The
Disabilities Trust
www.thedtgroup.org

Records Management Policy and Retention Schedule

Document type:	Policy
Version:	1.1
Author (Role):	Data Protection Officer
Consulted:	IGA, Teamworks Consultants, Fundraising, Finance, HR
Date	June 18
Validated by:	Policy Review Group
Date Validated:	20.07.2018
Ratified by:	Corporate Integrated Governance (CIG)
Date ratified:	10.10.2018
Name of responsible committee or individual:	Governance and Quality Assurance Director
Name of executive / specialist lead:	Data Protection Officer
Master Document Controller:	Senior Governance Administrator
Date uploaded to Hub:	12.10.2018
Review Date:	20.07.2021

Version Control

Version	Type of change	Date	Revisions from previous version
0.1	New policy to reflect GDPR and Data Security and Protection Toolkit requirements	June 2018	
0.2		June 2018	Removal of Forensic Readiness which is a requirement of HMG SPF and not applicable to DT

1.0	Ratified	October 2018	
1.1	Amendment	March 2020	Addition to the Retention Schedule of Education Records.

Associated Documentation:

- Health Record-Keeping Standards Guideline
- Information Governance Policy
- Data Protection Policy and Associated Procedures
- Information Security Policy
- Website Policy

Section	Contents	Page
	Staff Summary	4
1	Introduction	4
2	Purpose/Scope	5
3	Process ▪ Legal Obligations ▪ Records Creation, Capture, Maintenance and Quality ▪ Records Use - Control, Tracking, Security and Storage ▪ Records Access, Retrieval and Disclosure ▪ Records Retention, ▪ Records Appraisal ▪ Records Disposal, Archiving and Transfer ▪ Digital Records, Digital Continuity and Digital Preservation ▪ Dealing with specific records	6
4	Records Access, Retrieval and Disclosure	15
5	Dealing with specific records	18
6	Training Expectations of Staff	19
7	Implementation Plan	19
8	Monitoring Compliance with this Policy	19
9	References	19
10	Appendices	
A	Definitions	21
B	Roles & Responsibilities	22
C	Retention Periods for each Record Type	25
D	Process Flow Step by Step Guide to Creating Clinical Records	48
E	Process Flow Step by Step Guide to Creating Corporate Records	49
F	Process Flow for Tracking Records	50
G	Process Flow for Retrieving Archived Paper Records in Storage	51
H	Process Flow for Retaining Records	52
I	Process Flow Step by Step Guide to Disposing of Records	53

Staff Summary

The key points for all staff to understand and adhere to in respect of this policy are:

- The use of standardised file names and version control methods should be applied consistently throughout all record lifecycles.
- File records in a logical manner to aid future retrieval and avoid making unnecessary duplications to help reduce the risk of data being lost, or unlawfully disclosed.
- Where possible avoid printing copies of records.
- Paper records that are sensitive or hold confidential information should be placed in a secure storage area when not in use.
- Electronic records must be protected at all times from unauthorised disclosure, access and corruption. All electronic corporate/business records should be stored on shared drives or servers, which are regularly backed up.
- No record should be destroyed until the retention period for that particular record type has expired.
- Records believed to be ready for destruction should be documented onto the form "Authorisation for the Destruction of Records", a copy of which can be found on the Hub. The relevant Director / Assistant Director must authorise the destruction.
- All staff are personally responsible for making themselves aware of and complying with this policy.

1.0 Introduction

1.1 Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format (paper or digital) or media type (see 1.3 below), from their creation, all the way through their lifecycle to their disposal or permanent archive.

1.2 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 service users, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways. Records are required for a number of reasons and are essential to the organisation. Some examples of why records are needed are detailed below:

- To support service user care and continuity of care
- To support the day to day business and the delivery of care
- To support evidence based clinical practice
- To support sound administrative and managerial decision making, as part of the knowledge base for NHS related services
- To meet legal requirements, including requests from service users under subject access provisions of the General Data Protection Regulations, and the Data Protection Act

- To assist clinical and other types of audits
- To support improvements in clinical effectiveness through research and also to support archival functions by taking account of the historical importance of material and the needs of future research
- To support choice and control over treatment and services designed around service users.

1.3 Examples of types of record and media covered by this policy include:

- Service user clinical records (electronic or paper based)
- Integrated health and social care records
- Data processed for secondary use purposes. Secondary use is any use of person level or aggregate level data that is for direct care purposes. This can include data for service management, research or support for commissioning.
- Corporate records (such as HR, estates, financial, complaint-handling)
- Photographs, slides and other images
- Microform (i.e. microfiche/microfilm)
- Audio and video tapes, cassettes, CD-ROM etc
- E-mails
- Staff diaries
- Computerised records
- Scanned records
- SMS text messages (both outgoing from the Trust and incoming responses)
- Computer database outputs, disks and all other electronic records
- Material intended for short term or transitory use, including notes and copies of documents.
- Websites and intranets sites that provide key information for service users and staff.

1.4 The Trust 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 digital space
- clear standards for record keeping, tracking and destruction
- better use of staff time and more efficient workflows
- improved control, access, and retrieval of valuable information assets
- compliance with legislation and professional standards
- reduced business costs resulting from poor records management
- reduced volume of lost or duplicated information
- a better understanding of the types of records held
- an informed and educated workforce, able effectively to carry out records management responsibilities.

2.0 Purpose/Scope

2.1 The purpose of this policy is to provide clear guidance to all staff in the handling and management of all records both corporate and clinical, regardless of the media on which they are stored. Additionally, this policy sets out a framework within which staff responsible for managing the Trust's records can develop specific local procedures to ensure that records are managed and controlled effectively commensurate with legal, operational and information needs.

2.2 This policy supports at a local level the legal and best practice requirements set out with the Records Management Code of Practice for Health and Social Care 2016 for those who work within or under contract to NHS organisations in England, based on current legal requirements and professional best practice. This has been published by the Information Governance Alliance (Department of Health, NHS England, NHS Digital, and Public Health England).

2.3 **All staff are personally responsible for making themselves aware of and complying with this policy.**

3.0 Process

3.1 Legal and Regulatory Obligations

3.1.1 All NHS related 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 Code of Practice for Health and Social Care 2016, in particular:

- The Public Records Acts 1958 and 1967
- General Data Protection Regulations 2016
- Data Protection Act 2018
- The Freedom of Information Act 2000
- Lord Chancellor's Code of Practice on the Management of Records issued under section 46 of the Freedom of Information Act 2000 which directs public organisations to have records management systems which will help them perform their statutory function
- The Common Law Duty of Confidentiality
- The NHS Confidentiality Code of Practice

and any new legislation affecting records management as it arises.

3.1.2 All records (manual or electronic) containing personal data are covered by the General Data Protection Regulations 2016 and the Data Protection Act 2018 and consequently the provisions of the Act apply to all of the Trust's records containing person identifiable information including service user records and staff identifiable records.

3.1.3 For most health and social care professionals, there are relevant codes of practice issued by the registration bodies and membership organisations of staff. That guidance is designed to guard against professional misconduct and to provide high quality care in line with the professional bodies.

3.2 Records Creation, Capture, Maintenance and Quality

3.2.1 Record Creation

When creating information in the first instance, these principles apply:

- ***Available when needed*** - to enable a reconstruction of activities or events that have taken place.
- ***Accessible to all members of staff that require access in order to enable them to carry out their day to day work*** - the information must be located and displayed in a way consistent with its initial use and that the current version is clearly identified where multiple versions exist.
- ***Interpretable, clear and concise*** - the context of the information must be clear and be able to be interpreted appropriately, i.e. who created or added to the record and when, during which business process and how the record is related to other records. This is especially important for managing emails.[1]
- ***Trusted, accurate and relevant*** - the information must reliably represent the initial data that was actually used in, or created by, the business process whilst maintaining its integrity. The authenticity must be demonstrable and the content relevant.
- ***Secure*** - the information must be secure from unauthorised or inadvertent alteration or erasure. Access and disclosure must be properly controlled and audit trails used to track all use and changes. The information must be held in a robust format which remains readable for as long as the information is required or retained.

Employees should also consider the following when creating information for the first time:

- What is being recorded and how it should be recorded
- Why is it being recorded
- How to validate the information (and against what) in order to ensure that what is being recorded is the correct data
- How to identify errors and how to report errors and correct them accordingly
- The intended use of the information, understand what the records are used for (and therefore why timeliness, accuracy and completeness of recording is so important)
- How to update the information and how to add in information from other sources

[1] Email fixes information in time and assigns an action to an individual, which are two of the most important characteristics of an authentic record. However, a common problem with email is that it is rarely saved in the business context, which is the third characteristic to achieve an authentic record. The correct place to store email is in the record keeping system of the activity to which it relates. If an email is declared as a record, or as a component of a record, the entire email must be kept including attachments so the record remains integral, e.g., an email approving a business case must be saved with the business case file.

A step by step guide to creating clinical records can be found in Appendix D and a step by step guide to creating corporate records can be found in Appendix E.

3.2.2 Record Capture

For reasons of business efficiency or, in order to address problems with storage, consideration should be given to the option of scanning paper format records into electronic format. Where this is proposed, the factors to be taken into account include the:

- Costs of the initial (and any later) media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept.
- Need to consult in advance with the local Place of Deposit or The National Archives with regard to records which may have archival value, as the value may include the format in which it was created.
- Need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the 'BS 10008 Electronic Information Management – Ensuring the authenticity and integrity of electronic information'.
- In order to fully realise the benefits of reduced storage requirements and business efficiency, the Information Asset Owners (IAOs) should dispose of any paper records that have been copied into electronic format and stored in accordance with appropriate standards. Where the record constitutes confidential information it must be securely destroyed.

3.2.3 Record Maintenance

All information needs to be maintainable through time. The qualities of availability, accessibility, interpretation and trustworthiness must be maintained for as long as the information is needed (perhaps permanently) despite changes in the format.

3.2.4 Quality

All staff must ensure that high standards of data quality are applied at every phase of the records lifecycle.

3.3 Records Use - Control, Tracking, Security and Storage

3.3.1 Record Control

The use of standardised file names and version control methods should be applied consistently throughout all record lifecycles. Please refer to the table below for guidance on how to version control a document from the point of its creation, on-going maintenance and throughout its use.

How to Version Control a Document

Stage	Version Number	Filename
Initial creation	0.1	APolicyDocument_v0.1 - draft

Second draft to include some feedback	0.2	APolicyDocument_v0.2 - draft
Third draft to include changes from stakeholders	0.3	APolicyDocument_v0.3 - draft
All changes included, ready for approval	0.4	APolicyDocument_v0.4 - draft
Approved version – now ready for release	1.0	APolicyDocument_v1.0 - FINAL
DOCUMENT PUBLISHED AND RELEASED	**1.0**	APolicyDocument_v**1.0** - **FINAL**
Review now due		
Make amendments on the draft as applicable	1.1	APolicyDocument_v1.1 - draft
Incorporate feedback from stakeholders	1.2	APolicyDocument_v1.2 - draft
Issue for approval	1.3	APolicyDocument_v1.3 - draft
Incorporate feedback from the approvers	1.4	APolicyDocument_v1.4 - draft
Re-issue for final approval	1.5	APolicyDocument_v1.5 - draft
Approved version – now ready for release	2.0	APolicyDocument_v2.0 - FINAL
DOCUMENT RE-PUBLISHED AND RE-RELEASED	**2.0**	APolicyDocument_v**2.0** - **FINAL**

Where possible all staff must avoid duplication and printing copies of records. This increases risks of breaches of confidentiality and needlessly increases administrative and paper costs for the Trust. Where the creation of copies is unavoidable, they must be destroyed as soon as they are no longer required.

3.3.2 Record Tracking

Version Number	**Date of Change**	**Time of Change**	**Full Name**	**Reason for / Type of Change**
1.0	31/01/2010	14.30	John Smith	To include staff mobile contact numbers.
1.1	28/02/2010	10.00	Joanne Smith	Add additional data to include full postal address.

Example of a Manual Audit Trail for Electronic and/or Paper Records

The process flow for tracking both electronic and paper based records can be found in Appendix F.

3.3.3 Tracking Electronic Records

The tracking of electronic records is held automatically in the audit trails of the systems that hold the data. Where this type of audit trail does not exist for some systems, staff must enter a manual audit trail in the record itself that details the full name of the person to last update the record and the date and time the amendment was carried out (please refer to the example above).

Depending on the nature of the record, this level of detail may not always be applicable, however best practice is to ensure version control is always applied as a minimum. If a particular record cannot be version controlled, has no automatic system audit trail and a manual audit trail cannot be easily applied directly to the record itself, consideration should be given to a separate document that details the audit of amendments to that particular record.

Records should be closed (i.e. made inactive and transferred to a secondary storage) as soon as they have ceased to be in active use other than for reference purposes. An indication that a file of paper records, or folder of electronic records, has been closed, together with the date of closure, should be shown on the record itself, as well as noted in the index, manual audit trail or database of the files/folders.

Where possible, information on the intended disposal of electronic records is included in the metadata when the information is created. The storage of closed records follows accepted standards relating to environment, security and physical organisation of the files. This is handled by the Trust’s third party storage contractor which is used for archiving closed paper records and also the secure destruction of the records once the relevant retention period has expired.

The above table can be less detailed where applicable, for example the time of the change may only be required if a particular record is being updated numerous times during the same working day. Likewise additional columns can be added if further details about the type of change are required. The above manual audit trail can be used for both electronic and paper records.

3.3.4 Tracking Paper Records

Paper records do not have the facility of an automatic audit trail that electronic systems offer and so staff must enter a manual audit trail in the record itself that details the full name of the person to last update the record and the date and time the amendment was carried out (please refer to the example above). Depending on the nature of the record, this level of detail may not always be applicable, however best practice is to ensure version control is always applied as a minimum. If a particular record cannot be version controlled and a manual audit trail cannot be easily applied directly to the record itself, consideration should be given to a separate document that details the audit of amendments to that particular record.

Whilst the Trust is continually making changes to help reduce the amount of paper records produced in the first instance and to also convert some existing paper based records into electronic format using scanning, there is always likely to be the need for some paper based records within the Trust. In the first instance, staff must always look for alternative methods of creating, storing and maintaining records that do not involve the paper based means being the primary source. However, where a suitable electronic alternative is not readily available, staff must always seek to be as efficient as possible, file records in a logical manner to aid future retrieval and avoid making unnecessary duplications to help reduce the risk of data being lost, or unlawfully disclosed.

Staff must apply clear version control as described in section 3.3.1 and manual audit trail in the record itself, as described in the table above.

3.3.6 Record Security and Storage

The security of all Trust records is critical, as records provide evidence of business transactions, support management decisions and ensure public accountability requirements are met. Records in all formats should be stored securely to prevent unauthorised access, destruction, alteration or removal. Trust staff are responsible for the safe custody of all files and documents.

No paper records can be taken off Trust premises, e.g., home, except for a temporary period (i.e., overnight or at most a weekend) where a member of staff's travel to a meeting requires this. In all cases, only the minimum number of records relevant to that meeting is permitted. The member of staff must ensure the safe storage of those records whilst in their personal possession. The records must be returned to Trust premises by the next working day.

Paper records that are sensitive or hold confidential information should be placed in a secure storage area when not in use. Paper records must be stored in secure and preferably alarmed facilities with strict access controls in place. Electronic records must be protected at all times from unauthorised disclosure, access and corruption.

Storage of records in offices must conform to all current relevant legislation and guidance regarding Health and Safety, namely the Health & Safety at Work Act 1974 and Workplace (Health, Safety and Welfare) Regulations 1992. Records held in offices are generally those that are in current use with cupboards and convenient storage areas utilised to store any archived records. These records must be securely stored to prevent theft or unauthorised access.

Offsite storage areas must conform to all current relevant legislation and guidance regarding Health and Safety, namely the Health & Safety at Work Act 1974 and Workplace (Health, Safety and Welfare) Regulations 1992. The Trust has a contract with external suppliers to provide secure storage of records. All records stored off site must still comply with retention periods.

The Trust follows the protective marking scheme for service user information as being ‘NHS Confidential’, which corresponds to the classification of “Official Sensitive” under the Cabinet Office Government Security Classifications (2014).

3.5 Records Retention, Appraisal and Disposal

3.5.1 Records Retention

The table in Appendix C details the minimum retention period for each type of record[2]. Records (whatever the media) may be retained for longer than the minimum period, however, records should not ordinarily be retained for more than 30 years (this excludes a number of Human Resources record types, which should be retained until the individual's 70th birthday or until 6 years after cessation of employment if aged over 70 years at the time). The National Archives should be consulted where a longer retention period than 30 years is required, or for any records that pre date 1948.

The retention period varies dependent on the type of information being stored, clinical records should not ordinarily be retained for more than 30 years. The information being recorded and retained must be relevant, fit for the purpose it was intended and only retained for as long as it is genuinely required.

Please refer to the process flow for Retaining Records which can be found in Appendix I. Refer to Appendix C for the table detailing the retention periods for each record type.

3.6 Records Appraisal

The process of deciding what to do with records when their business use has ceased is called appraisal. The three outcomes of appraisal are: destroy/delete (see 3.5.3 below); keep for a longer period (see 3.5.1 above) or transfer to a place of deposit appointed under the Public Records Act 1958 (see 3.6 below).

3.7 Records Disposal

Disposal is defined as the point in the records lifecycle when it is either transferred to an archive, or securely destroyed. It is particularly important under the Freedom of Information legislation that the disposal of records is undertaken in accordance with this policy and in accordance with the retention requirements of any local and national inquiries such as the Independent Inquiry into Child Sex Abuse (IICSA) which has requested large parts of the Health and Social Care sector do not destroy any records that are, or may fail into, the remit of the inquiry. This includes children's records and any instances of allegations or investigations or any records of an institution where abuse has, or may have, occurred. Local guidance should be followed in relation to record retention instructions issued by inquiries.

No record should be destroyed until the retention period for that particular record type has expired. The retention periods for the most frequently used record types are listed in the table in Appendix C.

[2] The table does not contain all record types, only those records that are used or referred to most frequently in the organisation have been extracted for guidance. If information is required regarding another type of record, not listed in the table, please refer to the Records Management Code of Practice for Health and Social Care 2016 at: https://digital.nhs.uk/article/402/Information-Governance

Records believed to be ready for destruction should be documented onto the form “**Authorisation for the Destruction of Records**”.

Once all the details of the records that need destroying have been listed, the relevant Director / Assistant Director must authorise the destruction. At no point should any member of staff request destruction of any records without the signed permission of a Director / Assistant Director. This authorisation process should be used for records held locally on Trust premises as well as records held by the Trust’s records storage contractor, and the authorisation process should be used irrespective of whether the record is of a confidential nature or not.

The same authorisation form must be used for electronic records that require destruction/deletion. Contact the ICT department for details of how to ensure that all copies/instances of the records are deleted from any temporary cache or mirrored databases/systems.

The authorisation form listing the records that were destroyed, must be retained indefinitely in accordance with the retention period described in the table in Appendix C.

The destruction exercise relating to records held by the records storage contractor will be co-ordinated on a yearly basis by the Data Protection Officer on behalf of the relevant Information Asset Owners.

Confidential paper-based records held locally on Trust premises must be securely disposed of as soon as possible after they are eligible.

Please refer to the ‘Step by Step Guide to Disposing of Records’ process flow chart which can be found in Appendix J.

3.7.1 Records Archiving

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. If the records have no on-going administrative value but have or may have long-term historical or research value, or they have some administrative value but are more appropriately held as archives. Records with such value must be transferred to the organisation’s approved Place of Deposit. Where the organisation has no existing relationship with a Place of Deposit, The National Archives should be contacted in the first instance. Where the Trust is unsure whether records may have archival value, The National Archives or the Place of Deposit with which the organisation has an existing working relationship should be consulted.

Contact National Advisory Services at TNA (nas@nationalarchives.gov.uk, 020 8392 5330 x 2620). National Advisory Services are also able to advise on any other queries regarding the working of the Public Records Act in respect of

NHS records. A list of all the current appointed Places of Deposit is available on The National Archives website: http://www.nationalarchives.gov.uk/archives/deposit.htm

It is a legal requirement that NHS records which have been selected as archives should be held in a repository that has been approved for the purpose by The National Archives. Where an organisation is already in regular contact with its Place of Deposit, it should consult with it over decisions regarding selection and transfer of records. Where this is not the case, The National Archives should be contacted in the first instance.

The Government is reducing this timeframe for transfer from 30 to 20 years. In 2013, central government records were transferred to the National Archives for 1983 and 1984. Two years' worth of records are now being transferred each year, so that by 2022, the records will relate to 2001 and 2002.

There is an annual survey to monitor the progress of record transfers for all public sector organisations affected by the 20 year rule.

3.7.2 Records Transfer

The mechanisms for transferring records from one organisation to another should be tailored to the sensitivity of the material contained within the records and the media on which they are held. Before transferring any information that may be of a confidential nature you must have approval from the relevant Information Asset Owner for the business area concerned.

Ensure that all transfers of confidential records are handled in accordance with the Trust's:

- Data Protection Policy
- Information Security Policy

4 Records Access, Retrieval and Disclosure

4.1 Records Access

Records must be available to all authorised staff who require access to them for business purposes.

Records held in electronic format are often easier to access and maintain, however staff must always ensure that records are not being accessed unnecessarily, or kept for any longer than reasonably required just because it is easier to do so. If the records contain information that is person identifiable, personal or of a sensitive nature the principles of the General Data Protection Regulations 2016 and the Data Protection Act 2018 as well as the Caldicott Principles must be adhered to.

Records held in paper format are less easy to access, maintain and control than electronic records due to the very nature of them. Paper based records often only have the one master copy and are difficult to back up easily and cost effectively. Therefore, staff must take additional precautions when safeguarding and filing paper records to ensure that retrievals will be possible, when required at some point in the future. Where possible the filing and archiving of paper-based records should provide sufficient information to allow the identification of the records needed and wherever possible should be filed in accordance with the intended future destruction date, i.e. all records due to be destroyed on the same date should be filed together. This makes the secure destruction of these records much more straight forward.

4.2 Records Retrieval

All electronic corporate/business records should be stored on shared drives or servers, which are regularly backed up, and not on the C drives of Trust computers, laptops or peripheral devices. This enables the retrieval of information by staff other than the author where appropriate and necessary. It also greatly reduces the risk of loss due to the failure of laptop or desktop PC hard drives or theft.

The retrieval of electronic records is also easier to control due to the rights and restrictions that can automatically be applied to individual staff logins for the various systems that hold records. Managers are responsible for authorising and requesting the appropriate user rights for individual members of staff, however all staff continue to be responsible for security and integrity of the records and information which they record, handle, store, or otherwise come across during their day to day duties.

All information must be used consistently, only for purposes for which it was intended and never for an individual employee’s personal gain or purpose. If in doubt employees should seek guidance from the Data Protection Officer in the first instance, who will inform the relevant IAO for the business area concerned.

The Trust is committed to effective record keeping systems in logical filing systems and the application of metadata or ‘context’ to assist retrieval.

4.3 Retrieving Archived Paper Records held in Storage with External Storage Contractor

To retrieve archived paper records that have been boxed and stored with the organisation’s external storage contractor, please contact the relevant authorised user for your department. For details of the authorised users in each department and their levels of permissions, please refer to the ‘Records Management Resource Zone’ on the Hub
The storage contractor holds the same list of authorised users that can make requests for boxes to be retrieved from store and delivered to designated addresses across the organisation.

Please refer to the process flow for retrieving archived paper records in storage which can be found in Appendix G.

4.4 Records Disclosure

Person identifiable information held on corporate/business records must be treated as strictly confidential and may only be disclosed to individuals authorised as part of their day-to-day work to have access to it, or with the written consent of the person in question. There are exceptions where disclosure may be permitted, please refer to the Trust's Data Protection Policy for further advice.

4.5 Requests for Information by External Third Parties

Should members of staff be approached by a third party organisation for copies of any information they must refer the request to the appropriate team within the organisation. Under no circumstances should staff divulge any information, however small, to anyone external to the organisation. Refer to the Subject Access Requests Policy and Procedure for further details.

Staff must direct all such requests immediately, in accordance with the policy, to the teams trained to handle and process these requests or, alternatively, seek advice and support from their line manager in the appropriate direction of the request. This process ensures that all requests are handled in a consistent manner, whilst also ensuring that any disclosures of person identifiable information, when carried out, are in strict accordance with the GDPR and Data Protection Act 2018 and Common Law Duty of Confidentiality.

The requests may be, but are not limited to, Subject Access Requests, Police and Coroners' requests or any other type of request where staff are asked for copies of paper Service User information, copies of CCTV footage and any other documentation held by the Trust. Regardless of what is being requested and who the third party making the request is, staff must refer to the Trust's Subject Access Requests Policy and Procedure.

4.6 Requests for Information by Internal Trust Staff

Should staff be approached to provide copies of records, divulge information verbally or confirm specific details of records to internal Trust staff, this is acceptable providing the member of staff being approached is confident that the person requesting the information is actually a member of Trust staff and the Caldicott Principles are followed at all times, including the 'need to know'. Should the staff member be in any doubt, it is acceptable to ask for the request to be emailed in order to verify the requesting staff member's identity and legitimacy of the request. If there is any doubt following the email request then staff should discuss the request with their line manager or another appropriate manager before disclosing any information.

For full details on the procedures for handling requests for information by external third parties and/or internal Trust staff, please refer to the "Data Protection Policy" available on the Hub:

Data Protection Policy

4.7 Digital Records, Digital Continuity and Digital Preservation

The National Data Guardian's (Dame Fiona Caldicott) Review of Data Security, Consent and Opt-Outs introduces a new standard for unsupported software systems. The Trust will review its legacy systems and the future-proofing of its digital clinical record keeping systems to maintain the authenticity, reliability, integrity and usability of records within, as digital technology advances.

5 Dealing with specific records

5.1 Records at contract change

The Trust acknowledges the guidance in the Records Management Code of Practice for Health and Social Care 2016, at the end of a contract for service provision with regard to:

- Retaining records after the contract has ended until the time period for their liability has expired,or making arrangements by which the records can be obtained again.
- Transferring a copy or summary of the entire record of the current caseload to a new provider for continuity of service.
- Informing service users about the change of contract and depending on the circumstances seeking consent and offering the opportunity to object or talk to someone about the transfer.

5.2 Integrated Records

The Trust is party to or going to be party to integrated or joint care records. The Trust is mindful that the ownership of and access to those records must be attributed. The arrangements for doing so will depend on the record, and the Trust commits to the principle of service user consent; as well as an information sharing agreement as a mechanism for providing clarity and transparency on the standards that all participants must meet.

5.3 Controlled Drugs Regime

The Trust follows the procedures for handling information relating to controlled drugs, by NHS England, which includes the conditions for storage, retention and destruction of information.

5.4 Records created via social media

The Trust will be mindful that where social media is used as means of communicating business information to service users, a record of the activity may need to be captured through transcription or periodic storage and this information may need to be retained.

5.5 Website as a Business Record

The Trust will be mindful that as the internet replaces posters, publications and leaflets to interact with service users, websites form part of the record keeping system and must be preserved.

5.6 Cloud based records

The Trust will follow guidance on cloud storage from the Information Commissioner’s Office where records might be stored, rather than on discs or networks (e.g., CCTV images.)

6.0 Training Expectations for Staff

Training is delivered as specified within the Trust Training Needs Analysis (TNA).

7.0 Implementation Plan

The latest approved version of this policy will be posted on the Hub site for all members of staff to view. New members of staff should be signposted to how to find and access this policy and associated procedures during Trust Induction.

8.0 Monitoring Compliance with this Policy

A variety of methods will be used for monitoring compliance against the Records Management Policy including:

- Quarterly audit of the quality of information entered on the Hills Storage database and accuracy of the destruction dates set against records.
- Annual Confidentiality Audits carried out by IAOs.
- Quarterly information risk assurance given by heads of service in their role as IAOs.
- Annual review of user access to the Records Archiving system including a review of access rights.
- Annual audit of health records which includes record creation, record tracking, record retrieval and record retention, disposal and destruction.
- In line with Data Security and Protection Toolkit, an annual audit of Corporate Records undertaken in at least four corporate areas of the organisation.

9.0 References

9.1 Legislation

- Great Britain. 2018. Data Protection Act 2018. London: HMSO. Available at: www.legislation.gov.uk
- European Union. 2016. EU General Data Protection Regulations 2016. Available at: www.eugdpr.org
- Great Britain. 2000. Freedom of Information Act 2000. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2004. *Environmental Information Regulations 2004.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1990. *Computer Misuse Act 1990. Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1990. *Access to Health Records Act 1990. Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1958 and 1967. *Public Records Act 1958 and 1967.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1998. *Crime and Disorder Act 1998*. *Chapter*. London: HMSO. Available at: www.legislation.gov.uk

- Great Britain. 2000. *Electronic Communications Act 2000.* London: HMSO. Available at: www.legislation.gov.uk

9.2 Guidance

- Information Governance Alliance, 2016: Records Management Code of Practice for Health and Social Care 2016. Available at: https://digital.nhs.uk/article/402/Information-Governance
- NHS Digital: Data Security and Protection Toolkit. Available at: www.dsptoolkit.nhs.uk/
- Department of Health, 2003. Confidentiality: NHS Code of Practice Available at: https://digital.nhs.uk/article/402/Information-Governance
- Academy of Royal Colleges, 2013: Standards for the clinical structure and content of service user records. Available at: https://www.rcplondon.ac.uk/projects/outputs/standards-clinical-structure-and-content-service user-records
- Royal College of Physicians, 2015: Professional guidance on the structure and content of ambulance records
  Available at: https://www.rcplondon.ac.uk/projects/professional-guidance-structure-and-content-ambulance-records

10.0 Appendices

Appendix A Definitions

The definitions or explanation of terms relating to this policy are:-

Record	Records are defined as 'information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business'. (ISO 15489:2016) Traditionally records were held on paper, or microfiche, but are now predominantly created and held in electronic format or within electronic systems. The Data Protection Bill Part 7 defines a health record as: A "health record" means a record which— (a) consists of data concerning health, and (b) has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates;
Corporate Records	Records (other than health records) that are of, or relating to, an organisation's business activities covering all the functions, processes, activities and transactions of the organisation and of its employees. Examples of corporate information are policies and procedures, strategies and action plans, minutes and agendas, reports (e.g. annual, accounting, Board), Financial Standing Orders, invoices, public consultations, contracts.
Clinical Records / Health Records	A single record with a unique identifier containing information relating to the physical or mental health of a given service user who can be identified from that information and which has been recorded by, or on behalf of, a health professional, in connection with the care of that service user. This may comprise text, sound, image and/or paper and must contain sufficient information to support the diagnosis, justify the treatment and facilitate the on-going care of the service user to whom it refers.
(Records) Information Lifecycle	The five distinct phases that all records will follow are: creation, use, retention, appraisal and disposal. For further details on each phase please refer to section 3.0.

Person Identifiable Information	Information (or data) 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 identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. Information that can be used to uniquely identify, contact, or locate a single person, or can be used with other sources to uniquely identify a single individual, this includes both service users and Trust staff.

Appendix B Roles and Responsibilities

Trust Board

The Trust Board has overall responsibility for records management within the organisation with the Chief Executive being ultimately accountable for the proper management of all records within the organisation. The Executive Directors are accountable for the quality of records management within each of their Directorates.

Corporate Integrated Governance Group

The Corporate Integrated Governance Group consists of Executive Directors and Assistant Directors and is chaired by the Chief Executive. The Group carries delegated responsibility from the Trust Board for approving this policy.

Director of Governance and Quality Assurance

The Director of Governance and Quality Assurance has strategic responsibility for Information Governance including records management. The Director of Governance and Quality Assurance is also the Trust's Senior Information Risk Owner (SIRO) and as such is the director responsible for managing information risk.

Information Asset Owners

Information Asset Owners have direct responsibility for the records held in their work area, including the integrity, secure storage and quality of those records. IAOs are responsible for taking a pro-active role in championing good records management within their areas of responsibility as well as ensuring the appropriate use of the Trust's external document storage contractor.

The IAOs provide direct support to the Senior Information Risk Owner and are also responsible for identifying, managing and mitigating information risks in relation to records they are responsible for.

Data Protection Officer

The Data Protection Officer is responsible for providing general guidance and advice on the management and retention of records and the application of this policy.

Line Manager and Supervisors

All line managers and supervisors are responsible for ensuring that their staff are adequately trained and apply the appropriate guidelines on a day to day basis.

All Staff

All Trust staff, whether clinical or administrative, who create, receive and use records have records management responsibilities. This responsibility is established at, and defined by, the law (the Public Records Act). 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 associated guidance. Individuals are also bound by their own professional Codes of Conduct.

Appendix C

Retention Periods for each Record Type

The retention periods listed in the column “Disabilities Trust Retention Period” in the following table are the retention periods that staff should refer to and adhere to at all times, the Information Governance Alliance ‘Notes’ column is for additional information and reference only. The table below has been updated from the Records Management Code of Practice for Health and Social Care 2016, published by the Information Governance Alliance.

The table does not contain all record types, only those records that are used or referred to most frequently in the organisation have been extracted for guidance. If information is required regarding another type of record not listed in the table, please refer to the Code of Practice at:
https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

Record Type ***(in alphabetical order)***	**Example(s)**	**Disabilities Trust Retention Period** ***(from the date of creation unless otherwise stated)***	**Notes**
Clinical Records / Operations:			
Adult health records not covered by any other section in this schedule	Discharge or Service User last seen	**8 years**	Review and if no longer needed destroy
Adult safeguarding records		**10 years from date of last contact** or 8 years after death	
Adult social care records	End of care or client last seen	**8 years**	Review and if no longer needed destroy
Audit Trails of electronic health records		**Indefinitely**	NHS organisations are advised to retain all audit trails until further notice.
Children and young people (all types of records relating to children and young people)		**Retain until the service user's 25th birthday** or 26th if young person was 17 at conclusion of treatment, or 8 years after death.	If the illness or death could have potential relevance to adult conditions or have genetic implications, the advice of clinicians should be sought as to whether to retain the records for a longer period.
Children safeguarding records		**70 years** after last contact with the individual concerned	
Clinical audit records	Clinical Performance Indicators reports	**5 years**	

Clinical Diaries	End of the year to which they relate	**2 years**	Review and if no longer needed destroy
Clinical Protocols	Creation	**25 years**	Review and consider transfer to a Place of Deposit
Controlled drug documentation	Drug books	Requisitions – **2 years.** Registers and CDRBs – **2 years from last entry**	NHS England and NHS BSA guidance for controlled drugs can be found at: http://www.nhsbsa.nhs.uk/PrescriptionServices/1120.aspx and https://www.england.nhs.uk/wp-content/uploads/2013/11/som-cont-drugs.pdf The Medicines, Ethics and Practice (MEP) guidance can be found at the link (subscription required) http://www.rpharms.com/support/mep.asp#new Guidance from NHS England is that locally held controlled drugs information should be retained for 7 years. NHS BSA will hold primary data for 20 years and then review. NHS East and South East Specialist Pharmacy Services have prepared pharmacy records guidance including a specialised retention schedule for pharmacy. Please see:http://www.medicinesresources.nhs.uk/en/Communities/NHS/SPS-E-and-SE-England/Reports-

			Bulletins/Retention-of-pharmacy-records/
Datasets released by NHS Digital under a data sharing agreement	Date specified in the data sharing agreement	Delete with immediate effect	Delete according to NHS Digital instruction
Destruction Certificates or Electronic Metadata destruction stub or record of clinical information held on destroyed physical media	Destruction of record or information	**20 Years**	Review and consider transfer to a Place of Deposit
Daily handover sheet	Date of handover	**2 years** Review and if no longer needed destroy	This retention relates to the main record. The individual sheets held by staff must be destroyed confidentially at the end of the shift.
Destruction records of individual health records, case notes and other health-related records - paper and/or elec format. (refer to ‘destruction of records (other than health records)’ for corporate record destructions)		**Indefinitely**	

Electrocardiogram (ECG) records	ECG strips	**8 years**	Each chart should be labelled with the service user's name and unique identifier (the incident date and number). Any over-sized charts can be stored separately where a report is written into the health records (this must be noted on the main A3 PCR).
Equipment maintenance logs	Decommissioning of the equipment	**11 years**	Review and consider transfer to a Place of Deposit
Homicide / Serious Untoward Incident records		**20 years**	
Inspection of equipment records	Decommissioning of equipment	**11 Years**	Review and if no longer needed destroy
Litigation - records/documents related to any litigation		**Dependent on the case** – see notes	As advised by the organisation's legal advisor. All records to be reviewed. Normal review period is 10 years after the file is closed.
Mental Health records	Discharge or patient last seen	**20 years or 8 years after the Service User has died**	Review and if no longer needed destroy
Notifiable disease book	Creation	**6 years**	Review and if no longer needed destroy
Occupational health records (staff)		**6 years** after termination of employment, unless litigation ensues	
Occupationally Related Diseases (e.g. asbestosis, pneumoconiosis, byssinosos)		**40 years/5 years** after date of last entry in the record	For full details on Occupational Related Diseases, please go to: http://www.hse.gov.uk/riddor/occupational-diseases.htm

			A) Where the record is representative of the personal exposures of identifiable employees, for at least 40 years or B) In any other case, for at least 5 years.
(General) Operating Policies and Procedures		**3 years** retain the current version and previous version for 3 years Life of organisation plus 6 years (IGA)	From CQC outcome 21
Paediatric records		See Children and young people above	
Pharmacy prescription records - see also Controlled Drugs	Discharge or patient last seen	**2 Years**	Review and if no longer needed destroy
Physiotherapy records		Retain for the period of time appropriate to the Service User/speciality, e.g. children's records should be retained as per the retention period for children and young people; mentally disordered persons (within the meaning of the Mental Health Act	

		1983) 20 years after the last entry in the record or 8 years after the Service Users death if this occurred while in the care of the service.	
Psychology records		**30 Years** or 8 years after the Service User has died	
Record of long term illness or an illness that may reoccur	Discharge or patient last seen	**30 Years** or 8 years after the Service User has died	Review and if no longer needed destroy
Referrals not accepted	Date of rejection	**2 years** as an ephemeral record	Review and if no longer needed destroy
Requests for funding for care not accepted	Date of rejection	**2 years** as an ephemeral record	Review and if no longer needed destroy
Risk Assessments		Retain the latest risk assessment until a new one replaces it	
Scanned records (relating to service user care)	Electronic scanned copy of a PCR form (originally on paper)	**Adult - 8 years** (applies to ALL Ambulance Clinical Records) **Children and young people - Retain until the service user's 25th birthday** or 26th if young person was 17 at conclusion of	

		treatment, or 8 years after death.	
Service User Property Books/Logs	End of the year to which they relate	**2 years**	Review and if no longer needed destroy
Voice recordings, video records relating to service user care, video conferencing records related to service user care, DVD records related to service user care (includes Telemedicine records, Out of hour's records, GP cover and NHS 111 records).		**8 years**	
Corporate Records (administrative and organisational):			
Accident/ Incident forms	Datix	**10 years**	
Accident register (reporting of injuries, diseases and dangerous occurrences register)	Datix	**10 years**	
Agendas of board meetings, committees, sub-committees (master copies including associated papers)		**20 years**	
Agendas (other)		**2 years**	Including records relating to the school
Agreements / Contracts Financial contracts: Approval files Approved suppliers lists		 **15 years** **11 years**	

Non-sealed (property) contracts on termination		**6 years** after termination of contract	
Non-sealed (other) contracts on termination		**6 years** after termination of contract	
Sealed contracts (and associated records)		**15 years** (min)	Retain for a minimum of 15 years, after which they should be reviewed.
Maintenance contracts (routine)		**6 years** from end of contract	
Contractual arrangements with hospitals or other bodies outside the NHS, including papers relating to financial settlements made under the contract (e.g. waiting list initiative, private finance initiative)		**6 years** after end of financial year to which they relate	
Annual / corporate reports		**3 years**	
Assembly / Parliamentary questions, MP enquiries		**10 years**	
Audit Records, Internal & External in any format paper, electronic etc	Organisational Audits, Records Audits, Systems Audits	**2 years** from the date of completion of the audit	
Business plans, including local delivery plans		**20 years**	
Catering forms		**6 years**	

Close circuit TV images		**31 days** and erase permanently	ICO Code of Practice: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf The length of retention must be determined by the purpose for which the CCTV has been deployed. The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.
Commissioning decisions, appeal documentation, decision documentation		**6 years** from date of appeal and/or decision	
Complaints (see also litigation & litigation dossiers) Correspondence, investigation and outcomes Returns made to DH		**10 years** from completion of action Files closed annually and kept for **6 years** following closure	http://www.nationalarchives.gov.uk/documents/information-management/sched_complaints.pdf The incident is not closed until all subsequent processes have ceased including litigation. The file must not be kept on the service user file. A separate file must always be maintained. Including records relating to the school

Computer programmes written in-house, related documentation		Lifetime of software	
Contracts		See ‘Agreements / Contracts’	
Copyright declaration forms (Library Service)		**6 years**	
Data Input Forms where the data/information has been input to a computer system	Address notifications from local Councils	**2 years**	
Destruction of records (other than health records), records documenting the archiving, transfer to public records archive. (refer to ‘destruction records of individual health-related records’ for health record destructions)		**20 years**	
Diaries (office)		**1 year** after the end of the calendar year to which they refer	
Flexi working hours (personal record of hours actually worked)		**6 months**	
Freedom of Information requests		**3 years** after full disclosure	Where redactions have been made it is important to keep a copy of the redacted disclosed documents or if not practical, to keep a summary of the redactions.
Health and safety documentation		**3 years**	

History of the organisation or predecessors, its organisation and procedures	Establishment order	**20 years**	
Incident forms	Datix	**10 years**	
Indices (records management) registry lists of public records marked for permanent preservation, or containing the record of management of public records. File lists and document lists where public records or their management are not covered.		**20 years**	
Laundry lists and receipts		**2 years** from completion of audit	
Litigation dossiers (complaints including accident/incident reports) Records/documents relating to any form of litigation	Coroners' requests	**10 years**	Where a legal action has commenced, keep as advised by legal representatives
Manuals – policy and procedure (administrative and clinical, strategy documents)compo		**10 years** after life of the system (or superseded) to which the policies or procedures refer	Policy documents may have archival value. Including policies relating to the school
Meetings and minutes papers of major committees and sub-committees (master copies)		**20 years**	Including records relating to the school
Meetings and minutes papers (other, including reference copies of major committees)		**2 years**	Including records relating to the school

Occupancy reports		**2 years** after the year to which they relate	
Papers of minor or short-lived importance not covered elsewhere, eg advertising matter, covering letters, reminders, letters making appointments, anonymous or unintelligible letters, drafts, duplicates of documents known to be preserved elsewhere (unless they have important minutes on them) indices and registers compiled for temporary purposes, routine reports, punched cards, other documents that have ceased to be of value on settlement of the matter involved.		**2 years** after the settlement of the matter to which they relate	
Police Statements (made in the context of Service User episodes. Statements are requested by the Police to the Trust staff in relation to alleged injuries of, or by, service users)		**10 years** (congruent retention period as Incident Forms)	
Press cuttings		**1 year**	Where bound volumes exist, these may have archival value.
Press releases and important internal communications		**6 years**	
Project files (including abandoned or deferred projects): Over £100,000 on termination Less than £100,000 on termination Project team files (summary retained)		 **6 years** **2 years** **3 years**	

Public Consultations eg about future provision of services		**5 years**	
Quality control records: External Internal (relating to products)		 **2 years** **10 years**	
Quality assurance records eg Care Quality Commission, Healthcare Improvement Scotland, Care Inspectorate Scotland, Care Inspectorate Wales, Ofsted, Investors in People		**12 years**	
Receipts for registered and recorded mail		**2 years** following the end of the financial year to which they relate	
Reports (major)		**30 years**	Including records relating to the school
Requests for access to records (other than Freedom of Information or subject access requests)		**6 years** after last action	
Requisitions		**18 months**	
Serious incident files		**20 years**	
Service user information leaflets		**6 years after the leaflet has been superseded**	
Service user Surveys re access to services etc		**2 years**	
Software licences		Lifetime of software	
Specifications eg equipment, services		**6 years**	

Statistics including Korner returns, contract minimum data set, statistical returns to DOH, service user activity		**3 years** from date of submission	
Subject access requests (GDPR, DPA and AHR) records of requests		**3 years** after last action	Review and if no longer needed destroy
Time sheets (relating to a Group or Department where the timesheets are kept as a tool to manage resources/staffing levels)		**6 months**	
Visitor logs/books		**2 years** from last entry	
Estates / Procurement / Supplies records:			
Approval files (contracts and purchase orders)		**6 years** after end of the year the contract expired	
Approved suppliers lists		**11 years**	
Buildings, papers relating to occupation of the building (but not health and safety information)		**3 years** after occupation ceases	
Deeds of title		While the organisation has ownership of the building	Retain while the organisation has ownership of the building unless a Land Registry certificate has been issued, in which case the deeds should be placed in an archive. If there is no Land Registry

			certificate, the deeds should pass on with the sale of the building. Also applies to deeds relating to the school
Delivery notes		**2 years** after end of financial year to which they relate	
Drawings, plans and buildings (architect signed, not copies)		Lifetime of the building to which they relate	
Engineering works, plans and building records		Lifetime of the building to which they relate	
Equipment records of non-fixed equipment, including specification, test records, maintenance records and logs		**11 years**	If the records relate to vehicles (e.g. fleet vehicles etc) and where the vehicle no longer exists, providing there is a record that it was scrapped, the records can be destroyed.
Inspection reports eg boilers, lifts		Lifetime of installation	If there is any measurable risk of a liability in respect of installations beyond their operational lives, the records should be retained indefinitely.
Inventories of furniture, medical and surgical equipment not held on store charge and with a minimum life of 5 years Inventories of plant and permanent or fixed equipment		Keep until next inventory **5 years** after date of inventory	

Leases, the grant of leases, licences and other rights over property		Period of the lease plus **12 years**	
Photographs of buildings		**30 years**	
Plans, building (as built)		Lifetime of building	May have historical value.
Purchase Orders – see 'Approval Files' above			
Stock control reports -		**18 months**	
Stores records: Major (eg stores ledgers) Minor eg requisitions, issue notes, transfer vouchers, goods received books		 **6 years** **18 months**	
Structure plans, organisational charts i.e. the structure of the building plans		Lifetime of building	
Supplies records eg invitations to tender and inadmissible tenders, routine papers relating to catering and demands for furniture, equipment, stationery and other supplies		**18 months**	
Surveys, building and engineering works		Lifetime of building or installation	
Tenders / Purchase Orders / Quotations: Successful			

Unsuccessful		Tender period plus 6 year limitation period **6 years**	
Financial / Accounting records:			
Accounts, annual (final, one set only)		**30 years**	
Accounts, minor records; pass books, paying-in slips, cheque counterfoils, cancelled/discharged cheques, accounts of petty cash expenditure, travel and subsistence accounts, minor vouchers, duplicate receipt books, income records, laundry lists and receipts		**2 years** from completion of audit	Including records relating to the school
Accounts, working papers		**3 years** from completion of audit	
Advice notes, payment		**18 months**	
Audit reports, internal and external including management letters, value for money reports and system/final accounts memoranda		**2 years** after formal completion by statutory auditor	
Bank statements		**2 years** from completion of audit	Including records relating to the school
Banks Automated Clearing System (BACS) records		**6 years** after year end	
Bills, receipts and cleared cheques		**6 years**	Including records relating to the school

Budgets including working papers, reports, virements and journals		**2 years** from completion of audit	
Cash sheets		**6 years** after end of financial year to which they relate	
Estimates, including supporting calculations and statistics		**3 years** after end of financial year to which they relate	
Expense claims, including travel and subsistence claims, and claims and authorisations		**6 years** after end of financial year to which they relate	
Fraud case files/investigations		**6 years**	
Fraud national proactive exercises		**3 years**	
Free school meal registers where the register is used as a basis for funding		**6 years** after the year to which they relate	
Invoices, capital paid invoices, cash books		**6 years** after end of financial year to which they relate	Including records relating to the school e.g. Ledger, Invoices etc
Loans and grants managed by the school		**12 years** After the date of the last payment	
PAYE records		**6 years**	

		after termination of employment	
Payments		**6 years** after year end	
Payroll list of staff in the pay of the organisation		**6 years** after termination of employment	Destroy under confidential conditions. For superannuation purposes, organisations may wish to retain such records until the subject reaches benefit age.
Pupil Premium Fund Records		**6 years** after the date pupil leaves	
Receipts		**6 years** after end of financial year to which they relate	
Salaries		See ‘Wages / salaries’	
Student Grant Applications		**3 years** after end of financial year to which they relate	
Superannuation accounts and registers		**10 years**	
Tax forms		**6 years**	
Transport (staff pool car documentation)		**3 years** unless litigation ensues	
VAT records		**6 years** after end of financial year to which they relate	
Wages / salaries		**10 years**	

Fundraising:			
Donations		**6 years** after end of financial year to which they relate	
Supporter details		**2 years** after the individual’s support was given (or in the case of gifting in a Will – 2 years after settlement)	
Volunteer details		**2 years** after the volunteer last volunteered with the Trust	
Human Resources / Personnel records:			
CVs for non-executive directors: Successful applicants Unsuccessful applicants		 **5 years** following term of office **2 years**	
Industrial relations, not routine staff matters, including industrial tribunals		**10 years**	
Job advertisements - 1 year		**1 year**	
Job applications:			

Successful Unsuccessful		**3 years** following termination of employment **6 Months** from interview date	
Job descriptions		**3 years**	
Leavers’ dossiers		**6 years** after individual has left **Summary to be retained until individual’s 75th birthday** (or until 6 years after cessation of employment if aged over 70 years at the time) – see notes.	The summary should contain everything except attendance books, annual leave records, duty rosters, clock cards, timesheets, study leave applications, training Plans. The 6 year retention period is to take into account any ET claims, or EL claims that may arise after the employee leaves DT employment, requests for information from the pensions provider etc. Claims of this nature can include periods of up to 6 years or more, prior to the claim and where evidence could be needed from a number of sources, it is appropriate to retain as much as possible from the original file.
Letters of appointment		**6 years** after employment has terminated or until 70th birthday, whichever is later.	

Maternity/ Adoption/ Paternity/ Shared parental leave records		**6 years** after the end of the year to which the records relate	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960) as amended
National Minimum/ Living Wage records		**3 years** after the end of the period covered	National Minimum Wage Act 1998
Parental Leave		**Until the child is 18 years old**	To track what leave has been taken during the applicable period
Pension Forms (all)		**7 years**	
Personnel / human resources records, major, eg personal files, letters of appointment, contracts, references and related correspondence, registration authority forms, training records, equal opportunity monitoring forms (if retained))		**6 years** after individual has left **Summary to be retained until individual's 75th birthday** (or until 6 years after cessation of employment if aged over 70 years at the time) – see notes in the DOH guidance column	The summary should contain everything except attendance books, annual leave records, duty rosters, clock cards, timesheets, study leave applications, training Plans. The 6 year retention period is to take into account any ET claims, or EL claims that may arise after the employee leaves DT employment, requests for information from the pensions provider etc. Claims of this nature can include periods of up to 6 years or more, prior to the claim and where evidence could be needed from a number of sources, it is appropriate to retain as much as possible from the original file.
Personnel / human resources, minor, eg attendance books, annual leave records, duty rosters i.e. duty rosters held on the individual's record not the organisation or		**2 years** after the year to which they relate	

departmental rosters, clock cards, timesheets (relating to individual staff members)			
Sick Pay records		**6 years** after employment has terminated	A breach of employment contract claim can be made up to 6 years after employment ceases.
Staff car parking permits		**3 years**	
Study leave applications		**5 years**	
Timesheets (for individual members of staff)		**2 years** after the year to which they relate	
Training plans		**2 years**	
Working Time records		**2 years** after the year to which they relate	Working Time Regulations 1998 (SI 1998/1833)
Research:			
Advanced Medical Therapy Research Master File	Closure of research	**30 years** Review and consider transfer to a Place of Deposit	See guidance at: https://www.gov.uk/guidance/advanced-therapy-medicinal-products-regulation-and-licensing For clinical trials record retention please see the MHRC guidance at https://www.gov.uk/guidance/good-clinical-practice-for-clinical-trials
Research data sets	End of research	**Not more than 20 years** Review and consider transfer to a Place of Deposit	http://tools.jiscinfonet.ac.uk/downloads/bcs-rrs/managing-research-records.pdf

Research Ethics Committee’s documentation for research proposal	End of research	**5 years** Review and consider transfer to a Place of Deposit	"For details please see:http://www.hra.nhs.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics-committees/ Data must be held for sufficient time to allow any questions about the research to be answered. Depending on the type of research the data may not need to be kept once the purpose has expired. For example data used for passing an academic exam may be destroyed once the exam has been passed and there is no further academic need to hold the data. For more significant research a place of deposit may be interested in holding the research. It is best practice to consider this at the outset of research and orphaned personal data can inadvertently cause a data breach."

Research Ethics Committee’s minutes and papers	Year to which they relate	**Before 20 years** Review and consider transfer to a Place of Deposit	Committee papers must be transferred to a place of deposit as a public record: http://www.hra.nhs.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics-committees/
Education Records:			
Admissions Records			
Admissions – if the admission is successful		**1 year** from date of admission	School Admissions Code Statutory guidance for admission authorities, local authorities, schools adjudicators and admission appeals panels December 2014
Admissions – if the admission is unsuccessful		**1 year** from date of resolution	School Admissions Code Statutory guidance for admission authorities, local authorities, schools adjudicators and admission appeals panels December 2014
Register of Admissions		**3 years** after the date on which the entry was made	The School may wish to consider keeping the admission register permanently as an archive record of historical value.
Proofs of address supplied by parents as part of the admission process		**1 year** from end of current year	

Supplementary information for successful admissions	Such as religion, medical conditions	to be added to the pupil file	
Supplementary information for unsuccessful admissions		until appeals process completed	
Pupil’s Educational Record			
Child Protection Information		**25 years** from the date of birth of the pupil	If records are placed in the pupil file, it should be in a sealed envelope and retained for the same period of time as the pupil file
Pupil’s Educational Record		**25 years** from the date of birth of the pupil	A review of the file should be completed at the end of the retention period. The file should follow the pupil if he/she leaves the school including to another school or to a pupil referral unit
Attendance			
Attendance registers		**3 years** after the date on which the entry was made	
Correspondence relating to any absence (authorised or unauthorised)		**2 years** from the end of the current academic year	
Special Educational Needs files, reviews and Education, Health and Care Plan, including advice and information provided		**31 years** from the date of birth of the pupil	

to parents regarding educational needs and accessibility strategy		[Education, Health and Care Plan is valid until the individual reaches the age of 25 years – the retention period adds an additional 6 years from the of the plan in line with the Limitation Act]	
Curriculum			
Curriculum Returns		**3 years** from the end of the current year	
Examination Results		**6 years** from the end of the current year	SATS results should be recorded on the pupil's educational file and will therefore be retained until; the pupil reaches the age of 25 years. The school may wish to keep the composite record of all the whole years SATS results to allow suitable comparison
Examination Papers		To be kept until any appeals/validation process is complete	
Published Admission Number (PAN) Reports		**6 years** from the end of the current year	
Schemes of work, timetable, class record books, mark books, record of homework set		**1 year** from the end of the current year	It may be appropriate to review these records at the end of each

			year and allocate a further retention period
Pupil's Work		**1 year** from the end of the current year	Where possible, the pupil's work should be returned to the pupil at the end of the academic year. If this is not in the school's policy, then the retention period applies
School Trips			
Parental Consent Forms for school trips where there has been no major incident		**2 years** from the end of the current year	
Parental Consent Forms for school trips - where there has been a major incident		**25 years** From the date of birth of the pupil involved in the incident	The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils
Local Authority			
Attendance Returns		**1 year** from the end of the current year	
School Census Returns		**5 years** from the end of the current year	
Circulars and other information sent from the local authority		Operational use	
Central Government			
OFSTED reports and papers where a physical copy is held		Life of the report then review	

Returns made to central government		**6 years** from the end of the current year	
Circulars and other information sent from central government		Operational use	
Management of Governing Body			
Records relating to the election of parent and staff governors not appointed by the governors		**6 months** from the date of election	
Records relating to the appointment of co-opted governors		**25 years**	Provided that the decision has been recorded in the minutes, the records relating to the appointment can be destroyed once the co-opted governor has finished their term of office (except where there have been allegations concerning children)
Records relating to the election of chair and vice chair			Once the decision has been recorded in the minutes, the records relating to the election can be destroyed
Register of attendance at full governing board meetings		**6 years** from the date of last meeting in the book	
Papers relating to the management of the annual parents' meeting		**6 years** from the date of the meeting	
Records relating to Governor Monitoring Visits		**3 years**	

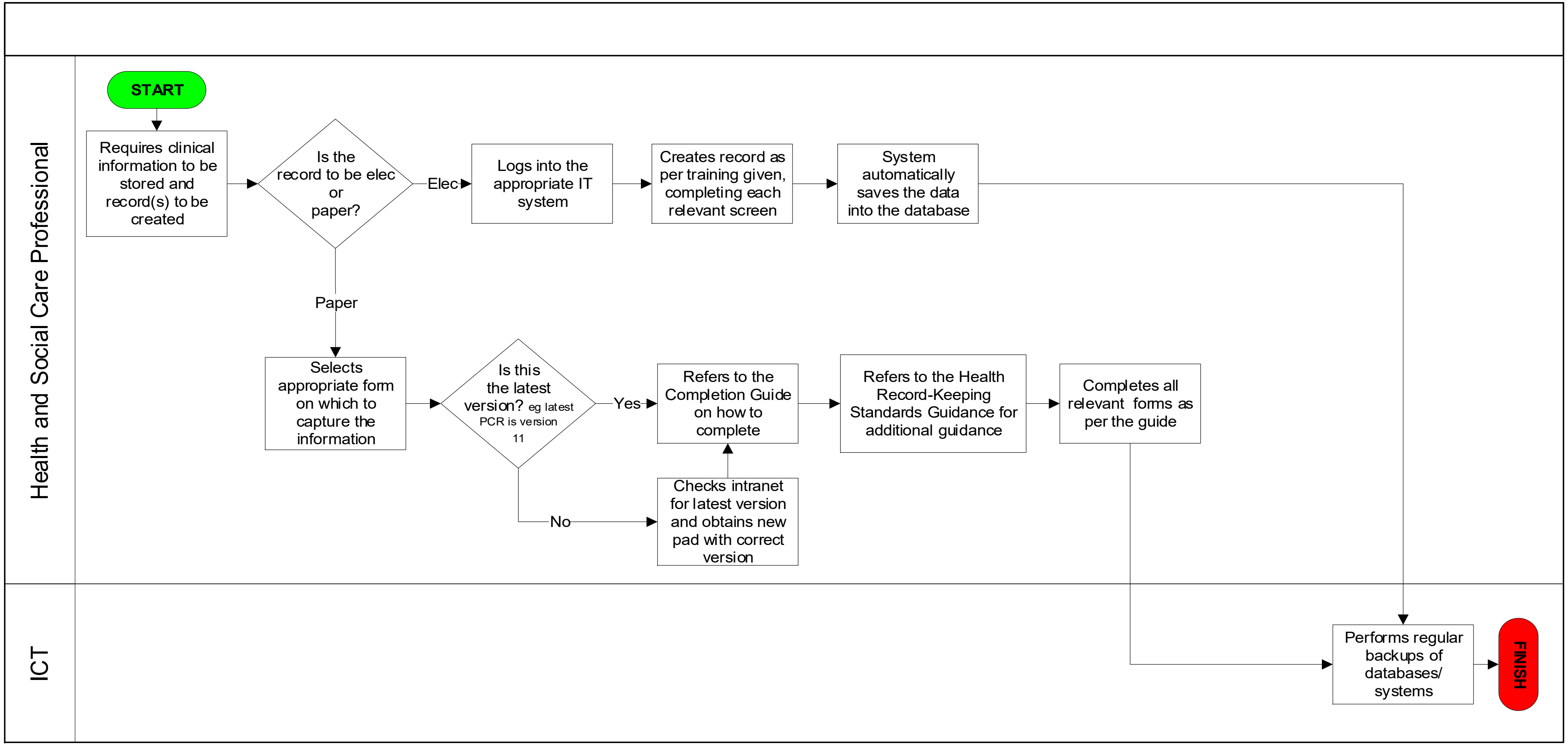
		from the date of the visit	
Annual Reports required by the DoE		**10 years** from the date of report	
Correspondence sent and received by the governing body or head teacher		**3 years** from the end of the current year	
Action plan created and administered by the governing body			Until superseded or whilst relevant
Scheme of delegation and terms of reference for committees		Until superseded of whilst relevant (Schools may wish to retain these records for reference purposes in case decisions need to be justified)	
Governor Management			
Records relating to the appointment of a clerk to the governing body		**6 years** from the date which clerk appointment ceases	
Records relating to the terms of office of serving governors (including evidence of appointment and governor declarations against disqualification criteria)		**6 years** from the date the appointment ceases	
Register of business interests		**6 years** from the date the appointment ceases	

Governors Code of Conduct		This is expected to be a dynamic document; one copy of each version should be kept for the life of the organisation	
Records relating to the training required and received by Governors		**6 years** from the date the Governor steps down	
Records relating to the induction programme for new Governors		**6 years** from the date appointment ceases	
Head Teacher and Senior Management Team			
Log Books of activity in the school maintained by the Head Teacher		**6 years** from the date of the last entry and review	It may be appropriate to archive these if they are of historical value
Reports created by the Head Teacher or the Management Team		**3 years** from the date of the report, then review annually if not destroyed	
Records created by Head Teacher and other members of staff with administrative responsibility which do not fall under any other category		**6 years** from the academic year to which they relate then review annually if not destroyed	
School Development Plans		**3 years** after the life of the plan	

Educational Administration			
Records relating to the creation and publication of the school brochure, prospectus and circulars to staff, pupils or parents.		**3 years** from the end of the academic year it relates to	
Consents relating to school activities		Consent will last whilst the pupil attends the school and should be destroyed when the pupil leaves	
Newletters and other items with a short operational use		**1 year** from the end of the academic year it relates to	It may be appropriate to archive these if they are of historical value
Visitor management systems (including electronic systems, visitor books and signing in sheets)		**6 years** from the date of the last entry	
School meal registers/summary sheets		**3 years** after the current year	
Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations		**6 years** from the academic year to which they relate then review annually if not destroyed	

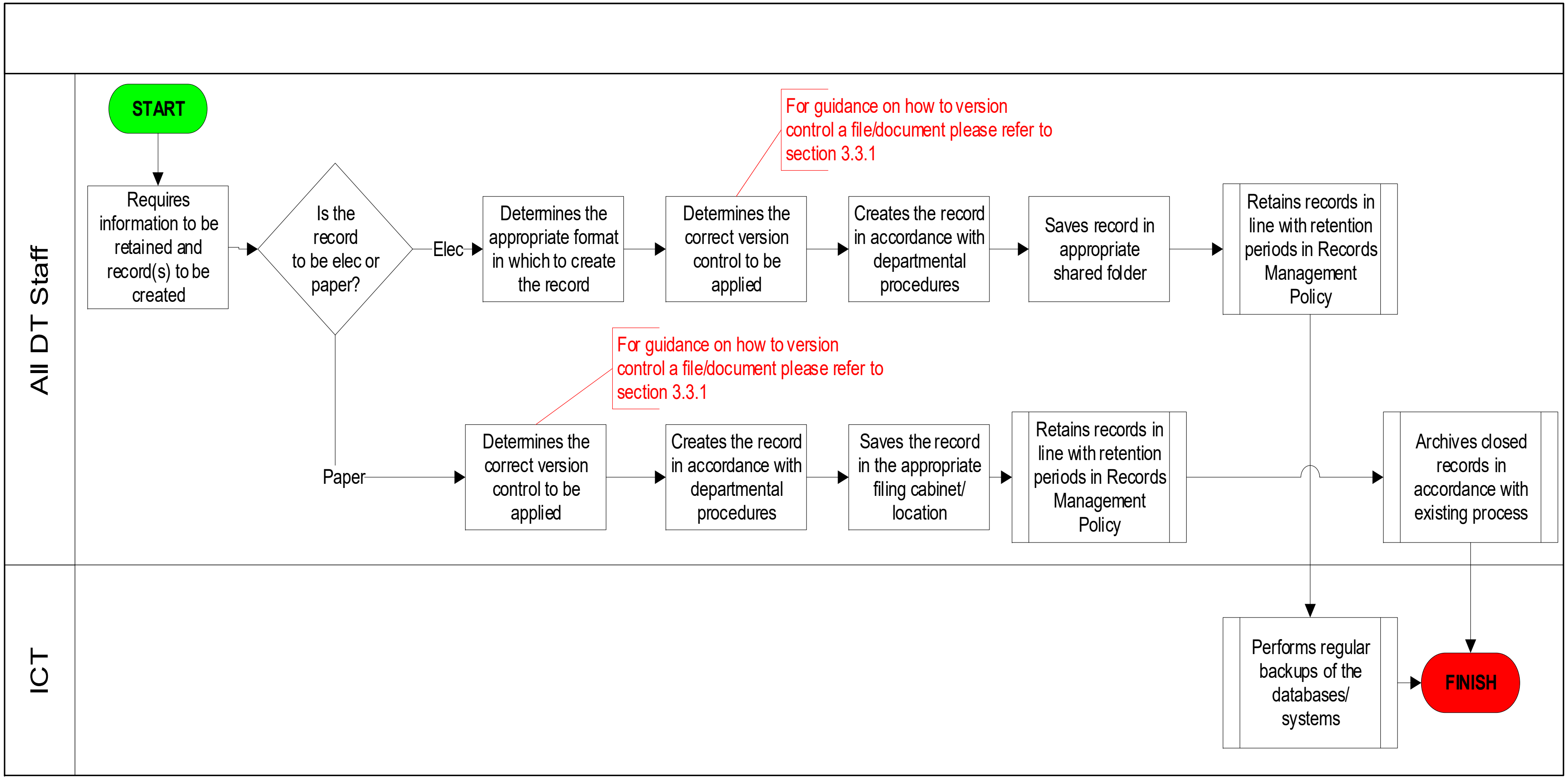
Appendix D

Process Flow: Step by Step Guide to Creating Clinical Records

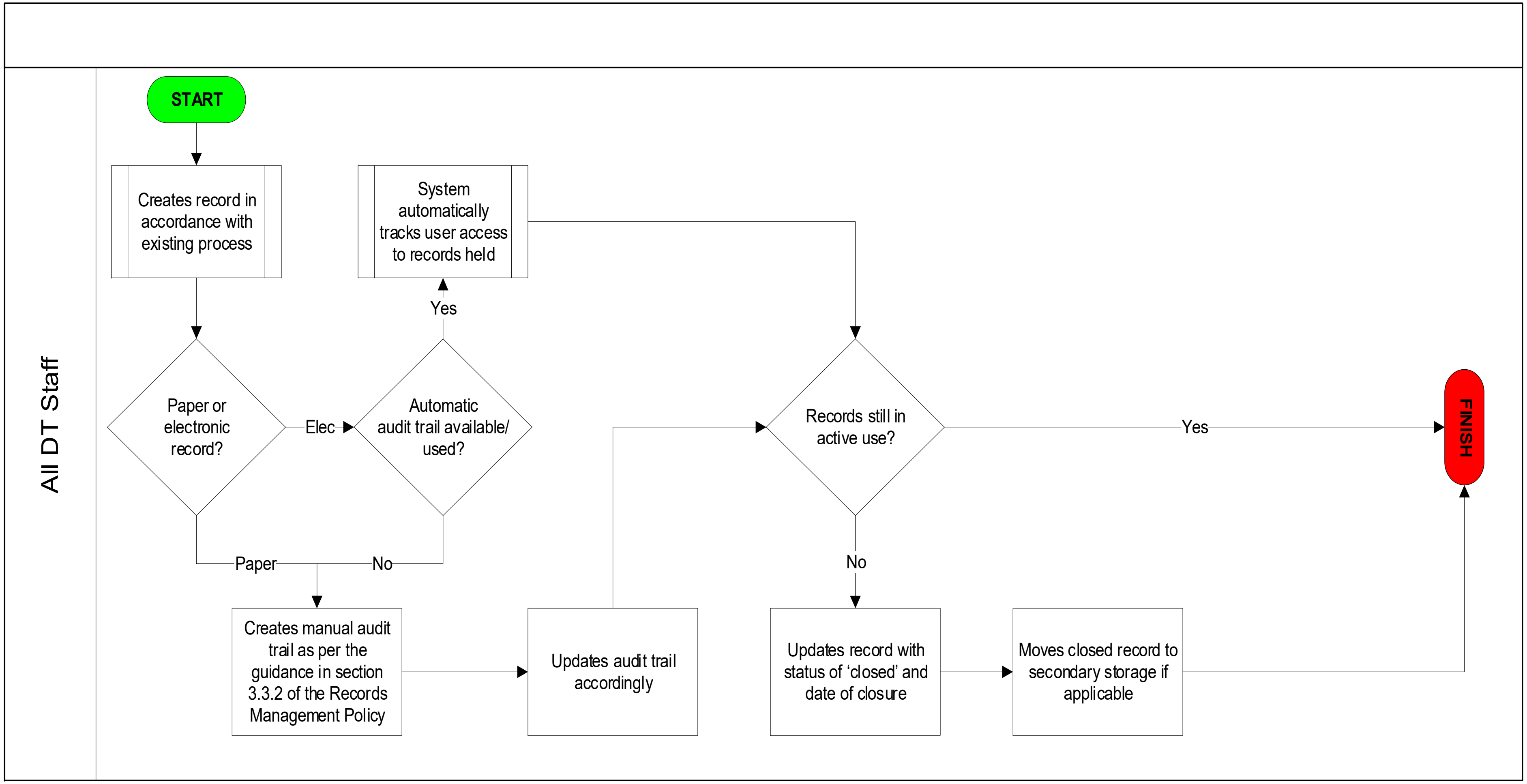

Health and Social Care Professional
ICT
START
Requires clinical information to be stored and record(s) to be created
Is the record to be elec or paper?
Elec
Logs into the appropriate IT system
Creates record as per training given, completing each relevant screen
System automatically saves the data into the database
Paper
Selects appropriate form on which to capture the information
Is this the latest version? eg latest PCR is version 11
Yes
Refers to the Completion Guide on how to complete
Refers to the Health Record-Keeping Standards Guidance for additional guidance
Completes all relevant forms as per the guide
No
Checks intranet for latest version and obtains new pad with correct version
Performs regular backups of databases/ systems
FINISH

Appendix E

Process Flow: Step by Step Guide to Creating Corporate Records

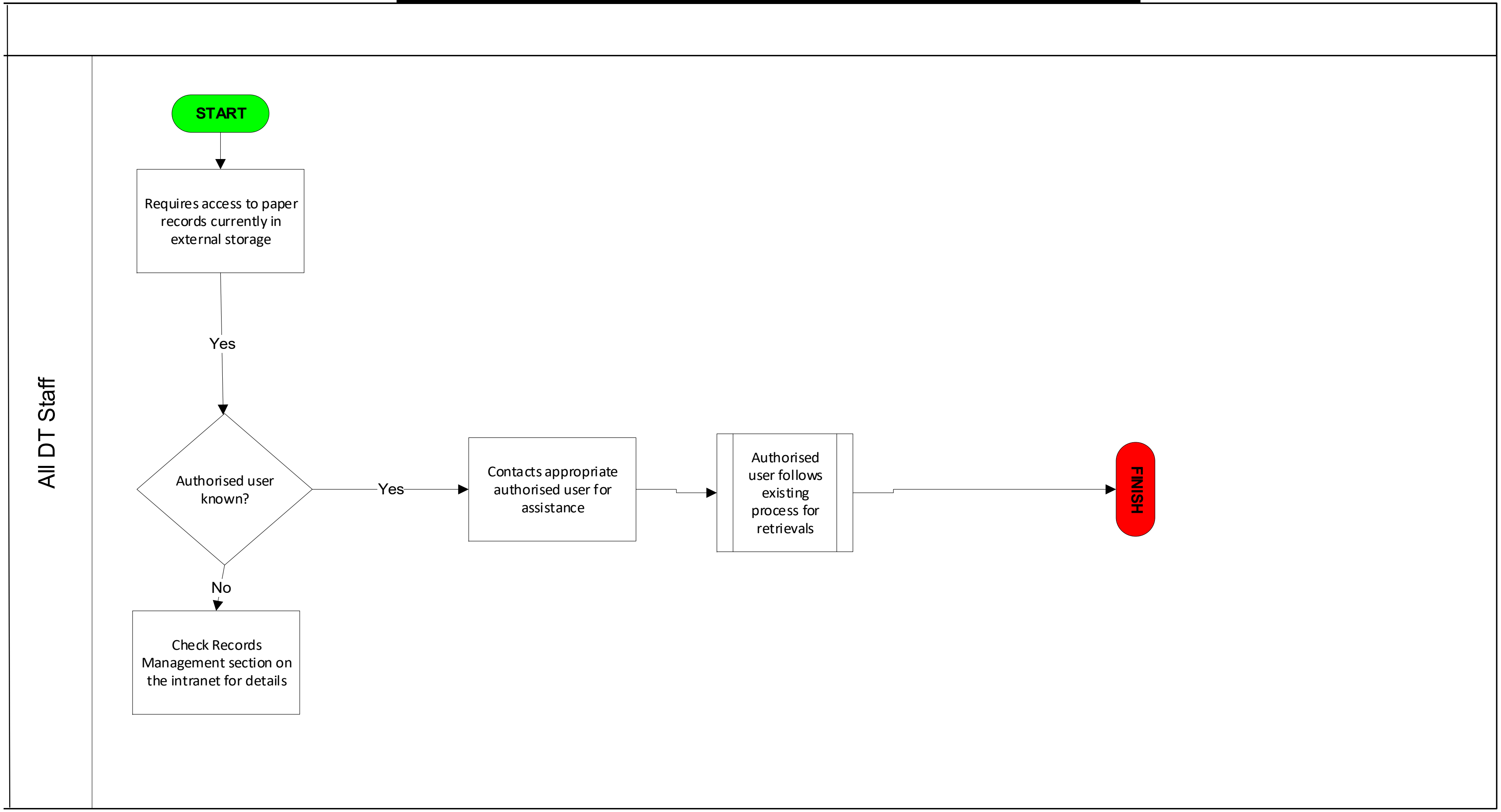

All DT Staff
ICT
START
Requires information to be retained and record(s) to be created
Is the record to be elec or paper?
Elec
Determines the appropriate format in which to create the record
Determines the correct version control to be applied
For guidance on how to version control a file/document please refer to section 3.3.1
Creates the record in accordance with departmental procedures
Saves record in appropriate shared folder
Retains records in line with retention periods in Records Management Policy
Paper
Determines the correct version control to be applied
For guidance on how to version control a file/document please refer to section 3.3.1
Creates the record in accordance with departmental procedures
Saves the record in the appropriate filing cabinet/ location
Retains records in line with retention periods in Records Management Policy
Archives closed records in accordance with existing process
Performs regular backups of the databases/ systems
FINISH

Process Flow: Tracking Records


All DT Staff
START
Creates record in accordance with existing process
Paper or electronic record?
Elec
Automatic audit trail available/ used?
Yes
System automatically tracks user access to records held
Paper
No
Creates manual audit trail as per the guidance in section 3.3.2 of the Records Management Policy
Updates audit trail accordingly
Records still in active use?
Yes
No
Updates record with status of 'closed' and date of closure
Moves closed record to secondary storage if applicable
FINISH

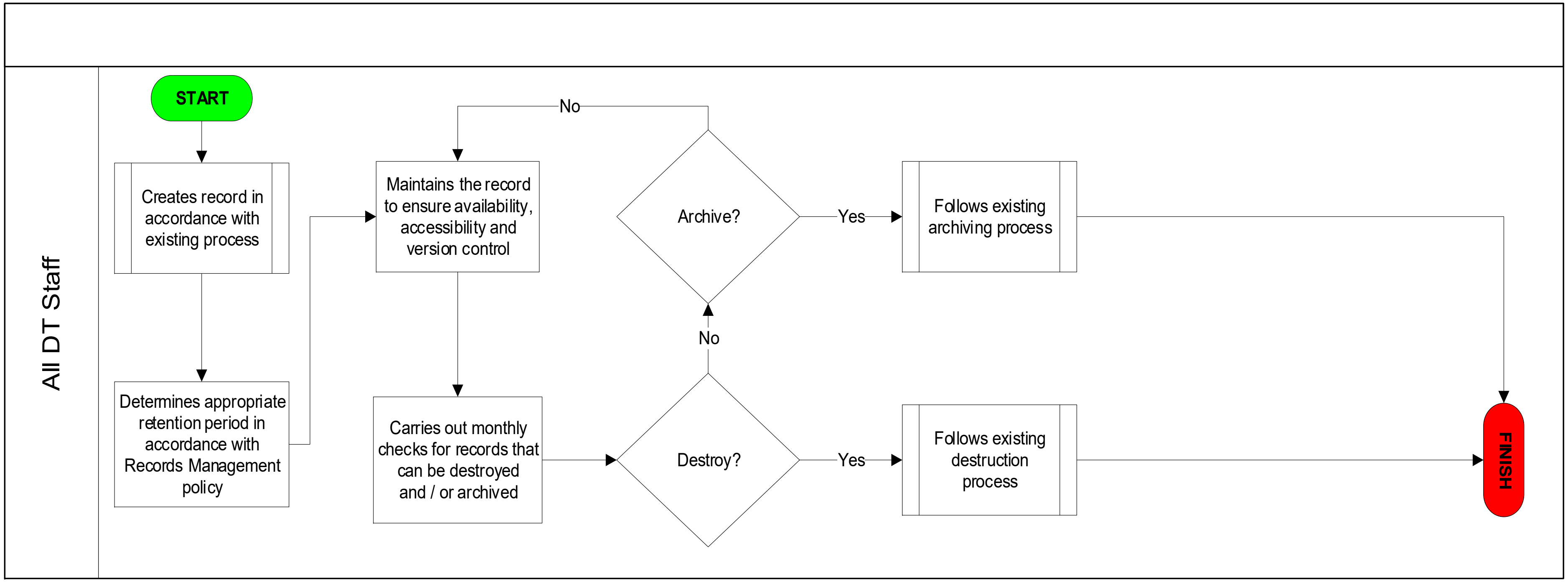
Appendix G

Process Flow: Retrieving Archived Paper Records in Storage


All DT Staff
START
Requires access to paper records currently in external storage
Yes
Authorised user known?
Yes
Contacts appropriate authorised user for assistance
Authorised user follows existing process for retrievals
FINISH
No
Check Records Management section on the intranet for details

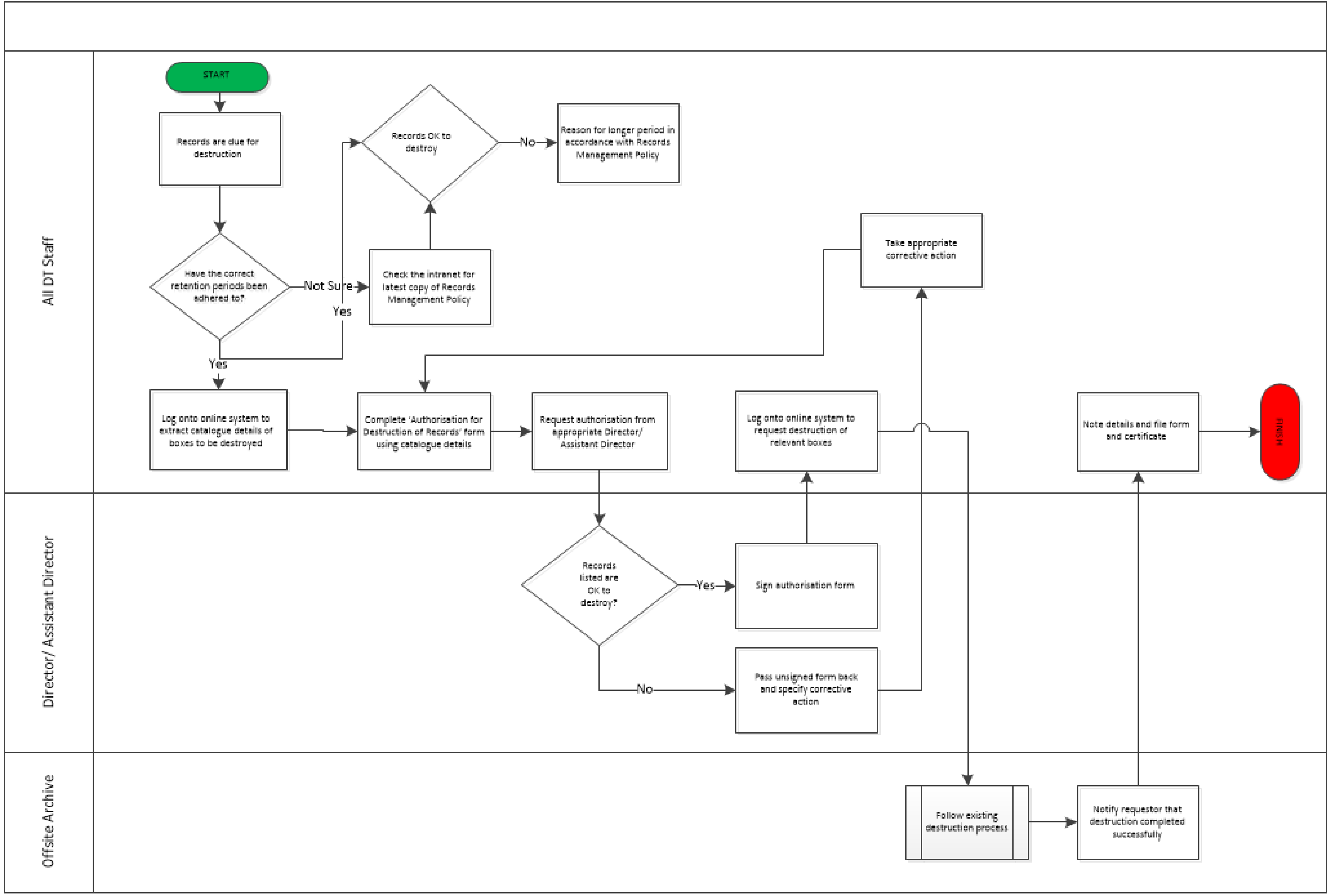
Appendix H

Process Flow: Retaining Records


All DT Staff
START
Creates record in accordance with existing process
Determines appropriate retention period in accordance with Records Management policy
Maintains the record to ensure availability, accessibility and version control
Carries out monthly checks for records that can be destroyed and / or archived
No
Archive?
Yes
No
Destroy?
Yes
Follows existing archiving process
Follows existing destruction process
FINISH

Appendix I

Process Flow: Step by Step Guide to Disposing of Records


All DT Staff
Director/ Assistant Director
Offsite Archive
START
Records are due for destruction
Have the correct retention periods been adhered to?
Not Sure
Yes
Yes
Check the intranet for latest copy of Records Management Policy
Records OK to destroy
No
Reason for longer period in accordance with Records Management Policy
Take appropriate corrective action
Log onto online system to extract catalogue details of boxes to be destroyed
Complete 'Authorisation for Destruction of Records' form using catalogue details
Request authorisation from appropriate Director/ Assistant Director
Log onto online system to request destruction of relevant boxes
Note details and file form and certificate
FINISH
Records listed are OK to destroy?
Yes
Sign authorisation form
No
Pass unsigned form back and specify corrective action
Follow existing destruction process
Notify requestor that destruction completed successfully