations under the Data Protection Act, the Freedom of Information Act and other relevant legislation including Records Management Code of Practice for Health and Social Care.

9.7 It is important that all patient/client records held on a clinical system have their NHS Number recorded and that these numbers have been validated. For further guidance please refer to the Trust's *Clinical Record Keeping Policy / NHS Number Retrieval, Verification and Use Procedure*.

9.8 Best practice principles of registration are:

- The file title must be unique
- The registration identity assigned to each file must be unique
- Both must be relevant to and easily understood by all users

9.9 Registration systems, including Trust and local document registers (e.g. policies, contracts and information asset registers), should be monitored regularly and reviewed at least once every two years to ensure that they continue to operate effectively and efficiently and meet the needs of users.

9.10 Where departments/teams use shared records/document areas, (e.g. shared network folders or applications such as Microsoft SharePoint), there must be documented guidance to ensure a consistent approach to the creation, use, filing and storage of records. It is essential that registration systems include a mechanism for avoiding duplicate records. Electronic records systems will also have an integral audit trail.

10 Filing Structure

10.1 A filing structure provides a framework for organising records. Within the Trust records should be filed within a functional filing structure determined by and depending on their relevance within the individual directorates / services. This ensures that records can be efficiently filed, retrieved and archived or, eventually, disposed of. Ideally, the electronic filing structure should reflect the way in which paper records are filed to ensure consistency.

11 File Naming Conventions

11.1 Naming conventions provide a set of rules which assist in allocating a title to a document at the time of creation, and which also provide a framework for a good filing system. They make it easier for people other than the creator to retrieve records.

11.2 Naming conventions for document titles should aim to:

a) Give a unique title to each document. Naming a document as just agenda or minutes without a description of the actual group and a meeting date makes it harder to track that particular document

b) Give a meaningful title which closely reflects the document contents and express elements of the title in a structured and predictable order with the most specific information at the beginning of the title and the most general at the end e.g. Records Management – Working Group – Final Report

c) Give a similarly structured and worded title to documents which are linked (for example, an earlier and a later version)

d) Where dates are required use the yyyymmdd format so that files will then appear in chronological order when filed electronically e.g. 20180116-RM Agenda. The operating system will date-stamp the document at time of creation and edit (Migrated files could lose the created/edit date).

e) Avoid using all uppercase in filenames as this makes it harder to read e.g. Records Management NHS Code of Practice is easier to read than RECORDSMANAGEMENTNHSCODEOFPRACTICE

f) Ensure all documents have a unique name that should differ to other copies of the same document. Use of a document status or stage may be added eg 20230304-Records and Document Management Policy V1.0 Draft, 20230304-Records and Document Management Policy V2.4 For Review, 20230304-Records and Document Management Policy V2.4 Final.

12 Version Control

12.1 Version control is the management of multiple revisions to the same document and enables us to identify one version from another and retrace its evolution. Document versions generally run linearly, version 1, version 2 and so on with sub-versions 1.1, 1.2 etc.

12.2 When working with a draft include the word ‘draft’ in the version and filename. Also include “Draft” as a watermark in the document so that it easy to identify that the document has not been approved.

13 NHS Identity and Trust Branding

13.1 When producing Trust publications such as policies, leaflets or brochures it is important that NHS Identity and the Trust’s branding guidelines are followed. It is good practice to include contact details for the service / department on the last page and a leaflet reference name / version number and date of approval.

13.2 The Trust’s *Patient and Public Information Policy* and the *NHS Brand Guidelines* give specific advice and guidance on the use of the NHS identity and brand. In order to portray a professional and business-like image it is important that these guidelines are followed. They cover aspects including use and positioning of logos, layout and standard typefaces (fonts) e.g. Arial. The Trust's Communications and Marketing Manager should be contacted for further advice and guidance.

14 Procedural Documents

14.1 Approved procedural documents, including strategies, policies, protocols and guidelines, record the processes by which SCHT plans and conducts its activities. They are necessary to ensure that the Trust's vision and goals, as recorded in the strategic plan are achieved, that risks to these objectives are adequately mitigated, legal and regulatory obligations are met, and that the Trust's intentions and methodologies are clearly understood by all stakeholders.

14.2 The control of procedural documents is essential, not only to comply with corporate and clinical governance standards but as an essential means of ensuring standardisation in the provision of safe care across the Trust and the successful reduction of risk.

14.3 The *Policy on the Development and Management of Procedural Documents* has been developed to ensure a structured and systematic approach to the development, review, ratification, dissemination and retention of procedural documents. It establishes a framework that ensures all policies and procedures are:

- of a consistently high standard
- up to date
- available to all staff
- implemented and complied with
- reviewed at regular intervals

14.4 All staff involved in the design, development, approval and review of procedural documents must ensure they are aware of their responsibilities as detailed in the *Policy on the Development and Management of Procedural Documents*. For further advice and guidance contact the Corporate Risk Manager.

15 Personal Confidential Data

15.1 The term Personal Confidential Data (PCD) is used in the Caldicott Information Governance Review and describes personal information about identified or identifiable individuals, which should be kept private or secret and includes deceased as well as living people. The term Personal Identifiable Data (PID) was previously used but has been superseded by Personal Confidential Data.

15.2 The review interpreted *'personal'* as including the Data Protection Act definition of personal data, but included data relating to the deceased as well as living people. *'Confidential'* includes both information *'given in confidence*' and *'that which is owed a duty of confidence' and is adapted to include 'sensitive*' as defined in the Data Protection Act 2018.

15.3 Examples of identifiable data are:

- Name
- Address
- Postcode
- Date of Birth
- NHS Number

15.4 Personal Confidential Data or information about either patients or employees recorded for any purpose should not be kept for longer than is necessary. Neither should it be used for any purpose other than that for which it was collected.

15.5 Personal Confidential Data or information must not be passed on to other people without the consent of the individual concerned except as permitted under the UK GDPR/ DPA 2018 or under the common law where there is an over-riding public interest. Further information is contained within the Trust's *Information Governance Policy - Data Protection section* and the *Confidentiality Code of Practice*.

15.6 When transferring Personal Confidential Data or information suitable security must be used. In the case of electronic transfer of Personal Confidential Data then the appropriate encryption process must be used following guidance given in the Trust's *Information Security Policy* and other relevant up to date advice that may be published from time to time.

15.7 Data Protection Impact Assessments (DPIAs) must be carried out where there is a new or change in use of personal data and a potentially high risk to privacy is possible. The Head of Information Governance will be able to support this process.

16 Personal Records

16.1 It is important that all those responsible for personal records are aware of their responsibilities under the UK GDPR / DPA 2018. This guidance below applies to all personal records, in particular staff records. Specific additional guidance on heath records is contained in the *Clinical Record Keeping Policy*.

16.2 To ensure that they are easy to read and not open to misinterpretation personal records should:

- Only state relevant and useful information
- Be complete, factual, consistent, accurate and consecutive
- Be written clearly, legibly and in such a manner that they cannot be erased
- Be held securely and confidentially
- The information contained within records should be used for the purpose for which it was obtained and only shared appropriately and lawfully
- Be accurately dated, timed and signed. (The signatories name should be printed at the side of the first entry or be matched to an authorised signatory list)
- The use of abbreviations should be kept to a minimum. If abbreviations are used, they should be written in full the first time they are used and/or from an agreed abbreviation list
- In paper records, erasers and liquid paper should not be used to cancel errors. A single line should be used to cross out and cancel mistakes or errors and this should be signed and dated by the person who has made the amendment
- Be readable on any photocopies
- Be bound and stored so that loss of documents is minimised
- Identifying problems that have arisen and the action taken to rectify them

16.3 Personal records should not include:

- Unnecessary abbreviations, jargon, meaningless phrases, irrelevant speculation, and offensive subjective statements
- Personal opinions regarding the subject
- Or be kept for longer than is necessary

16.4 Line Managers are responsible for ensuring that staff personal files they hold are kept up to date and are stored / transferred securely. The Data Protection Act principles must be complied with (see Appendix 1 for a summary).

17 Records tracking

17.1 Accurate recording and knowledge of the whereabouts of all records is essential if the information they contain is to be located quickly and efficiently. One of the main reasons why records get misplaced or lost[3] is because their next destination is not recorded anywhere.

17.2 Tracking mechanisms should record the following (minimum) information:

- The item reference number or other identifier (e.g. Staff Number)
- A description of the item (e.g. the file title)
- The person, team or department, or place to whom it is being sent
- The date of the transfer to them

17.3 If a record is missing or lost it must be recorded as an incident on DATIX.

18 Manual tracking systems

18.1 Common methods for manually tracking the movements of active records include the use of:

- A paper register – a book or index card to record transfers
- File “on loan” (library-type) cards for each absent file, held in alphabetical or numeric order
- File “absence” or “tracer” cards put in place of absent files

18.2 Manual systems often suffer because they are rarely updated, quickly rendering such systems ineffective.

19 Electronically operated tracking systems

19.1 Electronic methods of tracking include the use of:

- A computer database in place of paper/card index eg a SharePoint list
- Bar code labels and readers linked to computers
- Workflow software to track documents electronically
- Use of e-mails to record and confirm sending/receipt of records

19.2 An electronic system can drastically reduce the amount of paper generated, and therefore the volume of paper to be stored. Using an electronic tracking system rather than, for example, a card index, can be more efficient – speeding up information retrieval times, reducing misfiling, and the problems associated with the use of absence markers.

19.3 The success of any tracking system depends on the people using it and therefore all staff must be made aware of its importance and given adequate training and updating. Tracking systems should be implemented and reviewed in liaison with relevant the Local Records Management Leads.

20 Storing Records

Current Paper Records

20.1 Where possible, active records in constant or regular use, or those likely to be needed quickly, will be kept in bases near to the staff who will need them. They are to be stored securely in accordance with Trust Data Security and Protection Guidance.

[3] A ‘misplaced or lost record’ is when a record cannot be found or is not available when required

20.2 Records must be held in central locations, so that they can be accessed by authorised staff.

20.3 When a record is no longer in use it can be retained within the department as long as storage space allows. Approved offsite storage facilities can be used for additional storage and archiving requirements. All records put into storage must be tracked so they can be retrieved when/if required. The use of a 'storage and archiving register', storage boxes and labels are detailed in the Archiving section below.

20.4 Less frequently used or archived records can be moved to more effective and space efficient storage options. Points to consider are:

- Appropriate environmental storage conditions
- Mobile racking and warehouse-type units
- Off-site secure storage and retrieval services
- Microfilm, microfiche and digital scanners to capture and store images
- Picture archiving for diagnostic imaging

20.5 It is important to recognise that different record types and different storage media may require different approaches. Appropriate retrieval arrangements should be agreed before archiving, including appropriate strategies for migration of electronic information between systems. Guidance on suitable environmental conditions for electronic data storage media (as recommended in BS 4783) is available from the National Archives (www.nationalarchives.gov.uk).

20.6 Contracts for non-NHS agencies or staff must require that patient information is stored and retrieved according to specified security and confidentiality standards and Data Protection guidelines. Records identified for permanent preservation must be stored within "places of deposit" approved by the National Archives.

20.7 Records storage areas must provide a safe working environment, with adequate space and equipment in compliance with health and safety legislation and fire regulations.

20.8 Storage areas must have sufficient capacity to accommodate records for the required minimum retention periods and to accommodate the annual growth of new records and the following factors should also be taken into account:

- Security (especially for confidential material)
- The user's needs
- Type(s) of records to be stored
- Their size and quantities
- Usage and frequency of retrievals
- Suitability, space efficiency and financial considerations

Electronic Records

20.9 All the principles of records storage, retention, archiving and disposal apply to electronic records and appropriate records retention periods are detailed in the records retention schedules. Corporate electronic records are to be saved in SharePoint (Teams/Site Collections) or network drives. Files that are being worked on off-line must be synchronised at the next available opportunity.

20.10 It is important that any records held electronically are filed in a consistent manner and are easily identifiable when they need to be retrieved. Where possible, electronic records should be held on network servers or cloud based system with appropriate permissions set to control access and prevent deletion. If records are held on a non-networked drive, they should be backed up regularly when access to the network is available or to another suitable back-up device.

20.11 When shared library/network drives (folders) are used within a service or department it is important that the folder structure reflects the business needs and that there is documented guidance available to ensure all staff are aware of how to file/retrieve records efficiently. Where the Trust's SharePoint portal is used for the storage and use of records it is important that the Content Owners are aware of the need to ensure records are easily identifiable and are retained following the Trust's records retention guidance.

20.12 Consideration on archiving and deletion of electronic records should also be included in any guidance documentation. The Records Manager can give further advice and guidance on this matter as required.

Scanned Records

20.13 Where scanning is used, the main consideration is that the information can perform the same function as the paper counterpart did and like any evidence, scanned records can be challenged in a court. This is unlikely to be a problem provided it can be demonstrated that the scan is an authentic record and there are technical and Trust means to ensure the scanned records maintain their integrity, authenticity and usability as records, for the duration of the relevant retention period.[4]

20.14 The legal admissibility of scanned records, as with any digital information, is determined by how it can be shown that it is an authentic record. An indication of how the courts will interpret evidence can be found in the civil procedure rules and the court will decide if a record, either paper or electronic, can be admissible as evidence.[5]

20.15 Where it is practical, consideration should be made to whether scanning of certain paper records would be beneficial to a service or department.

20.16 A scan of not less than 300 dots per inch (or 118 dots per centimetre) as a minimum is recommended for most records although this may drop if clear printed text is being scanned. Scanned records should be saved in Adobe pdf format.

20.17 Original paper copies of the document should not be destroyed until the scanning and quality checks have taken place and the system they were scanned to has gone through a back-up phase

Other Non-Paper Records

20.18 Microfilm and fiche have been used for many years and Courts will accept them as evidence. Microfilming comes into its own as a relatively cost-efficient way to capture and store images of otherwise bulky or deteriorating archival material:

- To minimise storage costs of materials, which would otherwise be destroyed
- To make copies available for other uses (such as research) whilst safeguarding the original
- To reduce the storage space occupied by low activity paper records

[4] Records Management Code of Practice for Health and Social Care: https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/

[5] https:/www.justice.gov.uk/courts/procedure-rules/civil/rules/part31

20.19 Services within the Trust will hold visual images – either as diagrammatic images and still photographs (which may be prints, negatives, slides, transparencies, and digital images) or as moving images (film or video), X-rays, telemedicine, diagnostic progress monitoring.

20.20 Photograph and film collections assembled by clinical and other staff through their work within the Trust should be regarded as Public Records and subject to these guidelines. Note that the provisions of the Data Protection Act on registration of records and restriction of disclosure relate to photographs of identifiable individuals as well as to other personal records e.g. blanking out of eyes does not render them unidentifiable.

20.21 Film should be stored in dust-free metal cans and placed horizontally on metal shelves. Microform, sound recordings and video-tape should be stored in metal, cardboard or inert plastic containers, and placed vertically on metal shelving.

Records security: Work Base, Home Working, Agile Working

20.22 All staff should undertake a risk assessment when adopting new ways of working to ensure that the data security and protection requirements are met.

21 Transfer of Non Electronic Personal Confidential Data

21.1 The transfer of all Personal Confidential Data (PCD) must satisfy current legislation and follow the NHS and Trust codes of practice, policies and guidance on the protection and use of patient / staff information.

21.2 Security and confidentiality of records should be paramount; therefore, records should never be taken off site unnecessarily or without the approval of the line manager. If requesting records / PCD ensure the sender has your full address details. The use of a signature block with contact details at the bottom of e-mails is strongly recommended as good practice.

21.3 When transferring PCD, especially patient / staff records, staff should:

- Ensure a track and trace system is in place so that there is an audit trail of where that record is
- Ensure it is enclosed in a folder/envelope/double envelope or transported in a suitable secure container

For further specific guidance on the transfer of PCD refer to the Trust's *Information Security Policy* and the *Confidentiality Code of Practice*.

22 Handling and Transporting Records

22.1 Because it is essential that records remain legible and usable:

- No-one handling, using or transporting records should eat, drink or smoke near them
- People using sensitive records should not leave them unattended on desks. Particularly they should not be left exposed to the view of unauthorised staff, patients, other clients or the public
- Personal records being carried on a site e.g. from the archive storage to a department, should be enclosed in an envelope, secure mail pouch or secure lidded box
- Records should be handled carefully when being loaded, transported or unloaded. Records should **never** be thrown
- Records should be packed carefully into vehicles or on trolleys to ensure that they will not be damaged by the movement of the vehicle

- Vehicles must be fully covered so that records are protected from exposure to weather, excessive light and other risks such as theft
- No other materials that could cause risks to records (such as chemicals) should be transported with records
- Vehicles containing records should be locked when unattended
- Records being transported should always be kept out of sight

23 Taking Records Off Site

23.1 Security and confidentiality of records should be paramount. Therefore, records should never be taken off site unnecessarily or without the approval of the line manager.

23.2 It is essential that any such records are tracked out of the respective department so that other staff are aware of the location of the record. If records are taken home, they must be stored securely and in accordance with the staff member's Professional Code of Conduct.

23.3 **Records must not be left in vehicles overnight.**

23.4 The Records Manager and Local Records Managers can provide advice on the precautions to take. For further guidance refer to the Trust's Information Security Policy.

24 Transfer of Records to Other Organisations

24.1 Where records are required to be transferred to another organisation e.g. a child's Health Visiting records, they must be transferred in their entirety to the organisations that have a legitimate need for them. Therefore, care should be taken to include all documents in a record including those that have been scanned. Accurate tracking of these records is essential.

24.2 Local procedures will need to be documented and approved for any regular transfers and specific circumstances.

25 Records Retention

25.1 Retention periods apply to the master (primary) copy of documents not copies (secondary) produced for reference. There is no requirement to retain both an electronic and paper copy of a record. As long as the electronic copy is held on a system that has the necessary backup processes in place it should be considered to be the primary copy. Records detailed in the Records Held by Health and Social Care Organisations should be retained for the minimum period stated in the Retention Schedule. Where records are not mentioned in this schedule or new types of record are developed, the Department of Health and Social Care (DHSC) or the National Archives will be consulted. In these cases, contact the Records Manager for guidance.

25.2 Where it is proposed that records will be retained for a period other than that specified in the NHS Retention & Disposal Schedule this should be reported to the Records Manager for approval.

25.3 Please note that NHS organisations wishing to keep records more than 30 years old for operational reasons beyond the minimum period specified in the Records Management Code and Practice for Health and Social Care should consult 'The National Archives' for advice.

26 Retention Schedules

26.1 Records are required to be kept for a certain period either because of statutory requirements or because they may be needed for administrative purposes during this time. There are a number of different types of records and depending on their particular use there are reasons for retaining records for different periods of time. Below are some current examples:

- Clinical Diaries: 2 years
- Children and Young People's records: Retain until the patient's 25th or 26th birthday
- Adult Health records (where not covered in another section of the schedule): 8 years
- General Dental Services records: 10 years
- Patient information leaflets: 6 years
- Complaints Case File: 10 years

26.2 The above list is a summary of the actual retention guidance. Please refer to the Records Management Code of Practice retention schedule for full details of retention guidance. All records must be stored securely until minimum retention periods have expired. Whilst the destruction of records is irreversible the cost of keeping them can be high and recurring.

26.3 Before storing/archiving records they must be sorted so that each type of record is kept in a logical order (e.g. alphabetical or date order) in separate storage boxes. This will ensure a common destruction date for that box.

27 Final Action

27.1 At the end of the relevant minimum retention period, one or more of the following actions will apply:

a) **Review:** records may need to be kept for longer than the minimum retention period due to ongoing administrative need. If this is the case, the Records Manager should be consulted as the Trust's retention schedules will need to be amended accordingly and a further review date set. Otherwise, one of the following will apply:

b) **Transfer a Place of Deposit or consult the National Archives:** in line with the Public Records Act, if the records have no ongoing administrative value but have, or may have, long-term historical or research value. Records with such value must be transferred to the Trust's approved Place of Deposit.

c) **Destroy:** where the records are no longer required to be kept due to statutory requirement or administrative need and they have no long-term historical or research value. In the case of health records, this should be done in consultation with clinicians in the Trust to confirm there is no clinical reason for continued retention or the need to transfer the record.

27.2 **All clinical records are confidential** so, when required, they must be destroyed using a confidential destruction method. For further guidance on this refer to the Confidential Waste section below.

27.3 When **deleting personal data** refer to the ICO guidance, which helps organisations to fully understand their obligations and promote good practice

28 Archiving

28.1 All records for archiving must be sorted and placed in the appropriate storage boxes. When archiving records, care should be taken to ensure the same type of records are kept together as they will then have similar retention periods and destruction dates.

28.2 Below is the recommended process for archiving and retrieving records. The actual archive process may vary as the Trust still has two archiving and storage facilities in use:

1. **Children's Services**: the storage facility at Centurion Park is used for storing and archiving children and young people's records. The archiving and storage process for this service is co-ordinated by the Porters and Records Assistants based at Coral House.
2. **Archiving and Storage Facility** contracted to Glyn Upton Removals. This currently contains two separate areas of archiving and the following processes:
    a. **Corporate and Shropshire County Services:** The process used by the Shropshire County based services (previously using the Abbey Works storage facility) is detailed in Appendix 9.
    b. **Telford and SE Locality Services:** The Storage and Archiving service used by Telford and Wrekin based services is detailed Appendix 10.

28.3 It is essential that the processes are followed to ensure all records are archived in a manner that ensures efficient identification and timely retrieval of a record when required.

29 Archive Box Label

29.1 All storage boxes must have an approved archive label in order that the box contents can easily be identified.

29.2 These labels should contain the following:

- A box reference number which has a year identifier
- Brief details on the box contents. This should include a reference to the date of closure of the record e.g. *Discharged Patient Records A to H - Dec 2017*
- Review date, if appropriate, when the box contents need reviewing before disposal
- Disposal date
- Contact details of the person in order to identify the owner for each archive box. It is important that the role and department is recorded in case the specific individual leaves the Trust

30 Storage and Archive Register

30.1 All the details in 29.2 should be recorded in the service / department's Storage and Archive Register. A more detailed description of the contents should be recorded in this register to ensure anyone trying to trace a record is able to identify where it is stored.

30.2 **Files to Archiving**. The following details the minimum steps to be followed when preparing records for archiving. Services or departments may wish to add additional steps to meet their specific system or process requirements.

1 A nominated individual from each service/department will be responsible for preparing records for archiving

2 The records are to be sorted in order that retention periods are not mixed within boxes i.e. records with different retention periods must not be put in the same archive box

3 Records are to be sorted and put in the box in a logical order

4 The printing out of a contents sheet of the records contained in the box is recommended

5. Boxes are not to be overfilled as lids must fit securely and be able to be sealed using suitable packing tape or string
6. Archive labels should be completed with the required information
7. The archive label should be attached to the box. If two are used one should be on the short side and one on the long side (not top and bottom)
8. Finally, the archive boxes should be sealed by tape, string or a tamper proof tag if required

30.3 Please note: archive boxes will not be accepted into archive storage without completed labels. Procedures for archiving records can be found in the Standard Operating Procedure.

31 Records Disposal

31.1 Most NHS records, even administrative ones, contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy such records is fully effective and secures their complete illegibility. Normally this will involve shredding (Note: cross shredding is the minimum requirement), pulping, or incineration.

31.2 Removable media such as CDs, memory sticks, hard drive units, backup tapes, audio/video tapes containing identifiable information must be reformatted with a random pattern to ensure data cannot be recovered or they must be physically destroyed. Contact the IT Department for advice and guidance on secure disposal of such media. Guidelines are contained within the Trust's *Information Security Policy*.

31.3 The Records Management Code of Practice 2021 includes reference to high profile legal cases which have an impact on retention.

31.4 The following are examples of when information cannot be destroyed or disposed of:

- If it is subject to a form of access request, for example a Subject Access Request (SAR) or a FOIA request
- If it is required for notified legal proceedings, for example a court order, or where there is reasonable prospect of legal proceedings commencing (an impending court case). This information will possibly be required for the exercising or defending of a legal right or claim
- If it is required for a coroner's inquest
- If it is of interest to a public inquiry, for example, who will issue guidance to organisations on what kind of records they may require as part of the inquiry. Once notified, organisations can re-commence disposal, taking into account what records are required by the inquiry. If in doubt, check with the Inquiry Team.

32 Confidential Waste

32.1 It is important that any confidential records are disposed of in a safe and secure manner. Confidential waste includes any material that contains information that would identify an individual patient, employee or business sensitive information. Confidential waste must be kept secure and protected against accidental loss, damage or unauthorised access up until its final destruction.

32.2 Confidential Waste Services are in place in a number of Trust locations using lockable confidential waste bins/containers which are collected and shredded onsite. Where these services are in place the collection will be monitored by nominated staff. A Certificate of Destruction must be obtained by the person responsible for contracting these bulk destructions services as evidence that the confidential waste has been disposed of securely. They should also maintain a log of the destruction of confidential waste.

32.3 If there is no Confidential Waste Service in place at a location, a suitable ‘cross cut’ type shredder must be used. If there is a requirement for bulk destruction of confidential waste at these locations the Records Manager should be contacted to give advice and guidance.

32.4 Destruction of electronic records and tape must be undertaken in accordance with the Trust’s Information Security Policy.

32.5 The Records Manager/Management Lead can give specific advice and guidance regarding confidential waste.

33 Consultation

33.1 This procedure has been developed by the Records Manager in consultation with representatives from services and departments across the Trust through the Data Security and Protection Assurance Group and relevant local team meetings and discussions. The Records Manager has also discussed particular areas with relevant specialist staff and clinical and administrative leads. The policy has also been presented to the Data Security and Protection Assurance Group before submission to the Information Governance Operational Group for final approval.

34 Dissemination

34.1 These guidelines will be disseminated by the following methods:

- Published to the Website for Directors/Senior Managers – to disseminate within their areas
- Staff – via newsletters/team briefings/training
- Awareness raising by Records Manager and Local Records Management Leads

35 Training

35.1 All new staff (employed and non-employed) will be given appropriate training as part of their corporate induction as part of the annual mandatory training programme, and attendance will be recorded and monitored (if appropriate).

35.2 The Trust will provide appropriate training to all staff as part of its annual mandatory training programme and attendance will be recorded and monitored (if appropriate).

35.3 The Trust will provide appropriate role specific Cyber Security and Information Governance training for key roles following training needs analysis.

35.4 The Trust will ensure that their staff are aware of its policies and requirements regarding Information Risk and appropriate training arrangements will be made available.

35.5 Links between Information Risk and other Information Governance requirements will be clarified for staff.

36 Review

36.1 This policy will be reviewed every two years by the Records Manager, liaising with the DSPAG to ensure the content remains relevant and up to date and reflects any changes in legislation, standards and professional codes of practice.

37 Compliance Monitoring

37.1 To achieve compliance with the Care Quality Commission and the Data Security & Protection Toolkit requirements regular audits of record keeping standards and practice will be undertaken, co-ordinated by the Records Manager.

37.2 **Note:** For specific details on monitoring related to health records refer to the monitoring section of the *Clinical Record Keeping Policy*.

38 Records Audits

38.1 The Records Manager will co-ordinate the audit of records management systems, processes and records liaising with the Clinical Audit Team and appropriate committees/groups to ensure the audits:

- Identify areas of operation that are covered by the Trust's policies and identify which procedures and/or guidance should comply with the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

38.2 The results of the records management audits will be reported initially to the Data Security and Protection Assurance Group then to the Information Governance Operation Group for further dissemination to other committees/groups as required e.g. Service Delivery Group - Quality and Safety Groups, Quality and Safety Committee and the Audit Committee.

39 Incident Reporting

39.1 Compliance monitoring will also be undertaken by the Risk Management Team and the Records Manager scrutinising reported incidents and near misses that relate to record keeping in accordance with the Incident Reporting Code of Practice. They will ensure remedial actions are taken and report findings initially to the Data Security and Protection Assurance Group and then to the Information Governance Operation Group and other relevant committees/groups, managers and members of staff as required.

40 Records of historical value

40.1 NHS organisations may deposit records of historical value with their local county archive service. These records may have historical or social value, and so deemed worthy of long-term preservation. They will know what has been deposited previously if they have value in evidencing how the NHS used to work. They may also be of value to social historians and genealogists. Contact the IG for further guidance.

Appendix 1

1.1 References

The following documents were used to prepare this Policy:

- Records Management Code of Practice for 2021: https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/
- The Data Protection Act, 2018 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- UK General Data Protection Regulation (UKGDPR) https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- The Freedom of Information Act, 2000 https://www.legislation.gov.uk/ukpga/2000/36/contents
- Human Rights Act, 1998
- The Public Records Act, 1958 http://www.legislation.gov.uk/ukpga/Eliz2/6-7/51
- The Access to Health Care Records Act, 1990 https://www.legislation.gov.uk/ukpga/1990/23/contents
- The Access to Medical Reports Act, 1988 https://www.legislation.gov.uk/ukpga/1988/28/contents
- Care Quality Commission: Fundamental standards - Good Governance (Regulation 17) http://www.cqc.org.uk/content/fundamental-standards
- Data Security and Protection Toolkit https://www.dsptoolkit.nhs.uk/
- Data Security and Information Governance: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance
- NHS Confidentiality Code of Practice: https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
- The Care Record Guarantee: https://digital.nhs.uk/binaries/content/assets/legacy/pdf/1/8/care_record_guarantee.pdf
- NHS Choices – Your health and care records: http://www.nhs.uk/nhsengland/thenhs/records/healthrecords/pages/overview.aspx
- Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000: http://www.legislation.gov.uk/ukpga/2000/36/section/46
- The National Archives website: Standards and best practice for records managers – http://www.nationalarchives.gov.uk/information-management/projects-and-work/standards-records-managers.htm

1.2 Related Documents

Shropshire Community Health NHS Trust policies and procedures which relate to this policy include:

- Clinical Record Keeping Policy
- NHS Number Retrieval, Verification and Use Procedure
- Procedural Documents Policy
- Information Security Policy

- Data Protection Policy (incorporating Confidentiality, and Special Categories)
- Information Quality Assurance Policy
- Information Risk Policy
- Incident Reporting Policy
- Mandatory Training Policy and Procedure
- Accessible Information Standard Policy
- Waste Management Policy
- Freedom of Information Policy

These documents are available on the Trust's public website and Staff Zone.

1.3 Glossary

Definitions

Word	Definition/Explanation	Source
Active Record	A record that is still in use.	
Appraisal	The process of evaluating an Trust's activities to determine which records should be kept, and for how long, to meet the needs of the Trust, the requirements of the Department of Health and Social Care and Data Protection Act.	
Archive	The term used when records are no longer active and are unlikely to require retrieval but are required to be retained until their disposal date.	
Caldicott Principles	Seven principles that should be followed when considering sharing confidential information, put together by Dame Fiona Caldicott following a review she carried out in regard to confidentiality in 1997 and update in March 2013 following the Information Governance (Caldicott 2) Review	
Classification	The systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system. (BS ISO 15489-1:2016)	NHS Code of Practice
Confidential waste	Includes any material that contains information that would identify an individual patient, employee or business sensitive information.	

Word	Definition/Explanation	Source
Corporate Record	A document becomes a record when it has been finalised and becomes part of the Trust's corporate information (a document has content – a record has content, context & structure)	
Disposal	The implementation of appraisal and review decisions. These comprise the destruction of records and the transfer of custody of records (including the transfer of selected records to an archive institution). They may also include the movement of records from one system to another (for example paper to electronic).	National Archives
Disposal	The implementation of appraisal and review decisions. These comprise of the destruction of records and the transfer of custody of the records.	
Electronic Staff Record (ESR)	This is the national, integrated Human Resources (HR) and Payroll system which will be used by all 600+ NHS Trusts throughout England and Wales.	Electronic Staff Record Website
Electronic Patient Record (EPR)	The Trust's main EPR is RiO	
Encryption	Encryption is the means of converting information using a code that prevents it being understood by anyone who isn't authorised to read it. Files, emails, even whole hard drives can be encrypted. As a general rule the more bits used for encryption the stronger it will be, so 128-bit is stronger that 64-bit.	Get Safe Online Organisation
Filing System	A plan for organising records so that they can be found when needed. (The National Archives, Records Management Standard RMS 1.1)	NHS Code of Practice
Inactive Record	A record no longer being updated or in use.	
Index cards	A series of cards that may be arranged alphabetically for the purpose of facilitating references to names, file titles, etc. or numerically for file references.	National Archives
Indexing	The process of establishing access points to facilitate retrieval of records and/or information. (BS ISO 15489-1:2016)	NHS Code of Practice

Word	Definition/Explanation	Source
Information Commissioner Office	The Information Commissioner Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.	ICO
Jointly Held Records	A record held jointly by health and social care professionals, for example in a Mental Health and Social Care Trust. A jointly held record should be retained for the longest period for that type of record, i.e. if social care has a longer retention period than health, the record should be held for the longer period.	NHS Code of Practice
Master Patient Index (MPI)	In medical systems the Master Patient Index (MPI) is an index referencing all patients known to an area, enterprise or Trust. The terms Patient Master Index (PMI) and Master Patient Index are used interchangeably.	NHS Code of Practice
Metadata	Metadata is "data [information] that provides information about other data" It is structured information about a resource. Metadata enables a resource to be found by indicating what the resource is about and how it can be accessed with a series of structured descriptions e.g. for a document: the creator, date, subject and title	
NHS Number	Introduced in 1996, the NHS number is a unique 10 character number assigned to every individual registered with the NHS in England (and Wales). The first nine characters are the identifier and the tenth is a check digit used to confirm the number's validity. Babies born in England and Wales are allocated an NHS number by Maternity Units, at the point of Statutory Birth Notification. The NHS number is used as the common identifier for patients across different NHS Trusts and is a key component in the implementation of the NHS CRS.	NHS Code of Practice
NHS Record	An NHS record is anything which contains information (in any media) which has been created or gathered as a result of any aspect of the work of NHS employees – including consultants, agency or casual staff.	NHS Code of Practice

Word	Definition/Explanation	Source
Personal Confidential Data (PCD)	Personal Confidential Data is data that contains sufficient information to be able to identify the specific person to whom the data belongs (patient or staff) e.g. name, date of birth, address. This generally excludes publicly available contact lists e.g. staff telephone directories. Note: Previously referred to as Personal Identifiable Data (PID)	
Primary Record	The record that is deemed to be the master record and is therefore subject to the relevant retention schedule. A primary record on a particular record should be either an electronic copy or paper, not both.	
Protective Marking	The process of determining security and privacy restrictions on records. Previously called ‘classification’.	NHS Code of Practice
Pseudonymisation	A method which disguises the identity of patients by creating a pseudonym for each patient identifiable data item.	
Publication Scheme	A publication scheme is required of all NHS Trusts under the Freedom of Information Act. It details information which is available to the public now or will be in the future, where it can be obtained from and the format it is or will be available in. Schemes must be approved by the Information Commissioner and reviewed periodically to make sure they are accurate and up to date.	NHS Code of Practice
Record	Information created, received and maintained as evidence and information by an Trust or person, in pursuance of legal obligations, or in the transaction of business. (BS ISO 15489.2016)	NHS Code of Practice
Records System / Record Keeping System	An information system which captures, manages and provides access to records through time. (The National Archives, Records Management: Standards and Guidance – Introduction Standards for the Management of Government Records) Records created by the Trust should be arranged in a record-keeping system that will enable the Trust to obtain the maximum benefit from the quick and easy retrieval of information. Record-keeping systems should contain descriptive and technical documentation to enable the system and the records to be understood and to be	NHS Code of Practice

Word	Definition/Explanation	Source
	operated efficiently, and to provide an administrative context for effective management of the records, including a documented set of rules for referencing, titling, indexing and, if appropriate, the protective marking of records. These should be easily understood to enable the efficient retrieval of information and to maintain security and confidentiality.	
Referencing	A referencing system helps to provide a means of identifying and retrieving records. Can be used when creating a register or index of records. Several types of referencing can be used: Alphabetical, Numerical, Alphanumeric or Keyword.	National Archives
Register	A list of records, usually in simple sequence such as date and reference number, serving as a finding aid to the records.	National Archives
Registration	Registration is the act of giving a record a unique identifier on its entry into a record-keeping system.	NHS Code of Practice
Retention	The continued storage and maintenance of records for as long as they are required by the creating or holding Trust until their eventual disposal, according to their administrative, legal, financial and historical evaluation.	NHS Code of Practice
Retention Schedule	A schedule containing descriptions of specific record types and the minimum periods that those records should be retained for.	
Review	The examination of records to determine whether they should be destroyed, retained for a further period, transferred to an archival repository.	
Secondary Record	A copy of a primary record held locally for a time specified by that service or department. Only required to be retained for a set period in order to fulfil the requirement of that service or department.	
Storage	The term used when records are likely to require access/retrieval. Storage can be onsite or at the Trust's approved Records Storage and Archiving location.	
Subject Access Request (SAR)	Under the DPA a person can request to see a copy of their records. To do this they must make a subject access request	

Word	Definition/Explanation	Source
	following the process detailed in the Trust’s Data Protection Policy.	
Summary Care Records (SCR)	Summary Care Records (SCR) are an electronic record of important patient information, created from GP medical records. It can be seen and used by authorised staff in other areas of the health and care system involved in the patient's direct care.	
Tracking	Creating, capturing and maintaining information about the movement and use of records. (BS ISO 15489-1:2001)	NHS Code of Practice
Transfer of Records	Transfer (custody) – Change of custody, ownership and/or responsibility for records. (BS ISO 15489-1:2001) Transfer (movement) – Moving records from one location to another. (BS ISO 15489-1:2001) Records identified as more appropriately held as archives should be offered to The National Archives, which will make a decision regarding their long-term preservation.	NHS Code of Practice
Version Control	The management of multiple revisions to the same document that enables one version of a document to be identified from another.	National Archives

1.4 Abbreviations

Term / Abbreviation	Definition / description
AHPs	Allied Health Professionals
CQC	Care Quality Commission
DHSC	Department of Health and Social Care
DfE	Department for Education
DPA	Data Protection Act
DSPT	Data Security & Protection Toolkit
ESR	Electronic Staff Record
EPR	Electronic Patient Record
FOI	Freedom of Information
GDPR	General Data Protection Regulation
GMC	General Medical Council
HCPC	Health and Care Professions Council
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IG	Information Governance
IM&T	Information Management and Technology
ISO	International Standards Organisation
MCA	Mental Capacity Act
MPI	Master Patient Index
NHS CRS	NHS Care Records Service
NHSLA	NHS Litigation Authority
NMC	Nursing and Midwifery Council
PALS	Patient Advice and Liaison Service
PCD	Personal Confidential Data. **Note:** Previously referred to as Personal Identifiable Data (PID)
SCHT	Shropshire Community Health NHS Trust

Appendix 2

2.1 Information Asset Owner responsibilities

The IAO and IAA is responsible for working with others, such as Information Governance, Information, IT, corporate and operational leads, to ensure that we are meeting national requirements as set out in the Data Security and Protection Toolkit (DSPT); and our obligations under the data protection legislation. This includes adhering to Trust policies, developing and implementing processes and procedures and contributing to evidence to demonstrate compliance as part of the annual assessment for the Trust. The key areas of focus include: data quality, records management, know your asset, IT protection, and liaising with suppliers.

There are 10 National Data Guardian standards as set out below:

Standard 1 – Personal confidential data
Standard 2 – Staff responsibilities
Standard 3 – Training
Standard 4 – Managing access
Standard 5 – Process review
Standard 6 – Responding to incidents
Standard 7 – Continuity planning
Standard 8 – Unsupported systems
Standard 9 – IT Protection
Standard 10 – Accountable suppliers

Full guidance can be found here Help (dsptoolkit.nhs.uk)

The above guidance documents will form the foundation for discussion, learning and actions at the IAO and IAA Network groups to ensure that we are pro-actively working towards, contributing to and improving compliance.

Policies that are specifically related to the IAO and IAA roles are:

- Information Risk Policy
- Data Protection Policy (including confidentiality)
- Individual Rights Policy
- Information Security Policy
- Information Quality Assurance
- National Data Opt-Out