# Policy Document

**Reference: DSP16**

University Hospitals of North Midlands NHS Trust

# Information Lifecycle & Records Management (Corporate and Clinical Records)

| | |
|---|---|
| **Version:** | **3** |
| **Date Ratified:** | **January 2023 by Executive Data Security & Protection Group** |
| **To Be Reviewed Before:** | **January 2026** |
| **Policy Author:** | **Data Security & Protection Manager** |
| **Executive Lead:** | **Senior Information Risk Owner** |

## Version Control Schedule

| Version | Issue Date | Comments |
|---|---|---|
| 1 | April 2021 | New Policy. Reviewed by Records Management Group, Data Security & Protection Group and Ratified by Executive Data Security & Protection Group |
| 2 | September 2021 | inclusion of text relating to Clinical Records referencing Multidisciplinary Health Records Policy<br>Inclusion of a Governance Framework at Appendix 1 |
| 3 | January 2023 | Policy Review/Refresh<br>Page 10 – inclusion of requirement to access data for business use only under Staff Responsibilities<br>Page 17 – Updated link to NHSX Records Retention guidance/search engine<br>Page 6 – referenced the C64 Supporting Transgender individuals policy<br>Page 11 – 6.1 viii updated to reference DSP training stat and mand |

## Statement on Trust Policies

The latest version of 'Statement on Trust Policies' applies to this policy and can be accessed here

University Hospitals of North Midlands NHS Trust

## Equality Impact Assessment (EIA)

The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. The Equality Impact Analysis Form is designed to help consider the needs and assess the impact of each policy. To this end, EIAs will be undertaken for all policies.

| | |
|---|---|
| **Title of policy being assessed** | DSP16 – Information Lifecycle & Records Management Policy |
| **Policy reference & version number** | DSP16 v3 |
| **Summary of changes made on this review** | Review/Refreshed Policy |
| **Please list which service users, staff or other groups have been consulted with, in relation to this** | Records Management Group |
| **Were any amendments made as a result? If yes, please specify** | Review/refresh of Policy due to the due date |
| **Which Executive Director has been consulted on?** | Director of Digital Transformation |
| **Does this policy have the potential to affect any of the groups listed below differently - please complete the below.** Prompts for consideration are provided, but are not an exhaustive list | |

| Group | Is there a potential to impact on the group? (Yes/No/Unsure) | Please explain and give examples | **Actions taken to mitigate negative impact** *(e.g. what action has been taken or will be taken, who is responsible for taking a future action, and when it will be completed by – may include adjustment to wording of policy or leaflet to mitigate)* |
|---|---|---|---|
| **Age** | No | | |
| **Gender** | No | | |
| **Race** | No | | |
| **Religion & Belief** | No | | |
| **Sexual orientation** | No | | |
| **Pregnancy & Maternity** | No | | |
| **Marital status/civil partnership** | No | | |
| **Gender Reassignment** | No | | C64 Supporting Transgender Individuals is referenced in the Policy |

| Group | Is there a potential to impact on the group? (Yes/No/Unsure) | Please explain and give examples | Actions taken to mitigate negative impact *(e.g. what action has been taken or will be taken, who is responsible for taking a future action, and when it will be completed by – may include adjustment to wording of policy or leaflet to mitigate)* |
|---|---|---|---|
| **Human Rights** | No | | |
| **Carers** | No | | |
| **Socio/economic** | No | | |
| **Disability** | Yes | | • UHNM staff that have visual disabilities will have audio on their laptop/workstation which will read the text to them. This is the responsibility of the line manager and will already be actioned for those with a reported disability.<br>• Any request made to adjust the format e.g. size, colour of font will be met. This will be the reasonability of the admin colleague dealing with the request and will be actioned upon request |

| | | |
|---|---|---|
| **Are there any adjustments that need to be made to ensure that people with disabilities have the same access to and outcomes from the service or employment activities as those without disabilities?** (e.g. allow extra time for appointments, allow advocates to be present in the room, having access to visual aids, removing requirement to wait in unsuitable environments, etc.) | **Yes** | |
| | Audio available on laptops/workstations<br>Adjust the text format e.g. font size and colour | |
| **Will this policy require a full impact assessment and action plan?** (a full impact assessment will be required if you are unsure of the potential to affect a group differently, or if you believe there is a potential for it to affect a group differently and do not know how to mitigate against this - please contact the Corporate Governance Department for further information) | **Yes** | **No** |
| | | ✓ |

**CONTENTS** **Page**

## 1. INTRODUCTION

1.1 This document relates to all Trust's records, both Clinical (as detailed within the Multi-Disciplinary Health Records Policy (RE01)) and Non-Clinical, Corporate records. The Trust's Multi-Disciplinary Health Records Policy which deals with the specific requirements of a clinical record.

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

1.3 The **Records Management: NHS Code of Practice** has been published by the Department of Health as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

1.4 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.

1.5 The Trust Board of Directors has adopted this Information Lifecycle & Corporate Records Management policy and is committed to on-going improvement of its records management functions as it believes that it will gain a number of organisational benefits from so doing. These include:

- better use of physical and server space;
- better use of staff time;
- improved control of valuable information resources;
- compliance with legislation and standards; and
- reduced costs.

1.6 The Trust also believes that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of records management as a designated corporate function.

1.7 All NHS records are Public Records under the Public Records Acts. The Trust will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice, in particular:

- The Public Records Act 1958;
- The Data Protection Act 2018 (DPA)
- The General Data Protection Regulations [Ref (EU) 2016/679] (GDPR)
- The Access to Health Records Act 1990
- The Freedom of Information Act 2000;
- The Environmental Information Regulations 2004
- The Common Law Duty of Confidentiality;
- The NHS Confidentiality Code of Practice; and
- Any new legislation affecting records management as it arises.

1.8 The recording of pertinent information and record-keeping is fundamental and an integral requirement for the delivery of high quality healthcare. Well documented records are essential for good professional practice.

1.9 Records are a valuable resource because of the information they contain. That information is only usable if it is correctly recorded in the first place, is regularly up-dated, and is easily accessible when it is needed. Information is essential for the Trust to function appropriately and efficiently

and an effective record management service ensures that such information is properly managed and is available whenever, and wherever required, in whatever media it is required and also to:

- support patient care and continuity of care;
- support day to day business processes and procedure which underpin delivery of care;
- support evidence-based clinical practice;
- support sound administrative and managerial decision making, as part of the knowledge base for Trust services;
- meet legal requirements, including requests from patients, staff and others under the Data Protection Act 2018 (for living individuals) and the Access to Health Records Act 1990 in relation to patient records (for deceased patients);
- support clinical and other audit processes and;
- support improvements in clinical effectiveness through research and support archival functions by taking account of the historical importance of the material and the needs for future research.

Clinical information carries the same quality requirements and these records are covered in the Multi-Disciplinary Health Records Policy (RE01).

1.10 In developing this policy the Trust has given due regard to its legal requirements and obligations and the NHS Information Governance agenda and best practice standards including, but not limited to:-

- The legal and regulatory framework as set out within the "NHS Information Governance: Guidance on Legal & Professional Requirements"
- The "NHS Information Governance Toolkit" and its component requirements
- The "Records Management: NHS Code of Practice"
- The "Information Security Management: NHS Code of Practice"
- "ISO 27001 and 27002", the International Standards for Information Security
- "ISO 27799: Health Informatics - Information Security Management in Health Using ISO-IEC 27002"

## 2. STATEMENT OF INTENT / SCOPE OF THE POLICY

This policy applies to University Hospitals of North Midlands NHS Trust (UHNM), referred to as the 'Trust', and includes all hospitals and units managed by UHNM.

This policy relates to all records (both clinical and non-clinical) held in any format by the Trust. (The content of clinical records will be subject to the standards of clinical record keeping as detailed in the Multidisciplinary Health Records policy). These include:

- all administrative records (eg personnel, estates, financial and accounting records, notes associated with complaints, policies, procedures, meeting minutes etc); and

The aim of this policy is to promote best practice and provide:

- a framework for consistent, coherent and compatible records;
- a set of robust but flexible standards which are derived from the NHS Litigation Authority (NHSLA) and the requirements (standards) contained in the Data Security & Protection Toolkit. The standards are generic and should be applied to all areas.

This policy applies to all those working in the Trust, in whatever capacity. A failure to follow the requirements of the policy may result in investigation and management action being taken as considered appropriate.

This may include formal action in line with the Trust's disciplinary or capability procedures for

Trust employees; and other action in relation to other workers, which may result in the termination of an assignment, placement, secondment or honorary arrangement. Non-compliance may also lead to criminal action being taken.

Other relevant policies:

Data Quality Policy – C27
Multidisciplinary Health Records Policy – RE01
Clinical Photographic & Video Policy – RE02
Supporting Transgender Individuals – C64

## 3. SUMMARY

This document sets out a framework within which the staff responsible for managing the Trust's records can develop specific policies and procedures ensuring that these records are managed and controlled effectively, at best value, commensurate with legal, operational and information needs, and within which all other staff handling records can ensure compliance with the legal obligations and best practice surrounding records management.

The overall objective of this policy is to provide clear direction for the management of all Trust records, including both clinical and corporate records.

## 4. DEFINITIONS

### 4.1 Records Management

***Records Management*** is a 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.

### 4.2 Records Life Cycle

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 either confidential disposal or archival preservation.

### 4.3 Documents and Records

In this policy, ***Documents*** are defined as recorded information, in any form, created or received by the Trust. A document used in the transaction of the Trust's business or conduct of affairs that will need to be kept as evidence of business transactions, routine activities or as a result of legal obligations becomes a **'record'**.

## 4.4 Information

***Information*** is a corporate asset. All data and Trust records are important sources of administrative, evidential and historical information. They are vital to the Trust to support its current and future operations (including meeting the requirements of Freedom of Information legislation and the Environmental Information Regulations), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

## 4.5 Information Asset

Information assets are definable information resources owned or contracted by an organisation that are 'valuable' to the business of the organisation. This would include all databases/systems and applications and all manual records.

## 4.6 Person Identifiable / Confidential Information

Person identifiable / confidential information is information which could singly or compositely identify a person – in which the person is the focus of the information and which links that individual to details which would be regarded as private e.g. name and private address or postcode, name and home telephone number etc.

All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent. This includes the nationally recognised NHS number.

## 4.7 Special Category Information

This is information where loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community.

This is wider than, but includes, data defined as sensitive under the Data Protection Act 2018. In addition to personal and clinical information, financial and security information is also likely to be deemed "special category".

Examples of sensitive information include information in relation to a person's:

- Health or physical condition
- Sexual life
- Ethnic origin
- Religious beliefs
- Political views
- Criminal convictions
- Trade Union Membership

For this type of information even more stringent measures should be employed to ensure that the data remains secure.

## 4.8 Clinical Information

The term clinical records refers to recorded information, in any form, created or received and maintained by the Trust relating to the documentation of patient care and treatment. This includes but is not limited to the following:

- Patient health records (electronic or paper-based), and concerning all specialities;
- Records of private patients seen on NHS premises;
- Accident and Emergency, birth and other registers;
- Theatre, minor operations and other related registers;

- X-Ray and imaging reports, outputs and images;
- Photographs, slides, and other images;
- Microform (i.e. microfiche/microfilm);
- Audio and video tapes, cassettes, CD-ROMS etc.;
- E-mails relevant to patient care;
- Computerised records i.e. clinical records in all electronic formats;
- Scanned documents relevant to patient care.
- Letters relevant to patient care;
- Hand-Over sheets;
- Diaries relevant to patient care;
- MDT Lists;
- Medical Reports and;
- Clinical Trials/Audit information.

The content of clinical records will be subject to the standards of clinical record keeping as detailed in the Multidisciplinary Health Records policy

### 4.9 Corporate / Non Clinical Information

The term corporate records or non-clinical records includes but is again not limited to the following:

**All records relating to:**

- Estates/Engineering;
- Information Management & Technology (IM&T);
- Personnel/Human Resources;
- Financial;
- Purchasing/Supplies;
- Complaints.

**Examples would include:**

- Policies
- Standard Operating Procedures
- Minutes of Meetings
- Terms of Reference
- Contracts
- Personnel Records
- Disciplinary Records
- Payroll Records
- Budget Statements
- Staff Surveys
- Project Plans
- Training Records
- Action Plans
- Audit Reports

### 4.10 Governance Framework

A Governance Framework detailing the policies and SOPs relevant to Records Management can be found at Appendix 1.

## 5. ROLES AND RESPONSIBILITIES

The Trust Board is ultimately responsible for ensuring the Trust meets its legal responsibilities, and for the adoption of internal and external governance requirements. The Performance & Finance Committee will be updated on Data Security & Protection issues via highlight report, 6 times annually.

**Chief Executive**
The Chief Executive as the Accountable Officer for the Trust has overall accountability and responsibility for IG throughout the Trust and is required to provide assurance that all risks to the Trust, including those relating to information, are effectively managed and mitigated.

**Senior Information Risk Owner (SIRO)**
The Trust SIRO is responsible to the Chief Executive for Data Security & Protection and acts as an advocate for information risk on the Trust Board.

**Caldicott Guardian**
The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of Personal Identifiable Data (PID). The Caldicott Guardian is responsible for ensuring PID is shared in an appropriate and secure manner.

**Head of Data Security & Protection/Data Protection Officer**
The Head of Data Security & Protection/Data Protection Officer (DPO) has overall responsibility for managing the data security & protection function and as DPO will advise and monitor compliance with the GDPR and DPA. They are responsible for ensuring effective management, accountability, compliance and assurance for all aspects of the data security & protection agenda. They will also be the first point of contact with the Supervisory Authority – the Information Commissioner's Office.

**Data Security & Protection Manager**
The Trust's Data Security & Protection Manager is responsible for supporting the Data Protection Officer in the implementation of the Trust's DSP agenda, including compliance of records management policies and principles

**Data Security & Protection Advisor**
The Trust's Data Security & Protection Facilitator(s) is responsible for supporting the Data Security & Protection Manager in the delivery of the DSP agenda, including compliance of records management policies and principles.

**Data Security & Protection Executive Group (EDDSPG)**
The SIRO and Caldicott Guardian are joint chair of the Trust's Executive Digital and Data Security & Protection Group. This group is responsible for receiving assurances relating to the day to day management of the individual components of the Trust's Data Security & Protection Framework

**Data Security & Protection Operational Group (DSPOG)**
The Data Protection Officer chairs the Trust's DSPOG. This group is responsible for overseeing the day to day management of the individual components of the Trust's Data Security & Protection Framework, including monitoring adherence to Trust records management policies and principles

The Data Security & Protection Governance pack provides more detail on the make-up of the Groups which provide assurance that the Trust meets its obligations around data security & protection.

**Information Security Manager (RA and Privacy)**
Provides advice to the Trust, ensuring compliance, and conformance, with local and national requirements, and, generally, on information risk analysis/management incorporating the Privacy Officer role which focuses on ensuring privacy related alerts from electronic systems (e.g. Summary Care Record) are investigated for appropriateness, as well as other privacy compliance work as necessary, including monitoring adherence to Trust records management policies and principles

**Cyber Security Lead**
Provides advice to the Trust, ensuring compliance and conformance, with local and national requirements and, generally, on cyber security issues across the Trust, including monitoring adherence to Trust records management policies and principles.

**Health Records Manager**
Oversees the operational management of the Trust's paper health records ensuring that security is maintained in accordance with the legislation. The Health Records function also provides the subject access function for patients to access their clinical records, including monitoring adherence to Trust records management policies and principles

**Assistant Director of Human Resources/Governance Lead**
Has responsibility for ensuring that the HR function meets the legislated requirements of the Data Protection Act 2018 in terms of security of information and, where an official Subject Access Request is submitted, access to records by staff (both current and former), including monitoring adherence to Trust records management policies and principles). Divisions are responsible for the security of information and access to staff records that are held locally.

**All Staff**
All staff, via job roles and contracts of employment/professional registrations must comply with specific data security related legal and ethical obligations and therefore must be aware of the related standards which impact within their area of responsibility. Individual staff must ensure that they make themselves aware of all policies and associated Standard Operation Procedures referenced in this document and abide by their contents. Any personal and corporate information, is managed legally, securely, and efficiently in order to assist in the delivery of the best possible care/practice. Staff can email the Data Security & Protection team on DSPUHNM@uhnm.nhs.uk with any data security related queries. In addition, all staff are responsible for ensuring that they meet and adhere to all Trust records management policies, procedures and principles.

Staff should be aware that it is a criminal offence to access Personal Identifiable data (S.170 of the DPA 2018) without a valid business reason to do so, and that includes accessing patient information as well as staff's own records or those of family and friends, even with consent. The Trust views such actions as gross misconduct and disciplinary action, according to Trust procedures, may be taken if such access is identified

## 6. THE POLICY

### 6.1 Aims of the Records Management System

Records must be maintained in a system that ensures they are properly stored and protected throughout their life cycle; this includes all electronic records, including any records that are migrated across to new systems, as well as all manual records. Therefore, before procuring new systems or putting new processes in place, organisations should take into account the need to keep up with technological progress (e.g. new hardware, software updates) to ensure that records remain accessible and retrievable when required.

The aims of the Trust's Records Management System are to ensure that:

i. **records are available when needed** - from which the Trust is able to form a reconstruction of activities or events that have taken place;

ii. **records can be accessed** - records and the information within them are grouped in a logical structure to ensure quick and efficient filing and retrieval and so that they can be located and displayed in a way consistent with its initial use, and that the **current version is identified** where multiple versions exist. This will also aid implementation of authorised disposal arrangements, i.e. archiving or destruction;

iii. **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;

iv. **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;

v. **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. There should be suitable storage areas so that records, whether physical or electronic, remain accessible and usable throughout their life cycle, this includes ensuring that technological upgrades are supported;

vi. **records are secure** - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails track all access (e.g. sign in/out logs or computer generated audit trials), use and changes. A variety of security measures should be implemented for example, authorised access to storage and filing areas, lockable storage areas, user verification, password protection and access monitoring. This would also include maintaining a log of when records are issued form and/or returned from storage areas on site or to authorised off-site facilities;

vii. **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;

viii. **staff are trained** – the Data Security and Protection Stat and Man training is completed by all staff so that all are made aware of their responsibilities for record-keeping and record management; and

ix. **cross-referencing** of electronic records to their paper counterparts (where dual systems are maintained). A formal assessment should be undertaken and reviewed by the Corporate Records Management Group or Clinical Health records Group, depending on the nature of the information, where duplicate records are required to be retained.

Inventory of Record Collections

The Trust will establish and maintain mechanisms through which departments and other units should register the records they are maintaining. The inventory will be reviewed annually via the Corporate Records Audit. The inventory of record collections will facilitate:

i. the classification of records into series;
ii. the recording of the responsibility of individuals creating records; and
iii. the auditing of records management practices.

## 6.2 Creation of Records

Record creation is one of the most important processes in records management and all departments should create good records in an effective system. However, creating a record is not enough unless the record is then captured or filed into a filing system created and managed by the organisation.

It is important that records are kept in their context and the best way to achieve this is to file or classify them. Records cannot be tracked or used efficiently if they are not classified or if they are classified inappropriately. Records captured or filed in a corporate filing system will possess some of the necessary characteristics to be regarded as authentic and reliable.

Whatever the format of the records, they should be saved into a proper records management system.

A common format for the creation of records will ensure that those responsible for record retrieval are able to locate records more easily.

Staff should be aware of the differences between a document and a record. A document, as defined above, is any piece of written information in any form, produced or received by an organisation or person. It can include databases, website, email messages, word and excel files, letters, and memos. Some of these documents will be ephemeral or of very short-term value and should never end up in a records management system (such as invitations to lunch).

Some documents will need to be kept as evidence of business transactions, routine activities or as a result of legal obligations, such as policy documents. These should be placed into an official filing system and at this point, they become official records. In other words, all records start off as documents, but not all documents will ultimately become records.

**Basic rules to follow when creating records:**

6.2.1 All documents should have a clear descriptive name that is meaningful to the department responsible for the record and that would give a clear indication of the contents of the record to anybody else.
6.2.2 All documents should have a unique reference that is meaningful to the department responsible for the record.
6.2.3 All documents should use version control and version numbers should be changed each time the document is amended. Previous versions should be retained for an appropriate period depending on the nature of the information within the document.
6.2.4 All records and documents should be filed in an appropriately structured filing system
6.2.5 Records should have a protective mark applied where appropriate.

## 6.3 Logging a Query

From time to time it may be necessary to amend a clinical Health record (in certain circumstances patients have the right to rectify their records – always check with the Data Security & Protection team when these requests are made). Requests may be as the result of a query on behalf of the patient or member of staff and may include demographic or clinical information. Extreme caution should be exercised in such circumstances and staff need to follow the advice and guidance provided in their system training. If there is any doubt, staff should contact the Data Security& Protection Team (DSPUHNM@uhnm.nhs.uk).

## 6.4 Naming Conventions

Naming conventions should:

6.4.1 give a unique name to each record;
6.4.2 give a meaningful name which closely reflects the records' contents;
6.4.3 express elements of the name in a structured and predictable order;
6.4.4 locate the most specific information at the beginning of the name and the most general at the end;
6.4.5 give a similarly structured and worded name to records which are linked (for example, an earlier and a later version).

## 6.5 Filing structures

A clear and logical filing structure that aids retrieval of records should be used. Ideally, the filing structure should reflect the way in which paper records are filed to ensure consistency. However,

if it is not possible to do this, the names allocated to files and folders should allow intuitive filing.

Filing of the primary record to local drives (i.e. C drive usually 'my documents') on PCs is not permitted and on laptops is strongly discouraged.

The agreed filing structure should also help with the management of the retention and disposal of records.

## 6.6 File and Folder Referencing

A referencing system should be used that meets the organisation's business needs, and can be easily understood by staff members that create documents and records. Several types of referencing can be used, for example, alphanumeric; alphabetical; numeric or keyword.

The most common of these is alphanumeric, as it allows letters to be allocated for a business activity, for example, HR for Human Resources, followed by a unique number for each record or document created by the HR function.

It may be more feasible in some circumstances to give a unique reference to the file or folder in which the record is kept and identify the record by reference to date and format.

## 6.7 Tracking and Tracing

There should be tracking and tracing procedures in place that enable the movement and location of manual records to be controlled and provide an auditable trail of record transactions. The process need not be a complicated one, for example, a tracking procedure could comprise of a book that staff members sign when a record is physically removed from or returned to its usual place of storage (not when a record is simply removed from a filing cabinet by a member of staff from that department as part of their everyday duties).

Tracking mechanisms to be used should include:

6.7.1 the item reference number or identifier;
6.7.2 a description of the item (for example the file title);
6.7.3 the person, position or operational area having possession of the item;
6.7.4 the date of movement.

Examples of systems for monitoring the physical movement of records include:

- location cards;
- index cards;
- docket books;
- diary cards;
- transfer or transit slips;
- bar-coding;
- computer databases (e.g. electronic document management systems);

All physical corporate records must be tracked when they are removed from a filing system. Tracking will involve recording when the file was removed; who took ownership of the file (i.e. where it went to) and the tracker should be updated when the file is returned

The movement of any other manual records, including other clinical information that does not form part of the health records must be tracked.

The system adopted should maintain control of the issue of records, the transfer of records between persons or operational areas, and return of records to their home location for storage.

The simple marking of file jackets to indicate to whom the file is being sent is not in itself a

sufficient safeguard against files going astray.

All records tracking systems must include regular records audits and monitoring procedures.

### 6.8 Appraisal, Retention and disposal

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 business functions.

The destruction of records is an irreversible act, while the cost of preserving records worthy of permanent preservation is high and continuing.

The Trust has adopted the retention periods set out in the Records Management: NHS Code of Practice, a copy of which is published on the Trust's intranet – see the Data Security & Protection Intranet Page. Records should be reviewed regularly and destroyed when the retention period set out with the Records Management: NHS Code of Practice is met. If a need to retain records beyond this period is established the manager responsible for the records should submit a risk assessment to the Records Management Group, depending on the nature of the records, stating the reasons why the records need to be retained.

The retention schedules identify minimum retention periods and a local review will determine whether records are to be selected for permanent preservation, destroyed or retained by the organisation for research or litigation purposes. Whatever decisions are made they must be documented as part of a consistent and consistently applied records management policy within the organisation.

The guidelines shown below must be followed when using the retention schedules:

i. Retention periods in the retention schedules in Records Management: NHS Code of Practice is minimum retention periods and therefore local business requirements/instructions must be considered before applying retention periods in the schedules. A risk assessment should be completed where a need to retain records beyond the period documented in the NHS Records Management Code of Practice is identified.

ii. Local decisions should be considered where the final action is destruction bearing in mind the need to preserve records, the use of which may not be predictable at the present time, but which may be of historic value. NHS organisations should take advice from their local approved Place of Deposit or from The National Archives;

iii. Recommended minimum retention periods should be calculated from the end of the calendar year following the last entry in the record (date of last patient contact) or other specified dates as shown in the national retention schedules;

iv. The selection of files for permanent preservation is partly informed by precedent (the establishment of a continuity of selection) and partly by the historical context of the subject (the informed identification of a selection).

v. The provisions of the Data Protection Act 2018 must also be complied with, throughout a record's lifecycle and it is necessary to provide secure storage for them. There is also a data protection requirement not to keep personal data for longer than necessary taking account of the purpose for which it was collected;

When developing or purchasing new systems the organisation should consider how retention/disposal periods will work or can be factored into the system. For paper corporate records, this may be using clearly marked labels on each folder to state the minimum retention period, and a log kept so that records can be easily appraised.

Electronic document management systems, such as the Trust's intranet, may have the functionality built within them to set the disposal period for a record based on certain defined rules.

Methods used throughout the destruction process must provide adequate safeguards against the accidental loss or disclosure of the contents of the records. If contractors are used, they should be required to sign confidentiality undertakings and to produce written certification as proof of destruction.

A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved, so that the organisation is aware of those records that have been destroyed and are therefore no longer available. Disposal schedules would also constitute the basis of such a record.

## 6.9 Scanning of Records

BS 10008 and BIP 0008 Code of Practice standards relate to "Evidential weight and legal admissibility of information stored electronically" so that they can be relied upon in Court (Civil Evidence Act 1995). The Trust complies with the standards set in these codes of practice when scanning health records.

Non-health records also require formal documented procedures in place to ensure the integrity of records, including storage and retrieval and, auditable records of your scanning activities.

## 6.10 Selection of NHS Records for Permanent Preservation

All NHS records are public records under the terms of the Public Record Act 1958. The timescale for retention of Public Records is reducing, over a 10 year period, from 30 to 20 years. Records selected for permanent preservation must be transferred to the Public Record Office (PRO) or kept in a place of deposit, appointed under S.4(1) of the 1958 Act. In general, records worthy of preservation from NHS organisations are appropriate for deposit in the nearest Local Authority Record Office, which has been approved by The National Archives.

## 6.11 Disposing of Unwanted Records

### 6.11.1 How long should records be retained?

The length of the retention period depends upon the type of record and its importance to the activities of the Trust. The Department of Health's Records Management: NHS Code of Practice and the Retention and Disposal Schedules takes account of legal requirements and sets out the minimum retention periods for both clinical and corporate records. This link takes the user to a search function which it is hoped will make it easier to identify the particular retention scheduled being queried. The Trust has, however, discretion to keep records for longer, subject to a risk assessment detailing local needs, affordability and, where records contain personal information, the requirements of the Data Protection Act 2018. The retention schedule may not be a complete list of every type of record and the Trust may need to seek advice about the appropriate retention periods for record types not contained in the Schedule. In the first instance the Trust's health records manager or Data Security & Protection team should be consulted.

### 6.11.2 Who makes the decision?

There are two principal options for disposal of records - to destroy or to dispose for example, by passing on to another organisation. As can be seen from the Retention and Disposal Schedule, some records have fixed retention periods, whilst others will need more careful consideration. In many cases the staff in the department which ordinarily

uses them should be able to decide. If not specialist guidance should be sought via the Department of Health's Records Management Mailbox recordsmanagement@dh.gsi.gov.uk

Operational managers are responsible for ensuring that all records are periodically and routinely reviewed to determine what can be disposed of in the light of local and national guidance. The Trust's Records Management Group has been established to advise on local policy, particularly for the retention, archiving, or disposal of sensitive personal health records.

### 6.11.3 What are the options for disposal?

Most Trust records should be destroyed as soon as practicable after the expiry of the relevant minimum retention period, but there are other options for disposal. Because the destruction of records is an irreversible act, it is vital to consider all the available options in order to arrive at the right decision.

Disposal does not just mean destruction. It can also mean the transfer of records from one type of media to another e.g. paper to microfilm or to computer; or from one user to another. It could involve depositing records with an organisation which wishes to carry on using it e.g. a hospital or Local Authority Record Office, the National Archives or another bona fide research body, for example a university or established research institute recognised by a Local Research Ethics Committee, or to commercial off-site storage if the organisation wishes to retain the records in original paper format but does not have the storage space available within its premises, as previously stated a log of all records retained off-site should be maintained by the Trust and this log should be reviewed regularly by the Corporate Records Management Group. Advice about these options (and the implications of the Public Record Act) is available from the National Archives.

### 6.11.4 What are the rules for destruction?

NHS health records contain sensitive and confidential information. It is therefore vital that confidentiality is safeguarded at every stage of the lifecycle of the record including destruction and that the method used to destroy such records is fully effective and ensures their complete illegibility. Information on the requirements for Health Records destruction is contained in the Multi-Disciplinary Health Records Policy.

Non-health records can be securely destroyed using the Trust's Confidential Waste Bins. For bulk destruction (in the case of office moves, for example) – contact the Data Security & Prevention team for advice. This information is removed and securely destroyed under a contract to the Trust and the service is audited by the DSP Team.

## 7. REVIEW

This Policy is subject to review when any of the following conditions are met:

- The adoption of the Policy highlights errors or omissions in its content;
- Where other policies/strategies/guidance issued by the Trust conflict with the information contained herein;
- Where the procedural or guidance framework of the NHS evolves/changes such that revision would bring about improvement;
- The review date has elapsed;

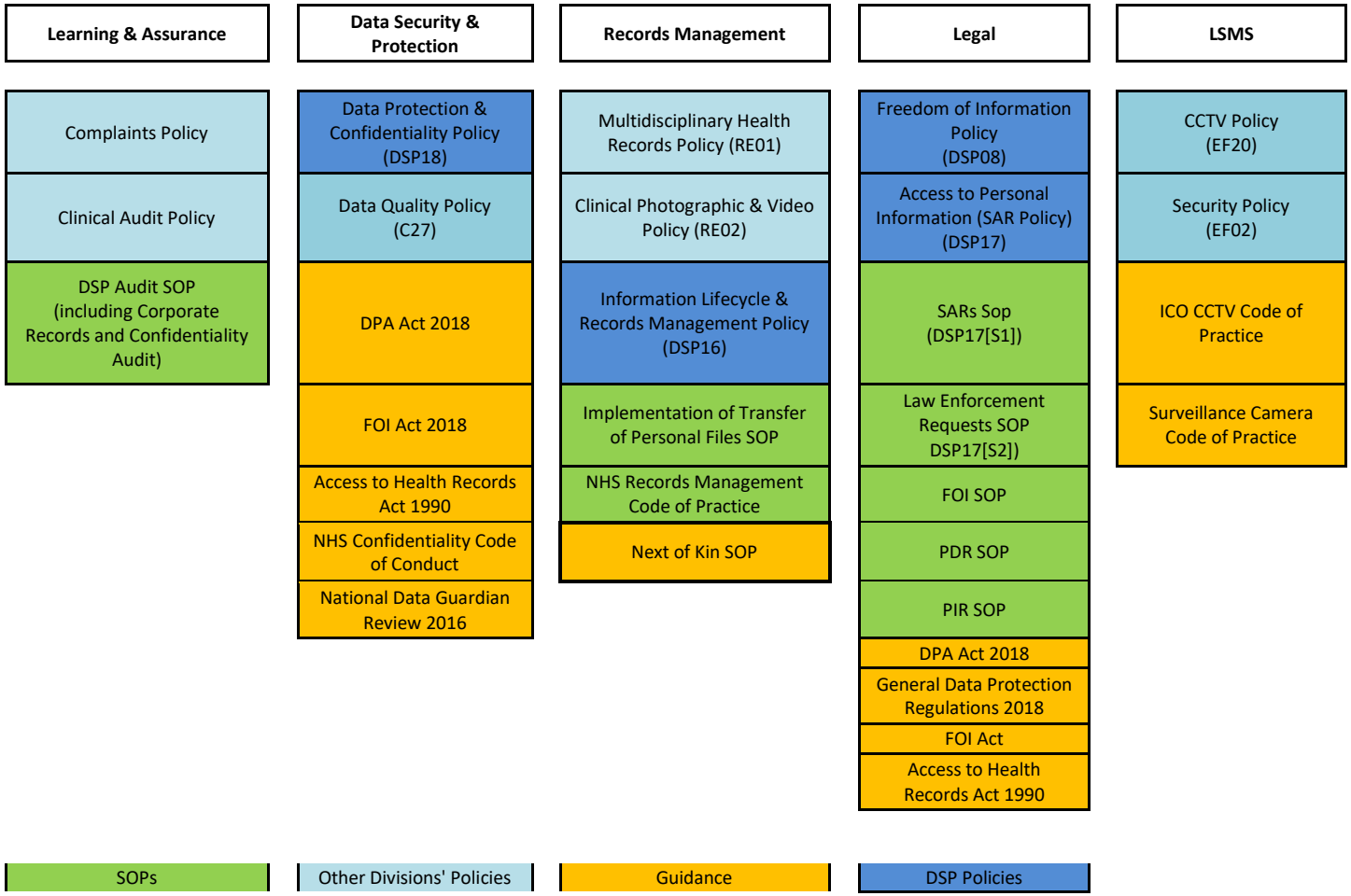
## 8. AUDITING AND MONITORING

This policy will be assessed against the NHS Digital information governance and security requirements (Data Security & Protection Toolkit) and alongside the DSP Governance Pack to assure the Trust that full DSP requirements are being met

### 8.1 Associated and Related Procedural Documents

Copies of the associated policies, process and guidance documents can be found on the Trust's Intranet (Policies page)

## Appendix 1


Learning & Assurance
Data Security & Protection
Records Management
Legal
LSMS
Complaints Policy
Clinical Audit Policy
DSP Audit SOP (including Corporate Records and Confidentiality Audit)
Data Protection & Confidentiality Policy (DSP18)
Data Quality Policy (C27)
DPA Act 2018
FOI Act 2018
Access to Health Records Act 1990
NHS Confidentiality Code of Conduct
National Data Guardian Review 2016
Multidisciplinary Health Records Policy (RE01)
Clinical Photographic & Video Policy (RE02)
Information Lifecycle & Records Management Policy (DSP16)
Implementation of Transfer of Personal Files SOP
NHS Records Management Code of Practice
Next of Kin SOP
Freedom of Information Policy (DSP08)
Access to Personal Information (SAR Policy) (DSP17)
SARs Sop (DSP17[S1])
Law Enforcement Requests SOP DSP17[S2])
FOI SOP
PDR SOP
PIR SOP
DPA Act 2018
General Data Protection Regulations 2018
FOI Act
Access to Health Records Act 1990
CCTV Policy (EF20)
Security Policy (EF02)
ICO CCTV Code of Practice
Surveillance Camera Code of Practice
SOPs
Other Divisions' Policies
Guidance
DSP Policies