

Records Management Policy

Once printed off, this is an uncontrolled document. Please check the Intranet for the most up to date copy

Version	8.0
Approved by	Caldicott & Information Governance Committee
Date approved	April 2021
Ratified by	Executive Management Committee
Date ratified	18th May 2021
Author	Information Governance Manager
Lead Director	Director of Finance acting as Senior Information Risk Owner
Name of Responsible individual/committee	Caldicott & Information Governance committee TPSG –
Consultation	Caldicott & Information Governance committee
BHT Document Reference	BHT Pol 125
Department Document Reference	IG0079
Date Issued	April 2021
Review Date	April 2024
Target Audience	All Trust Staff
Location	Swan Live Intranet Policies & Guidelines/Policies & Strategies/Freedom of Information & Records Management
Equality Impact Assessment	April 2021

DOCUMENT CONTROL

Approval and Authorisation

Completion of the following detail signifies the review and approval of this document, as minuted in the senior management group meeting shown.

Version	Authorising Group	Approver	Date
5.0	Trust Management Committee	Anne Chilcott	Nov 11
6.0	Executive Management Committee	Lorraine Pask	Jan 2016
6.1	Caldicott and Information Governance Committee	Lorraine Pask	June 2017
7.0	Executive Management Committee		July 2018
8.0	Executive Management Committee		June 2021

Change History

Version	Status	Reason for change	Author	Date
4.1	Draft	Formal Review – minor changes to references, minor wording changes and new sections 9- Records Management Guidance Documents and 11 – Monitoring of the Policy	Anne Chilcott	Sept 11
5.0	Approved	Caldicott & IG Committee Chairman's action	Anne Chilcott	October 11
5.0	Ratified	Trust Management Committee	Anne Chilcott	Nov 11
5.1	Draft	Informal annual review – New sub section 5.1 Classification marking for NHS Information, added new sub section 4.3, 4.4	Anne Chilcott	Nov 12
5.2	Draft	Formal review - New sub section 7.3 – '20 year rule'	Lorraine Pask	May 2015
	Approved	Caldicott and IG Committee	Lorraine Pask	Sept 2015
6.0	Approved	Trust Policy and Strategy Group Executive Management Committee	Lorraine Pask	Dec 2015 Jan 2016
6.1	Draft	Section 2.1 updated to include BS10008 standard regarding scanning of health records	Lorraine Pask	May 2017
6.1	Approved	Noted at the caldicott Committee	Lorraine Pask	June 2017
6.2	Draft	Formal review to incorporate requirements from GDPR Added new section 6.2 to 6.7 – responsibilities of individual creating a record	Lorraine Pask	March 2018
6.2	Approved	Caldicott and IG Committee		March 2018
6.2	Approved	TPSG		July 2018
7.1	Draft	Formal review – web links added under Document References. Reference to EU GDPR changed to UK GDPR following UK's exit from EU	Lorraine Pask	April 2021
7.1	Approved	Caldicott and IG Committee and via Chairman's action		April 2021
7.1	Approved	TPSG		May 2021

Document References

Ref #	Document title		
1	Department of Health & Social Care – Records Management Code of Practice for Health and Social Care 2016 Records Management Code of Practice for Health and Social Care 2016 - NHS Digital		Internet
2	Records Management Guidance		Intranet
3	How to Manage and organise shared Drives	IG0092	Intranet
4	Where to Store and How to Share Electronic documents [4]	IG0093	Intranet
5	Off-site Storage of Records Procedure	IG0094	Intranet
6	Health Records Management Policy	MR002	Intranet
7	Records Management Strategy	IG0080	Intranet
8	UK General Data Protection Regulation Guide to the UK General Data Protection Regulation (UK GDPR) ICO		Internet
9	Freedom of Information Policy	IG0097	Intranet
10	Data Protection Policy	IG0117	Intranet
11	Subject Access Request Policy	IG0104	Intranet

Contents

1. Introduction.....	1
2. Scope and Definitions.....	2
3. Aims of our Records Management System.....	3
4. Roles and Responsibilities.....	4
5. Legal and Professional Obligations	5
6. Registration of Record Collections.....	6
7. Retention, Transfer and Disposal Schedules	9
8. Records Management Systems Audit.....	10
9. Records Management Guidance Documents	10
10. Training	10
11. Monitoring.....	10
12. Review	11

1. Introduction

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

1.2 As a Public Authority subject to the Freedom of Information Act (FOIA) the Trust has a duty to follow the Code of Practice for Records Management published by the Lord Chancellor in accordance with section 46 of the FOIA. The code provides guidance to public authorities on keeping, managing and destroying records.

The Data Protection Act sets in law how personal and sensitive information may be processed and largely influences the way we handle care records. Further guidance on the confidentiality aspects of record keeping is provided in the NHS Confidentiality Code of Practice and the Trust Data Protection Policy.

The Records Management Code of Practice for Health and Social Care 2016 provides records management guidance for NHS and Social Care organisations based on current legal requirements and professional best practice. The Trust is committed to following the guidance issued in the code of practice and the procedures outlined in this policy are largely based on the guidance included in this Code of Practice.

1.3 The Trust's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the Trust and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways. Any information, whatever its medium, is considered public sector information and subject to the Re-use of Public Sector Information Regulations 2015 (RPSI). RPSI does not apply to information that would be exempt from disclosure under information access legislation, i.e. the UK General Data Protection Regulation (UK GDPR), the Freedom of Information Act (FOIA)

1.4 Good records management is a mandatory corporate function and the Trust is committed to its ongoing improvement. This policy has been adopted by the Trust Board and the organisational benefits from doing so 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.

1.5 This document sets out a framework within which the staff responsible for managing the Trust's records can develop specific policies and procedures to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.

1.6 This policy document should be read in conjunction with the Trust's Records Management Strategy which sets out how the policy requirements will be delivered.

2. Scope and Definitions

2.1 This policy relates to all clinical and non-clinical operational records held in any format by the Trust. These include:

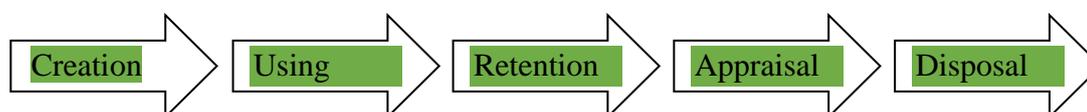
- all corporate/administrative records (e.g. personnel, estates, financial and accounting records, notes associated with complaints, client records, business accounting details and commercial correspondence through to supplier and partner emails)
- all patient health records (for all specialties and including private patients, including x-ray and imaging reports, emails, computerised records, microfiche, scanned records, text messages, registers, etc.)

This policy is mandatory and applies to all information in all formats. 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 or the UK GDPR and Data Protection Act 2018.

2.2 **Records Management** is a discipline which utilises an administrative system to direct and control the creation, version control, access, 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; this must be achieved in a standard, consistent way of applying templates to common sets of records,
- record keeping;
- record maintenance (including tracking of record movements);
- access and disclosure;
- closure and transfer;
- retention
- appraisal;
- archiving; and
- disposal.

2.3 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.



Stage 1: Creation

This part of the life cycle is when we put pen to paper, make an entry into a database or start a new electronic document. It is known as the first phase. It can be created by internal employees or received from an external source and it is complete and accurate.

Stage 2: Using

This stage takes place after information is distributed. This is when records are used on a day to day basis to help generate organisational decisions, document further action or support other Trust operations. It is also considered the Active Phase

Stage 3: Retention

Retention is when records are not used on a day to day basis and are stored in the Records Management system. Even though they are not used on a day to day basis, they will be kept for legal or financial reasons until they have met their retention period. The retention phase includes filing, transfers and retrievals. The information may be retrieved during this period to be used as a resource for reference or to aid in a business decision. Records should not be removed from a Records Management system; the information should be copied and tracked to ensure no amendments were made.

Stage 4: Appraisal

The appraisal stage is when a record has reached the end of its assigned retention period. It is then reviewed and if appropriate destroyed under confidential destruction conditions. Not all records will be destroyed once the retention period has been met. Any records that have historical value should be considered for removal to the designated Place of Deposit. For details of the agreed Place of Deposit, or further guidance if you are unsure whether your records have historical value can be sought from the Corporate Records Management Team.

Stage 5: Disposal

The disposal stage is when the appraisal phase has been completed and a documented agreement has been made that records can be confidentially destroyed. For medical records, this should be done in collaboration with the Head of Medical Records. For all records, the appraisal and destruction process should be recorded on a departmental records inventory and if applicable a destruction certificate produced to ensure there is a record of which documents have been sent for destruction.

- 2.4 In this policy, **Records** are defined as ‘recorded information, in any form, created or received and maintained by the Trust in the transaction of its business or conduct of affairs and kept as evidence of such activity’.
- 2.5 **Information** is a corporate asset. The Trust’s 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 Re-use of Public Sector Information Regulations 2015), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

3. Aims of our Records Management System

- 3.1 The aims of our Records Management System are to ensure that:
- **records are available when needed** - from which the Trust is able to form a reconstruction of activities or events that have taken place.
 - **records can be accessed** - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist;
 - **records - history** - the history of the record can be understood: who created or added to the record and when, during which business process, and how the record is related to other records;

- **records tracking** – systems are to be put in place to enable tracking and location of records;
- **records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;
- **records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;
- **records are secure** - from unauthorised or inadvertent alteration or erasure, access and disclosure are properly controlled and audit trails will track all use and changes. Records are held in a robust format which remains readable for as long as records are required;
- **records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- **staff are trained** - so that all staff are made aware of their responsibilities for record-keeping and record management.

4. Roles and Responsibilities

Trust Board

The Trust Board is ultimately responsible for ensuring that the Trust corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements. Included within its responsibilities to maintain minimum standards of information governance is a responsibility for ensuring the quality of record keeping and record management in the Trust.

Chief Executive

4.1 The Chief Executive has overall responsibility for records management in the Trust. As accountable officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate, accurate information is available as required.

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

4.3 Director for Records Management

The Senior Information Risk Owner is the Director for Records Management and has key individual empowerment to make operational decisions with clear responsibility for the management of all categories of records within the organisation, and corporate responsibility at a senior management level to the Trust Board for records management. The day to day management of records is devolved to Information Asset Owners (IAO) and local records managers.

4.4 Information Asset Owners (IAO)

The IAO is a nominated senior member of staff who has the responsibility and accountability for records management within his/her operational area and will provide an essential supporting role to the Senior Information Risk Owner. The IAO will oversee the records management function and delegate responsibility to appropriate individuals, adopt policies and procedures to guide personnel and ensure auditability.

4.5 Executive Management Committee

The Executive Management Committee is responsible for ensuring that this policy is implemented, through the Records Management Strategy, and that the records management system and processes are developed, co-ordinated, audited and monitored. Coordination of this work is the responsibility of the Senior Information Risk Owner.

4.6 Head of Medical Records

The Head of Medical Records is responsible for the overall development and maintenance of health records management practices throughout the Trust, in particular for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

4.7 Local record managers

The responsibility for local records management is devolved to the relevant directors, directorate managers and department managers. Heads of Departments, other units and business functions within the Trust have overall responsibility for the management of records generated by their activities, i.e. for ensuring that records controlled within their unit are managed in a way which meets the aims of the Trust's records management policies.

Senior Information Asset Owners are responsible for identifying local record managers within their areas of responsibility.

4.8 All Staff

All Trust staff, whether clinical or administrative, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work in the Trust and manage those records in keeping with this policy and with any guidance subsequently produced.

5. Legal and Professional Obligations

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
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality; and
- The NHS Confidentiality Code of Practice
- Information Security Management NHS Code of Practice
- Copyright, Designs and Patent Act 1988
- Re-use of Public Sector Information Regulations 2015
- UK General Data Protection Regulation

And any new legislation affecting records management as it arises.

Failure to comply with the regulations could result in reputational damage to the Trust and carries substantial financial penalties imposed by the Information Commissioner. This policy applies to all employees and must be strictly observed.

6. Registration of Record Collections

6.1 Senior Information Asset Owners or their designated deputies are to establish and maintain mechanisms through which departments can identify the records they are maintaining. This should be achieved through registers and an inventory of record collections which will facilitate:

- the classification of records into series; and
- the recording of the responsibility of individuals creating records.

The register should be regularly reviewed.

6.2 Version Control

Document version control allows the management of multiple revisions to the same document and is important as it enables users to distinguish between different versions of a document and to identify if the document they are using is the latest version. When creating a document where more than one version does, or is likely to exist, a unique version number should be included in the document name and clearly displayed in the document.

Consecutive whole numbers should be used to identify major revisions to documents. i.e. version 1, version 2 etc. The addition of the word Draft or Final at the end of the file name can be used to indicate the status of the document

e.g.Record v1.0 Draft First draft version
.....Record v1.1 Draft Second draft version
.....Record v2.0 Final Third and final version

In key documents (policies, strategies etc) it is useful to display after the title page a version control table showing the development history of the document and the version changes that have been applied.

6.3 Record Confidentiality and Access

All NHS records are public records and thus are subject to a number of statutory provisions regarding confidentiality, access and disclosure. Patients entrust the NHS or allow it to gather sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect this trust. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, confidential service.

Specific guidance on patient confidentiality issues is given in the Department of Health and Social Care publication 'Confidentiality: NHS Code of Practice'.

The Trust's Health Records Management Policy is built on the guidance contained within this overarching Records Management policy. The policy defines a structure and clinical records management guidance to promote and maintain effectively a consistent and standardised practice throughout the Trust.

The Data Protection Act 2018 and UK GDPR also make provision in law for patients to obtain copies or otherwise gain access to their health records. The Trust Subject Access Request policy covers this aspect of records management and advice on the procedure can be obtained from the Trust Medical Records department.

In 2000 the government introduced the Freedom of information Act providing members of the public with the general right of access to recorded information held by a wide range of bodies across the public sector. The effect of this legislation is to make it possible for people to obtain copies of a wide range of Trust records that in the past would have remained confidential. Staff need to be aware that the records they keep may well be released to the public at a future date and the increased importance of adhering to the guidance provided in the Trust Freedom of Information Policy.

6.4 **Non-Paper Records**

Increasingly our records are being created and recorded electronically and held in a digital format. The principles of sound record management apply equally to electronic records as they do to traditional paper records. Electronic records should be organised into secure filing systems and maintained, reviewed and archived or disposed of in line with the guidance in this document. When considering the use of alternative storage media, maintenance in the form of back up and planned migration to new platforms should be considered and discussed with the IT Department, and subsequently designed and scheduled to ensure continuing access to readable information.

In many cases copies of documents are distributed electronically and the original held in paper form. This often leads to duplicate records being unnecessarily retained, sometimes for periods beyond the recommended minimum retention period. This is particularly prevalent on file servers shared by several people/departments. Responsibility for the maintenance of such filing systems should be clearly defined and if appropriate restrictions placed on the ability to create new record folders.

E-mail has become a primary communication tool increasingly replacing letters and memoranda as a means of communicating and distributing information. The Trust has a separate policy on e-mail security and storage which users should be familiar with.

E-mail accounts should not be used to file records on a permanent basis but should be regarded as transient storage areas for working documents. Important e-mails or documents distributed by e-mail that need to be retained should be copied to the appropriate paper or electronic network file system and the e-mail copy destroyed as soon as practicable.

The increasing use of e-mail for personal communication can lead to business e-mails containing opinion and comment that may be inappropriate and would not have been included in more formal documents. Users should be aware that, if relevant, copies of e-mails held in the Trust will be released to requesters under the provisions of the Freedom of Information Act.

6.5 **Record Maintenance, Access and Disclosure**

All staff should ensure that Trust records are managed and maintained responsibly and respectfully, kept up to date and stored safely. The movement

and location of paper records should be controlled to ensure that a record can be easily retrieved at any time.

There are a range of statutory provisions that give individuals the right of access to information created or held by the trust such as Subject Access requests and Freedom of Information requests. In addition under the new data protection legislation, individuals are given enhanced information rights e.g. the right to rectification, right to erasure, right to restrict processing, right to data portability, right to object, and rights in relation to automated decision making and profiling. Good record management will enable the Trust to process and respond to information requests in a timely manner.

There are a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties and similarly a range of provisions that require or permit disclosure.

6.6 **Storage of Records**

When not required for operational purposes records should be kept in a secure storage area. Records in current use should ideally be stored close to the point of use while records no longer in current use can be transferred to secondary or archive storage more remote from the operational area.

Records should be stored in an appropriate environment to ensure they remain fit for purpose during their expected period of retention. When evaluating the suitability of a location for record storage the following points should be considered:

Environment. Is the location suitable for the type of material being stored? Is the area free from hazards that may cause the records to deteriorate or place at risk staff that may need to access the records? i.e. excessive dust, damp, restricted access.

Security. Is the level of security offered by the location acceptable for the type of record being stored?

Ease of Access. Can records be easily located and retrieved? Some restrictions on access may be acceptable for records that are not frequently recalled.

Layout. Consideration should be given to the design of the storage location to ensure the most cost-effective use is made of the space available.

A comprehensive record should be maintained of any records sent for commercial storage including a proposed date for review/destruction. A mechanism for reviewing these records for disposal should be developed and implemented to ensure records are not retained longer than necessary.

6.7 **Appraisal of Records**

The process of deciding what to do with records when their business use has ceased is called appraisal.

There will be one of three outcomes from appraisal:

- Destroy/delete
- To keep for a longer period
- To transfer to a place of deposit

Staff in the operational area that ordinarily uses the records will usually be able to decide whether to destroy or keep for a longer period. Operational managers

are responsible for making sure that all records are periodically and routinely reviewed to determine what can be disposed of or destroyed in the light of local and national guidance.

7. Retention, Transfer and Disposal Schedules

- 7.1 It is a fundamental requirement that all 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.
- 7.2 The Trust has adopted the retention periods set out in the Records Management Code of Practice for Health and Social Care 2016 which is available on the Internet (see Document Reference, Ref 1). It contains a comprehensive list of NHS clinical and corporate records and for each type of record sets out a recommended minimum period of retention along with advice on final disposal.
- 7.3 Place of Deposit - 20 year rule – As required by the Public Records Act 1958, and following implementation of the Constitutional Reform and Governance Act 2010, in particular Part 6: Public Records and Freedom of Information, central government departments and certain other public bodies including NHS, need to identify non-active records of historical value and transfer them for permanent preservation to National Archives or to another appointed Place of Deposit (PoD) by the time they are 20 years old. This rule applies to NHS also but is applicable only to 'corporate records' – records (other than health records) that are of, or relate to an organisation's business activities covering all the functions, processes, activities and transactions of the organisation and of its employees.

Records must be selected in accordance with the guidance contained within the Records Management Code of Practice for Health & Social Care 2016 and any supplementary guidance issued by the National Archives or local guidance from the relevant PoD. A documented list of any records being transferred to a PoD must be kept and a copy sent to the Information Governance department.

Once the appropriate minimum period has expired, the need to retain records further for local use should be reviewed periodically. Because of the sensitive and confidential nature of such records and the need to ensure that decisions on retention balance the interests of professional staff, including any research in which they are or may be engaged, and the resources available for storage, it is recommended that the views of the professional staff should be sought.

The overall responsibility for managing the process for the retention, disposal and destruction of patient health records lies with the Trust Clinical Records Manager. For further details please contact the Medical Records Department.

Records should not be kept longer than is necessary and should be disposed of at the right time. Unnecessary retention of records not only consumes time, space and equipment use but may also incur liabilities in respect of the Freedom of Information Act 2000 and the Data Protection Law, as we would be liable to disclose it upon request.

8. Records Management Systems Audit

8.1 The Trust will audit its records management practices for compliance with this framework.

8.2 The audit will:

- Identify areas of operational or information management /security risk
- Highlight where non-conformance to the procedures is occurring to enable tightening of controls and adjustment to related procedures.

8.3 The results of audits will be reported to the Caldicott & Information Governance and Committee.

9. Records Management Guidance Documents

The Trust has provided a number of guidance documents for staff in order to assist in day to day records management duties:

- Records Management Guidance ref [2]
- IG0092 How to Manage and organise shared Drives ref [3]
- IG0093 Where to Store and How to Share Electronic documents ref [4]
- IG0094 Off-site Storage of Records Procedure ref [5]
- MR002 Health Records Management Policy ref [6]
- IG0080 Records Management Strategy ref [7]

10. Training

10.1 All Trust staff will be made aware of their responsibilities for record-keeping and record management through generic and specific training programmes and guidance.

11. Monitoring

Minimum requirement to be monitored	Process for monitoring e.g. audit	Responsible individual to undertake monitoring and production of a report	Frequency of monitoring/ auditing	Responsible individuals receiving the monitoring report and for development of action plan	Responsible committee for review of action plan	Responsible committee for monitoring of action and audit to ensure satisfactory conclusion
Ensuring that Trust records are managed, stored, archived and destroyed in line with the Records Management NHS Code of Practice	Data Security and Protection Toolkit (DSPT) expected standards Information Commissioner's Office guidance	Information Asset Owners (IAO) or Information Asset Administrators	Annually	Senior Information Risk Owner	Caldicott and IG Committee	Caldicott and IG Committee
A continual, systematic approach to responding to Subject Access, FOI requests and the Trust Publication Scheme in line with the DSP standards	DSPT expected standards Report to Caldicott and IG Committee	Information Asset Owners or Information Asset Administrators	Annually Quarterly	Divisional Head/IAO	Caldicott and IG Committee	EMC Caldicott and IG Committee

Records Management Policy

Process for managing records audits and the production of a Trust wide Information Asset Register and Publication Scheme	DSP Toolkit Compliance audit by IG Team	Senior Information Risk Owner and Information Asset Owners	Annually Quarterly	IAO	Caldicott and IG Committee	EMC Caldicott and IG Committee
--	--	--	---------------------------	-----	----------------------------	---------------------------------------

12. Review

12.1 This document should be subject to review when any of the following conditions are met:

- a. The adoption of the Code of Conduct highlights errors and omissions in its content
- b. Where other standards/guidance issued by the Trust or Government legislation conflict with the information contained
- c. Where the knowledgebase regarding interpretation of the legislation evolves to the extent that revision would bring about improvement
- d. Three years from the date of approval of the current version