NHS
Doncaster and Bassetlaw
Teaching Hospitals
NHS Foundation Trust

Information Records Management - Code of Practice

This procedural document supersedes: CORP/ICT 14 v.7 – Information Records Management – Code of Practice

Did you print this document yourself?

The Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version. **If, for exceptional reasons, you need to print a policy off, <u>it is only valid for 24 hours.</u>**

Executive Sponsor(s):	Sam Wilde, Chief Finance Officer
Name and title of author/reviewer: (this version)	Roy G Underwood, Data Protection Officer/ Head of Information Governance
Date revised:	August 2025
Approved by (Committee/Group:	Information Governance & Cyber Group
Date Approved:	27 October 2025
Date issued:	04 November 2025
Next review date:	April 2028 (Policy valid until October 2028)
Target audience:	Trust-wide

Amendment Form

Version	Date Issued	Brief Summary of Changes	Author
Version 8	Aug 2025	• Tri-Annual review • The Trust's Records Management Systems are now administered by the Information Governance **& Cyber** Group and the Clinical Records Committee	Data Protection Officer/Head of Information Governance
Version 7	Oct 2021	• Revised Records Management Guidance from NHSx • Amendments to the GDPR reference post-Brexit 2021	Data Protection Officer/Head of Information Governance
Version 6	21 July 2020	• Tri-Annual review, with changes to 'current data protection legislation', Records Management Guidance from NHS Digital, and future policy monitoring • Policy layout changed in accordance with guidance • Change references from Care Groups to Divisions	Data Protection Officer/Head of Information Governance
Version 5	1 April 2015	• Tri-Annual review, minor changes to Policy Monitoring • Policy layout changed in accordance with guidance • Change references from CSUs to Care Groups	Head of Information Governance
Version 4	May 2012	• Tri-Annual review • Changes to the Caldicott Guardian/SIRO responsibilities • CQC Outcome 21 referenced • Divisional Units changing to Clinical Service Units	Head of Information Governance
Version 3	October 2008/April 2009	• Bi-annual review → changing to Tri-Annual review • Re-organised to NHSLA Format • Changes to the Caldicott Guardian/SIRO responsibilities • Divisional changes and responsibilities including Information Asset Owners and Administrators (IAOs and IAAs) • The need for auditable Corporate Records Inventory and Management systems at all levels under the supervision of individual Divisions • Safe haven contact points for the labeling, dispatch and receipt of health records • Notice of 2008 review and update to the Part 2 CoP provided by the Department of Health • Changes to monitoring the effectiveness of the	Head of Information Governance

		policy - Amended reference to the laws which allow access to personal data	
Version 2	January 2007	- Bi-annual review - DoH has issued a revised Records Management: Code of Practice Parts 1 and 2 (RMCoP v1.0 170605) - Reference included to the Trust Policy: CORP/REC 8 – Policy for the Legal Retention and Destruction of Hospital Patient Records.	Head of Information Governance

Contents

Page No.

1. INTRODUCTION 5
2. DEFINITIONS 6
 2.1 Records 6
 2.2 Records Management 6
 2.3 Records Life Cycle 6
 2.4 Machine-Readable Records 6
3. IMPORTANCE OF GOOD RECORDS MANAGEMENT 6
4. RECORDS MANAGEMENT ORGANISATION 7
5. RESPONSIBILITIES 7
 5.1 Caldicott Guardian 7
 5.2 Governance Groups 7
 5.3 Divisional and Departmental General Managers 8
 5.4 Divisional and Departmental Information Records Managers 8
 5.5 Individual Members of Staff 8
6. RECORDS MANAGEMENT SYSTEMS 9
7. RECORDS MANAGEMENT PROCEDURES 9
 7.1 Records Creation 9
 7.2 Records Organisation 10
 7.3 Records Maintenance 10
 7.4 Records Use 10
 7.5 Records Retention and Disposal 10
8. TRAINING 11
9. EQUALITY IMPACT ASSESSMENT 11
10. MONITORING THE POLICY 11
11. DATA PROTECTION 12
APPENDIX 1 – EQUALITY IMPACT ASSESSMENT - PART 1 INITIAL SCREENING 13

1 INTRODUCTION

The Freedom of Information Act 2000 ("The Act") imposes certain obligations on public authorities, which for these purposes includes the Trust. It provides the public with wider rights of access to the Trust's records and also requires the Trust to implement and maintain a comprehensive Records Management system.

The Trust's Policy on Freedom of Information is that it will comply fully with the Act and will place in the public domain as much information about its activities as is practicable and, subject to the exemptions permitted under the Act, will make all other information available on request. In particular, the Trust will conform with the Lord Chancellor's Code of Practice on the Management of Records produced by the Department of Constitutional Affairs[1], and the Records Management Code of Practice for Health and Social Care 2016 which sets out what people working with or in NHS organisations in England need to do to manage records correctly.

The revised Records Management Code of Practice from NHSE is based on current legal requirements and professional best practice.

The Code of Practice sets out how long records should be retained, either due to their ongoing administrative value or as a result of statutory requirement.

This Code of Practice mainly provides guidance on the implementation of the records management aspects of the Trust's Freedom of Information Policy[2]. There is a parallel Code of Practice, which provides guidance on the handling of requests for information submitted under the Act. This Code of Practice covers all types of records held by the Trust. Medical Records and related confidential information held under the auspice of the UK General Data Protection Regulation 2021 (UK GDPR) and the Data Protection Act 2018[3], are also subject to the Trusts Records Management Policies & Procedures.

This policy aligns with the principles and guidance set out in ISO 15489 – Information and Documentation – Records Management, the international standard for records management. ISO 15489 provides a framework for the effective management of records throughout their lifecycle, from creation and capture to classification, storage, access, and eventual disposal.
This complements the Trust's obligations under the Freedom of Information Act 2000, UK GDPR 2021, and the Data Protection Act 2018, and is further supported by the Records Management Code of Practice for Health and Social Care 2016 and the NHSE Records Management Code of Practice.

[1] Government help with the Management of Records can be found at: Information management - The National Archives

[4] The Trust's Freedom of Information Policy and Procedures

[3] More commonly known as 'current data protection legislation'

2 DEFINITIONS

2.1 Records

"Records" means papers, minutes, diaries, maps, photographs, sound or video recordings, machine-readable records and electronic records - including e-mail - or other documentary material, regardless of physical form, created or received by the Trust and its staff in the normal course of Trust business. Such documents constitute (with a few exceptions such as those that are the subject of a separate agreement concerning the assignment of intellectual property rights between the Trust and an individual) Trust Records and remain its property.

2.2 Records Management

"Records Management" means activities involved in the management of information throughout its life cycle.

2.3 Records Life Cycle

"Records Life Cycle" means the life span of a record from creation to destruction, including information acquisition, creation, retention, storage, retrieval, communication, utilisation and eventual destruction.

2.4 Machine-Readable Records

"Machine-Readable Records" means electronic records, including e-mails. They meet the legal, operational and archival requirements of the Trust, support accountability, and are subject to the same legislation as paper records. Electronic records should be able to function as evidence of business activities and processes, with the same degree of confidence as paper records. They should be accessible and provide appropriate access within and between business processes and prevent unauthorised access. From the point at which an electronic document is filed as a record, it becomes part of the Trust's Corporate Records.

3 IMPORTANCE OF GOOD RECORDS MANAGEMENT

While it is essential that Doncaster & Bassetlaw Teaching Hospitals NHS Foundation Trust (DBTH) comply with the Act in implementing a Trust Information Records Management system, good record keeping practice is important in its own right. It helps to ensure that the administration of the Trust is efficient and effective because:

- It ensures that information can be found and that the process of doing so is quick and simple, which in turn saves staffs time and hence staff costs.
- It ensures that the Trust's operations are transparent and facilitates the auditing of the Trust's affairs.
- It protects the Trust's legal position by ensuring that important documents are retained and are easily accessible.

- By ensuring that records are not duplicated and are not held for longer than necessary, it reduces the requirement for storage space and equipment, thereby providing additional space for other use.
- By demonstrating that the Trust is administratively efficient it enhances the Trust's reputation.

4 RECORDS MANAGEMENT ORGANISATION

The Trust's Records Management Systems are administered by the Information Governance & Cyber Group and the Clinical Records Committee. These groups work closely with individual Divisions and Departments across the Trust to assist them in implementing this Code of Practice.

5 RESPONSIBILITIES

5.1 Caldicott Guardian

The Trust **Caldicott Guardian** (who is the Trust Medical Director) and the Trust **SIRO** (Senior Information Risk Owner) who is the Chief Information Officer (CIO) have overall responsibility to the Trust Board of Directors for the maintenance and use of this Code of Practice.

5.2 Governance Groups

Governance Groups[4] - The **Information Governance & Cyber Group** and **Clinical Records Committee** are generally responsible for policy and advise on the appropriate management and 'best practice' concerning:

- The Trust's centrally held corporate records and local public archives.
- The Trust's medical records libraries.
- The Trust's records management policies and procedures under review and ensuring that these comply with good practice in the NHS and other public sector organisations.
- Advice and assistance to the Trust's Caldicott Guardian on changes to the Trust's records management policies and procedures.
- The setting of consistent standards for records management practices across the Trust is in line with all relevant Data Security & Protection Toolkit (DSPT) Assertions. Detailed guidance can be found on the Information Governance page here: https://extranet.dbth.nhs.uk/digital-transformation/information-governance/ and on the Trust Website here: https://www.dbth.nhs.uk/about-us/our-publications/information-governance/
- The provision of appropriate assistance, advice and training to staff about efficient record-keeping practices.
- The rationalization and control of central space for the management of the Trust corporate records and advising on the enhancement of record keeping conditions in offices and storage areas.
- The Trust's Divisions and Directorates in responding to requests for information, including requests made under the Freedom of Information Act 2000.

[4] Care Quality Commission (CQC) Outcome 21: Records Management

5.3 Divisional and Departmental General Managers

Divisional and Departmental General Managers – are responsible for:

- Ensuring that they comply with these procedures and that local arrangements are in place to this end.
- Appointing Divisional & Departmental Information Records Managers.
- Providing appropriate space for the storage of Divisional/Departmental records.

5.4 Divisional and Departmental Information Records Managers

Divisional and Departmental Information Records Managers – (including IAOs and IAAs) are responsible for:

- Ensuring that these procedures are implemented across the Divisions and Departments and that they operate efficiently and effectively.
- Ensuring that these procedures are applied not only to paper records but also all other forms of record.
- Using systems such as the Trust Website/Intranet to publish, inventory and track their departmental records, including their destruction when necessary and appropriate.
- Ensuring that departmentally held records are disposed of in accordance with the retention schedules set out in Appendix A of this Code of Practice.
- Liaising with the Information Governance Group and the Freedom of Information Team.
- Informing the Information Governance Group of staff changes within their working areas to ensure that the records management databases are kept up to date.

5.5 Individual Members of Staff

Individual members of staff are responsible for:

- Ensuring that they are aware of their own responsibilities under the Freedom of Information Policy and its associated Codes of Practice.
- Keeping their work records, including those held electronically, in good order and accessible.
- Using the Trust Website to publish and track their work records.
- Filing and weeding records on a regular basis.
- Disposing of records in accordance with the retention schedules set out in the NHS Digital links to this Code of Practice.
- Liaising with the Departmental Information Records Manager as required.

6 RECORDS MANAGEMENT SYSTEMS

Trust's records management systems should include two main elements – (i) the recording and (ii) the storage of records. Taken together these cover the listing, accessibility and final disposition of all Trust records.

Proposals for a records management and retrieval database continue to be evaluated by the Information Governance and IT Teams.

It is proposed that there will be three stages in the storage requirements of a physical record. These are:

- ***Immediate***. Records that have recently been created, or are in current use, will normally be stored as close to the user as possible. In most cases these records will be stored in the user's own office. When no longer required for immediate use, some records may be destroyed, while others will be moved into short-term storage.

- ***Short-term***. When a record is no longer required for immediate use, it would normally be stored where it can be retrieved within 24 hours. It is the responsibility of Divisions and Directorates to identify suitable space for short-term storage of Departmental records. The Information Governance Group can provide advice on appropriate conditions for short-term storage.

- ***Long Term***. Most records that are no longer required for immediate or short-term use should be destroyed in accordance with either:

  - the Trust's Policy CORP/REC 8: Legal Retention and Destruction of Hospital Patient Records

  - and/or the Guidance[7] given by the NHSE's 'Records Management: Code of Practice'.

Records that the Trust is required to keep for longer periods, and in some cases in perpetuity, will either be moved to long-term storage or archived.

7 RECORDS MANAGEMENT PROCEDURES

7.1 Records Creation

- All new and significant 'records of interest to the Public' should have an appropriate entry made onto the Trust Website by the member of staff responsible for creating the record through their departmental FOI and/or Website lead. Some of these records or documents (usually created in .pdf format) may have been produced in conjunction with Communications & Engagement.

The 'Public Interest Test' and associated exemptions must always be considered before any record is placed onto the Trust's public website www.dbth.nhs.uk/. Please seek guidance from the Trust FOI Team[5] if you need help.

Local Policies, Procedures and Guidelines will not – for now – be made public, rather they will be managed through the new Trust Intranet however, they may still satisfy the requirements for release under the Public Interest Test provisions of the FOIA. Each request will be considered on its own merits.

This is essential if the Trust's Published Information Records are to be properly and lawfully managed.

[5] Freedom of Information Management is under the Director of Communications

7.2 Records Organisation

- Records must be organised consistently and comprehensively to ensure that they are accessible. It is essential that the filing systems[6] used by Divisions and Departments achieve this.

7.3 Records Maintenance

- Records must be kept up-to-date and maintained in good condition to ensure that they remain usable and do not deteriorate.
- Duplicate records and multiple versions of the same record should be kept to a minimum. In principle, there is only a requirement for a single, master copy of each record to be held by its creator. Ideally, where these records meet the 'public interest test', consideration should be given to their publication on the Trust Website.
- Confidential records must be kept secure. Hard copy records should be stored in locked cabinets or rooms. When properly authorised, confidential and/or contentious electronic records should be password-protected (a register of those data files and their passwords should be kept by Divisional and Departmental Management staff).

7.4 Records Use

- Care must be exercised in the handling of all records, and they should be returned to designated storage promptly after use.
- Where a record is loaned to another person, department or external organisation, this should be recorded so that the whereabouts of the record can be tracked.
- Health records should ideally leave and return to the trust through a 'safe haven'[7] contact point appropriately labeled and packaged. Their whereabouts should be held up to date on the iFIT Casenote Tracking System when applicable. Details of these safe haven considerations and sighting should be in line with the Trust Safe Haven policy e.g. in the interests of safe and prompt patient management
- Confidential records must be kept secure and should be handled and seen only by those persons authorised[8] to do so.

7.5 Records Retention and Disposal

- Records should not be retained any longer than is necessary for the efficient operation of the Trust[9].
- Records that are of sufficient and continuing administrative and/or historical value to the Trust will become the responsibility of the Board of Directors.
- Records that have outlived their administrative usefulness should be destroyed systematically in accordance with the retention schedules set out in this Code of Practice. For Health Records, you must always comply with the requirements of the Trust Policy: CORP/REC 8 – Policy for the Legal Retention and Destruction of Hospital Patient Records.

[6] UK GDPR 2021, Data Protection Act 2018, and the Freedom of Information Act 2000

[7] CORP/ICT 8: Safe Haven Guidelines

[8] Caldicott et al, 1997

[9] Records Management Code of Practice - NHS Transformation Directorate

- Under the Freedom of Information Act 2000, it is now a criminal offence to destroy or dispose of records once the Trust has received a formal request to access the information contained in those records.

8 TRAINING

Information Governance training is now **MANDATORY** for **ALL** Trust staff[10].

Staff - including Volunteers - must complete their SET Information Governance (IG) training at least annually, and this will be recorded on their ESR Training Record[11]:

Please note: The training requirements of staff will be identified through a learning needs analysis (LNA). Role specific education will be coordinated/delivered by the topic lead. Alternatively, training may be accessed via an approved e-learning platform where available.

9 EQUALITY IMPACT ASSESSMENT

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 disadvantaged over others. Our objectives and responsibilities relating to equality and diversity are outlined within our equality schemes. When considering the needs and assessing the impact of a procedural document, any discriminatory factors must be identified.

An Equality Impact Assessment (EIA) has been conducted on this procedural document in line with the principles of the Equality Analysis Policy (CORP/EMP 27), the Equality Diversity and Inclusion Policy (CORP/EMP 59) and the Civility, Respect and Resolution Policy (CORP/EMP 58).

The purpose of the EIA is to minimise and if possible, remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified. (See Appendix 1).

10 MONITORING THE POLICY

Monitoring the effectiveness and understanding of the policy will be facilitated by periodic Internal Audit review and testing of individual understanding within Information Governance Training and Staff Awareness 'Flyers'.

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
Ensuring that information can be found Ensuring that important documents are retained and are easily accessible. Ensuring that records are not duplicated and are not held for longer	The Trust Information Governance & Cyber Group	Twice yearly	To the IG&C Group in line with DSPT Toolkit standards

[10] Information Governance Policy: CORP/ICT 9

[11] Some staff, like Volunteers and Locums etc, may not have an ESR training record however, that does not mean that they are excluded from the same levels of training expected of 'employed staff' who have the same or similar access to the Trust's Confidential and Sensitive Information Assets

than necessary. Demonstrating that the Trust is administratively efficient.			

11 DATA PROTECTION

Any personal data processing associated with this policy will be carried out under ‘Current data protection legislation’ as in the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR) 2021.

For further information on data processing carried out by the trust, please refer to our Privacy Notices and other information which you can find on the trust website:
https://www.dbth.nhs.uk/about-us/our-publications/information-governance/

APPENDIX 1 – EQUALITY IMPACT ASSESSMENT - PART 1 INITIAL SCREENING

Policy	Executive Directorate	Assessor (s)	New or Existing Policy?	Date of Assessment
CORP/ICT 14 v.8	Digital Transformation Directorate	Roy Underwood	Existing Policy	Aug/Sept 2025

1) **Who is responsible for this policy?** Name of Division/Directorate: Digital Transformation Directorate

2) **Describe the purpose of the service / function / policy / project/ strategy?** To manage all Trust records in an organized and coherent way

3) **Are there any associated objectives?** Legislation, targets national expectation, standards? NHSE Code of Practice

4) **What factors contribute or detract from achieving intended outcomes?** Trust compliance

5) **Does the policy have an impact in terms of age, race, disability, gender, gender reassignment, sexual orientation, marriage/civil partnership, maternity/pregnancy and religion/belief?** NO

- **If yes, please describe current or planned activities to address the impact** [e.g. Monitoring, consultation]

6) **Is there any scope for new measures which would promote equality?** NO

7) **Are any of the following groups adversely affected by the policy?**

Protected Characteristics	Affected?	Impact
a) Age	No	
b) Disability	No	
c) Gender	No	
d) Gender Reassignment	No	
e) Marriage/Civil Partnership	No	
f) Maternity/Pregnancy	No	
g) Race	No	
h) Religion/Belief	No	
i) Sexual Orientation	No	

8) **Provide the Equality Rating of the service / function /policy / project / strategy – tick (✓) outcome box**

Outcome 1 ✓	**Outcome 2**	**Outcome 3**	**Outcome 4**

If you have rated the policy as having an outcome of 2, 3 or 4, it is necessary to carry out a detailed assessment and complete a* **Detailed Equality Analysis form in Appendix 4

Date for next review: July 2028

Checked by: David Linacre **Date:** September 2025