# Corporate Records Policy

## Document Information

This is a controlled document. It should not be altered in any way without the express permission of the author or their representative. On receipt of a new version, please destroy all previous versions.

| | | | |
|---|---|---|---|
| Date of Issue: | April 2026 | Next Review Date: | April 2027 |
| Version: | | Last Review Date: | April 2026 |
| Author: | Information Governance Officer | | |
| Director Responsible | Chief Executive Office | | |
| | | | |
| **Approval Route: Information Governance Steering Group** | | | |
| **Approved By:** | | **Date Approved:** | |
| Records Management Operational Group | | April 2026 (by exception) | |
| | | | |
| | | | |
| | | | |
| Links or overlaps with other policies: | | | |
| | | | |
| We are committed to preventing discrimination, valuing diversity and achieving equality of opportunity. No person (staff, patient or public) will receive less favourable treatment on the grounds of the nine protected characteristics (as governed by the Equality Act 2010): Sexual Orientation; Gender; Age; Gender Reassignment; Pregnancy and Maternity; Disability; Religion or Belief; Race; Marriage and Civil Partnership. In addition to these nine, the Trust will not discriminate on the grounds of domestic circumstances, social-economic status, political affiliation or trade union membership.<br><br>We are committed to ensuring all services, policies, projects and strategies undergo equality analysis. For more information about equality analysis and Equality Impact Assessments please refer to the Equality and Diversity Policy. | | | |

Amendment History

| Issue | Status | Date | Reason for Change | Authorised |
|---|---|---|---|---|
| 1 | Final | April 2026 | | Records Management Operational Group |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# 1 Introduction

1.1 This policy sets out the structure for the management of Torbay and South Devon NHS Foundation Trust's corporate records.

1.2 Documents and records are not the same. Records are created to provide information about what happened, what was decided, and how to do things. Records have strict compliance requirements regarding their retention, access, and destruction.

1.3 The records lifecycle, or the information lifecycle, is a term that describes a controlled regime in which information is managed from the point that it is created to the point that it is either destroyed or permanently preserved as being of historical or research interest.

1.4 Effective records management ensures that information is properly managed and is available whenever and wherever there is a need for that information.

1.5 A breach of this Policy may result in disciplinary proceedings.

# 2 Scope

2.1 All directorates and regions fall within the scope of this Policy. This includes staff who are employed on a permanent, fixed term or zero-hours basis, contractors, temporary staff, secondees and volunteers. It also covers non-executive directors and non-executive associate directors. We refer to the terms "Staff" within this Policy to cover all of these different types of staff.

2.2 Compliance with this Policy is mandatory and applies to all information, in all formats. It covers all stages within the information lifecycle, including creation / receipt, maintenance / use, document appraisal, records declaration, record appraisal, retention, and disposition.

2.3 There is a separate policy for management of information collected as part of a health or social care record. Please see the Health and Social Care Records Policies, procedures and guidance for more information.

2.4 This policy refers to all corporate information at all stages of the information lifecycle:

- Record creation
- Record classification and storage
- Record use
- Record sharing and reuse
- Record archival
- Record appraisal
- Record destruction

## 3 Definitions

3.1 The following terms are used in this Policy and have the meanings set out below:

- **Data Protection** - The protection of Personal Data and the actions we take to ensure that we comply with the law.
- **EIR** - The Environmental Information Regulations 2004
- **FOIA** - The Freedom of Information Act 2000
- **Health and Social Care records -** A health and social care record is any record created in the provision or administration of direct care to an individual. The information is most commonly recorded in electronic or paper format; however, some records are in a manual form or a mixture of both. Health records may include notes made during consultations, correspondence between health professionals such as referral and discharge letters, results of tests and their interpretation, X-ray films, videotapes, audiotapes photographs, and tissue samples taken for diagnostic purposes. They may also include reports written for third parties.
- **Information Asset Owners (IAOs)** - IAOs are senior individuals responsible for each identified information asset (e.g. dataset, database or ICT system) at the appropriate business level within the Trust.
- **Information Governance** - This is our overall strategy and framework we apply for managing information within our organisation. Good Information Governance supports our compliance with our Data Protection obligations.
- **Personal Data** - Any information relating to an identified or identifiable person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name or a number. This includes Pseudonymised Data. For the purposes of this Policy, this also includes all information relating to an identified or identifiable person who has died.
- **Pseudonymised Data** - Data which has had identifiers removed from it so that it is no longer possible to identify a specific person without the use of those identifiers or additional information, which is kept separately and is subject to technical and organisational controls.
- **Record** - Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of Trust activities.
- **Record Retention and Disposal Schedules** - The Records Retention and Disposal Schedule is available via the Trust's intranet and define the minimum retention periods adopted by the Trust.
- **Staff -** Staff who are employed on a permanent, or fixed term or zerohours basis, contractors, temporary staff, secondees and volunteers. It also covers non-executive directors and non-executive associate directors.
- **Subject Access Requests** - A request from individuals for access to the Personal Data we Process about them, including providing copies of it. We must comply with these requests generally within one month under UK GDPR.
- **UK GDPR** – UK GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with

regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

## 4 Legal and professional obligations relating to record keeping

4.1 As a public authority, the Trust is required to comply with various legal obligations which relate to the management of our Records including:

- The Public Records Act 1958
- The Access to Health Records Act 1990
- The Freedom of Information Act 2000
- The Inquiries Act 2005
- UK GDPR
- The Data Protection Act 2018
- The NHS Records Management Code of Practice
- The Code of Practice on the Management of Records issued under section 46 of
- the Freedom of Information Act 2000
- NHS Information Governance: Guidance on Legal and Professional Obligations
- ISO15489 (the International British Standard for Records Management).
- BS10008 Standards for Legal Admissibility

4.2 Staff may also have professional obligations imposed upon them by their professional registration, such as the General Medical Council and Nursing and Midwifery Council.

4.3 Records of the NHS and its predecessor bodies are subject to the Public Records Act 1958, which imposes a statutory duty of care directly upon all individuals who have direct responsibility for any such records.

4.4 The Inquiries Act 2005 provides a statutory public inquiry with powers to formally request any relevant information from any person or organisation.

4.4.1 At the time of writing there are two statutory public inquiries which have requested that large parts of the health and social care sector do not destroy any records that are, or may fall into the remit of the Inquiry:

- The Infected Blood Inquiry
- The COVID-19 Inquiry

4.4.2 **All records that are in scope of an inquiry as set out in its terms of reference must be retained.**

## 5. Responsibilities

### 5.1 Chief Executive Officer

5.1.1 The Chief Executive has the ultimate responsibility for compliance with all relevant Acts and guidance within the Trust. They have delegated the responsibility for bringing data

protection issues to the Board and the Caldicott Guardian.

### 5.2 SIRO

5.2.1 The SIRO has oversight of information risks within the organisation and will inform and advise the board on how to mitigate the risk in accordance with the organisation's risk appetite.

### 5.3 Data Protection Officer

5.3.1 The Data Protection Officer (DPO) is responsible for the following:

- Ensuring the Trust complies with all relevant Acts and Guidance in relation to Data Protection and access to information.
- Promoting Data Protection awareness throughout the Trust by providing written procedures / guidance that are widely disseminated and available to staff
- Co-ordinating the work of other staff with data protection responsibilities
- Ensuring patients and service users are provided with information on their rights under data protection legislation and how the information we collect is held, used, shared and stored
- Monitoring compliance with the Data Protection Act 2018, UK-GPDR and Freedom of Information legislation.
- Ensuring the effectiveness of procedures through the use of compliance checks/audits and ensures appropriate action is taken where non-compliance is identified
- Assisting with investigations into breaches of confidentiality or data loss.
- Co-ordinate, investigate and report incidents involving the breaching of person confidential data
- Maintaining the registration with the Information Commissioner for data handling activities
- Implement and maintain a process for handling Subject Access Requests including from patients, services users, and third parties, Solicitors, Courts and Police
- The role of DPO will have operational independence and reporting mechanisms to senior management and should be effectively embedded within the data protection documentation and procedures.

### 5.4 Information Asset Owners

5.4.1 Information Asset Owners are responsible for ensuring the identified information assets are appropriately managed and protected. Their role is to understand what information is held, what is added and removed, how information is moved and who has access and why.

5.4.2 They are responsible for managing access and any identified risks relating to the asset.

5.4.3 IAOs must provide assurance in relation to the asset they manage to the Data Protection Officer and SIRO upon request.

5.4.4 Information Asset Owners/Information Asset Administrators are responsible for making sure that all records are periodically and routinely reviewed to determine what can be

disposed of or destroyed in accordance with the NHS Records Management Code of Practice and TSDFT Retention and Disposal Schedule.

### 5.5 Service / Line Managers

5.5.1 Service / Line Managers may act as IAOs for information held at a departmental level.

5.5.2 Service / Line Managers may also be responsible for day-to-day management of information accessed and used within their department.

5.5.3 They will ensure that all staff in their department:

- Complete mandatory Records Management training as part of their Information Governance Training and keep this up to date on an annual basis
- Do not alter, deface, block, erase, destroy or conceal records
- Manage all records in accordance with this policy.

### 5.6 All Staff

5.6.1 Staff must complete the mandatory Records Management training as part of their Information Governance Training and keep this up to date on an annual basis.

5.6.2 Staff must not alter, deface, block, erase, destroy or conceal records with the intention of preventing disclosure under a request relating to the Freedom of Information Act 2000, Environmental Information Regulations 2004, the Inquiries Act 2005 or UK GDPR.

5.6.3 All staff must Manage records in accordance with this policy.

5.6.4 All Staff have a duty to undertake the appropriate records management training provided by the Trust and maintain the records they create and use in accordance with this document.

### 5.7 Information Governance

5.7.1 It is the responsibility of the Data Security and Protection Lead to lead and provide expert strategic, tactical and operational support on all matters relating to TSDFT for Corporate Records Management who will work with the Information Governance Steering Group to implement, monitor and review these guidelines.

5.7.2 The Trusts Information Governance Team will provide additional, advice and support to all staff in connection with the holding, obtaining, recording, using and storage of information.

5.7.3 The Information Governance Steering Group will be responsible for determining and implementing local retention and disposal guidelines including temporary extended periods of retention considering good practice both locally and nationally and any inquiry guidance.

## 6 Record naming

6.1 Record naming is an important process in records management, and it is essential that a unified approach is adopted within all areas to aid in the management of records.

6.2 Standard naming conventions should be adopted for all records created.

6.2.1 All titles should be meaningful and relevant. The following rules should be followed:

- Keep file names short, but comprehensible, using commonly recognised acronyms or abbreviations where appropriate.
- Order the elements in a file name in the most appropriate way to retrieve the record, with the most important element first
- Avoid repetition and redundancy: in particular, the title of a folder should not be repeated in the document title. This will aid efficient searching.
- If it is important that documents can be sorted by date, number or name, to ensure correct sort order, numbers below 10 should be given in two digits, dates in the form YYYYMMDD or YYMM.
- Avoid non-alphanumeric characters, such as ? ; : / \ < > * & $ £ + =. Hyphens may be used.
- Date, subject and author should be given if appropriate, e.g. for a letter or email
- When saving items such as digital photographs and scanned images, the title should be changed from the system-generated number to a something meaningful.
- A description of the application (e.g. PowerPoint, Access) should not be included in the document title - this is apparent from the document icon and extension.

## 7 Record maintenance

7.1 All documents and records (electronic and paper) should be maintained in accordance with this Policy.

7.2 Records should only ever be kept on approved Trust systems.

7.3 Staff are encouraged to save in electronic format wherever applicable. For corporate records which cannot be digitised and require off site storing, contact the Information Governance team for support and advice – tsdft.igteam@nhs.net

7.4 Paper file storage must be secured from unauthorised access and meet fire regulations. The movement and location of paper records must also be controlled and tracked end to end to ensure that a record can be easily retrieved at any time. This will enable the original record to be traced and located if required. The tracking history must be held in a shared location.

7.4.1 The Trust contracts a formal archive provider to ensure that paper records removed from the Trust are archived in accordance with the Trust's legal obligations.

7.4.2 Records should be stored in a secure location when not being used e.g. lockable filing cabinets, cupboards, rooms (locked and/or alarmed outside of normal working hours)

7.4.3 The accommodation should comply with health and safety requirements, have proper

environmental controls and adequate protection against fire, flood and theft.

7.5 Information Asset Owners should ensure they have a contingency or business continuity plan to provide protection for records which are vital to the continued functioning of the Trust's services.

7.6 Records and information must be captured, managed and preserved in an organised system that maintains its integrity and authenticity. Records management facilitates control over the volume of records produced through the use of disposal schedules, which detail the time period for which different types of record should be retained by an organisation.

7.7 Appropriate watermarks should be used to assure appropriate protection of records in draft formats.

7.8 Appropriate version control should be used to assure appropriate disclosure of records.

7.8.1 Draft versions of documents should have a .X reference number, for example version 0.1 for the first draft version and version 3.4 for the fourth draft of the 3rd version document.

7.8.2 Published versions of documents should have a full number reference, for example version 1.

7.9 Duplication should be avoided unless necessary. It should be clear who is responsible for retaining the master version of a Record and copies should be clearly marked as such to avoid confusion.

## 8 Record retention and appraisal

### 8.1 Record retention

8.1.1 All records should be retained for a minimum period as defined in the NHS Records Management Code of Practice, and TSDFT Retention and Destruction Schedule.

8.1.2 If the retention period detailed in the NHS Records Management Code of Practice and the TSDFT Retention and Destruction Schedule differ, the TSDFT Retention and Destruction Schedule should take precedence, and guidance should be sought from the Information Governance Team on tsdft.igteam@nhs.net

8.1.3 The recommended retention periods shown on NHS Records Management Code of Practice and TSDFT Retention and Disposal Schedule apply to the official or master copy of the Records. Any duplicates or local copies made for working purposes should be kept for as short a period as possible.

8.1.4 Some types of Records which may be created and kept locally are the responsibility of the local department but may be found under a different function on the retention schedule: for example, where recruitment / interview is carried out by departments, the department shall be responsible for ensuring the disposal of the Records relating to unsuccessful candidate. This type of Record is listed under Human Resources in the

retention schedule.

8.1.5 When a record has met the minimum retention period as determined by the NHS Records Management Code of Practice and TSDFT Retention and Destruction Schedule, an appraisal should be carried out to ensure that there is no reason that the record needs to be retained for a longer period of time.

8.1.6 Unless by exception, Corporate records should not be appraised at an individual level, but as a group to ensure that the appraisals are consistent.

### 8.2 Records appraisal

8.2.1 A record appraisal will have one of three outcomes:

a) Record held for ongoing use
b) Record transfer for archiving
c) Record disposal

8.2.2 There are several questions to consider when conducting records appraisal. These are:

- Is there a statutory requirement to retain these records (for example – a Public Inquiry)?
- Does the record contain information which has been, or is likely to be subject to litigation?
- Is the record a draft, to which the final document has not yet been issued?
- Is there a requirement to keep these records for an audit trail (for example - transaction history)?
- Does the record form core information as part of a larger document (for example a paper within a Board report)?
- Has the information been subject to a Freedom of Information request?
- Is the record of historical interest?

8.2.3 If the answer to any of the above questions is ‘Yes’ advice should be sought from the Information Governance Team on tsdft.igteam@nhs.net

8.2.4 If the answer to all of the above questions is ‘No’, the records may be considered for disposal.

### 8.3 Records held

8.3.1 Records may be held for continued use or within the Trust’s archives.

8.3.2 Any records held in the Trust’s archives must be appropriately inventoried. This will include:

- details of the nature of the record
- a unique box / reference number (barcoded boxes are available from the Medical Records Library)
- any data subjects who the records pertain to
- the original retention date
- the appraisal date

- the review date (for the records to be re-assessed)

### 8.4 Records transferred for archiving

8.4.1 Records selected for archival preservation and no longer in regular use should be transferred to a 'Place of Deposit'. This must be approved by The National Archives and have adequate storage and public access facilities. For more information contact the Information Governance Team.

8.4.2 The Information Governance Team will liaise with The National Archives as appropriate to assist in the preparation and transfer of any records to the Place of Deposit.

### 8.5 Records disposal

8.5.1 Disposal is the implementation of appraisal and review decisions, and the term should not be confused with destruction. A review decision may result in the destruction of Records but may also result in the transfer of custody of Records, or movement of Records from one system to another.

8.5.2 Records which have been appraised for disposal should be put to one side and clearly separated from records in active use.

8.5.3 A disposal request should be submitted to the Information Governance Team for approval at the Information Governance Steering Group or other delegated meeting.

8.5.4 Records that do not contain personal data or confidential material can be destroyed in a less secure manner (confidential waste bins).

8.5.5 Short-lived documents such as telephone messages, post its etc. do not need to be kept as Records. If they are business critical, they should be transferred to a more formal document which should be saved as a Record and stored and declared within a central records repository.

## 9. Records Destruction

### 9.1 Destruction of paper records

9.1.1 If as a result of appraisal, a decision is made to destroy or delete a record, there must be evidence of the decision, these are referred to as Certificates of Destruction.

9.1.1.1 If approval is given to destroy the records locally, a destruction certificate must be generated and submitted to the Information Governance Team on the completion of the destruction.

9.1.1.2 Certificates of Destruction must contain the following information to provide clear evidence that specific records have been destroyed:

- details of the nature of the record
- a unique box / reference number (barcoded boxes are available from the

Medical Records Library)

- the original retention date
- the appraisal date
- the destruction date
- A signature of who approved the destruction
- A signature of who enacted the destruction

9.1.2 Destruction of any corporate records must be approved the Data Protection Officer or delegated authority.

9.1.3 If the Trust has contracted a third-party supplier to destroy the records, a destruction certificate will be provided to the Information Governance Team on the completion of the destruction.

9.1.3.1 All contracted third-party destroyers of paper materials must be ISO15489-1:2016 accredited.

## 9.2 Destruction of digital records

9.2.1 Destruction of digital records is the permanent action of removing information before the point of restoration.

9.2.2 Destruction of digital records is more challenging as deletion may not equate the permanent destruction of information. Therefore, the Trust must be assured that all ISO standards regarding IT systems are in place to enable appropriate destruction of digital information.

9.2.2.1 ISO 27001:2022 Annex A 7.14 states that two approaches can be taken to ensure secure and permanent erasure of information on equipment:

- Equipment that holds storage media devices that contain information should be physically destroyed.
- Annex A 7.10 and Annex A 8.10 concerning Storage Media and Information Deletion ensure all data stored on equipment is erased, overwritten or destroyed in a manner that precludes retrieval by malicious parties.

9.2.3 Where a record that has reached its retention period and has been approved for destruction, then the record should be deleted if the system allows that function. A separate record should be kept of what record has been deleted. This will function as the certificate of destruction.

9.2.4 If a system doesn't allow permanent deletion, then all reasonable efforts must be made to remove the record from use. It should be marked in such a way that anyone accessing the record can recognise it as a dormant or archived record.

9.2.5 If deletion is not possible, the Information Governance Team should be altered to the system and a risk reported.

## Rapid Equality Impact Assessment *(for use when writing policies and procedures)*

| | | | |
|---|---|---|---|
| **Policy Title** (and number) | ***Corporate Records Policy*** | **Version and Date** | ***0.1*** |
| **Policy Author** | Information Governance Policy | | |

An equality impact assessment (EIA) is a process designed to ensure that a policy, project or scheme does not discriminate or disadvantage people. EIAs also improve and promote equality. Consider the nature and extent of the impact, not the number of people affected.

**EQUALITY ANALYSIS:** How well do people from protected groups fare in relation to the general population?
***PLEASE NOTE: Any 'Yes' answers may trigger a full EIA and must be referred to the equality leads below***

**Is it likely that the policy/procedure could treat people from protected groups less favorably than the general population? (see below)**

| | | | | | |
|---|---|---|---|---|---|
| Age | Yes ☐ No☒ | Disability | Yes ☐ No☒ | Sexual Orientation | Yes ☐ No☒ |
| Race | Yes ☐ No☒ | Gender | Yes ☐ No☒ | Religion/Belief (non) | Yes ☐ No☒ |
| Gender Reassignment | Yes ☐ No☐ | Pregnancy/ Maternity | Yes ☐ No☒ | Marriage/ Civil Partnership | Yes ☐ No☒ |

| | |
|---|---|
| **Is it likely that the policy/procedure could affect particular 'Inclusion Health' groups less favorably than the general population?** (substance misuse; teenage mums; carers[1]; travellers[2]; homeless[3]; convictions; social isolation[4]; refugees) | Yes ☐ No☒ |

**Please provide details for each protected group where you have indicated 'Yes'.**

**VISION AND VALUES:** Policies must aim to remove unintentional barriers and promote inclusion

| | |
|---|---|
| Is inclusive language[5] used throughout? | Yes ☒ No☐ |
| Are the services outlined in the policy/procedure fully accessible[6]? | Yes ☒ No☐ |
| Does the policy/procedure encourage individualised and person-centered care? | Yes ☒ No☐ |
| Could there be an adverse impact on an individual's independence or autonomy[7]? | Yes ☒ No☐ |

If 'Yes', how will you mitigate this risk to ensure fair and equal access?

**EXTERNAL FACTORS**

| | |
|---|---|
| **Is the policy/procedure a result of national legislation which cannot be modified in any way?** | Yes ☒ No☐ |

**What is the reason for writing this policy?** (Is it a result in a change of legislation/ national research?)

To facilitate a standardized approach to policy documents across the Trust

**Who was consulted when drafting this policy/procedure? What were the recommendations/suggestions?**

**ACTION PLAN:** Please list all actions identified to address any impacts

| **Action** | **Person responsible** | **Completion date** |
|---|---|---|
| | | |

**AUTHORISATION:**
By signing below, I confirm that the named person responsible above is aware of the actions assigned to them

| | | | |
|---|---|---|---|
| **Name of person completing the form** | | **Signature** | |
| **Validated by (line manager)** | | **Signature** | |

**Any issues Please contact Diversity & Inclusion Lead**
**For Torbay and South Devon NHS Trusts, please call 01803 656676 or email pfd.sdhct@nhs.net**

[1] Consider any additional needs of carers/ parents/ advocates etc, in addition to the service user
[2] Travellers may not be registered with a GP - consider how they may access/ be aware of services available to them
[3] Consider any provisions for those with no fixed abode, particularly relating to impact on discharge
[4] Consider how someone will be aware of (or access) a service if socially or geographically isolated
[5] Language must be relevant and appropriate, for example referring to partners, not husbands or wives
[6] Consider both physical access to services and how information/ communication in available in an accessible format
[7] Example: a telephone-based service may discriminate against people who are d/Deaf. Whilst someone may be able to act on their behalf, this does not promote independence or autonomy