Records Management Policy

Table of Contents

Summary of Key Points

- The Old Needleworks Foundation (the organisation) is dependent on its records to operate efficiently and to account for its actions. This policy defines a structure for the organisation to ensure adequate records are maintained, managed and controlled effectively and at best value, commensurate with legal, operational and information needs.
- This policy is an overarching policy designed to provide all professionals working within the organisation with information on the principles of good documentation and record keeping within their administrative and clinical practice and to ensure consistent standards across professional groups.
- In addition, to complement this policy there is specific guidance for the management of clinical records, for archiving paper records and standard operating procedures containing guidance for processing requests for access to health and corporate records to ensure compliance with General Data Protection Regulation /Data Protection Act 2018.
- Records management, through the proper control of the content, storage, and volume of records, reduces vulnerability to legal challenge or financial loss and promotes best value in terms of human and space resources through greater coordination of information and storage systems, enabling effective access to records when required for effective service user care.

Document Type	Policy
Unique Identifier	IG-001
Document Author	Shaun Tudge (Trustee – Data Protection Officer)
Target Audience	All staff, coaches and counsellors within services delivered by the organisation.
Date Ratified	10/06/2024
Expiry Date	09/06/2027

The validity of this policy is only assured when viewed via the The Old Needle Works Foundation – A hub of Wellbeing

The internet version is the definitive version.

This document has been produced in line with current accessibility guidance. If you require this document in an alternative format, please contact the Team on 01527 69100 or by email to info@theoldneedleworks.co.uk

Version History

Version	Circulation date	Job title of person(s) or name of group circulated to	Brief summary of change
0.1	June 2024	Elaine Grant (Chief Executive) Shaun Tudge (Trustee / Data Protection Officer)	New Policy for the organisation

1. Introduction

The Old Needleworks Foundation (the organisation) is dependent on its records to operate efficiently and to account for its actions. This policy defines a structure for the organisation to ensure adequate records are maintained, managed and controlled effectively and at best value, commensurate with legal, operational and information needs.

This policy is an overarching policy designed to provide all professionals working within the organisation with information on the principles of good documentation and record keeping within their administrative and clinical practice and to ensure consistent standards across professional groups. In addition, to complement this policy there is specific guidance for the management of service user records, for archiving paper records and guidance for processing requests for access to health and organisational records.

The organisation's records are our organisational memory, providing evidence of actions and decisions and representing a vital asset to support our daily functions and operations. They support policy formation and managerial decision-making, protect the interests of the organisation and the rights of service users, staff and members of the public who have dealings with us. They support consistency, continuity, efficiency, and productivity and help us deliver our services in consistent and equitable ways.

2. Purpose of Document

- An effective records management policy ensures that such information is properly managed and available to support:
- Service user care
- The day-to-day business, which underpins care and service delivery.
- Evidence-based practice
- Management decision-making
- Partnership working
- Legal requirements including General Data Protection Regulation 2016/ Data Protection Act 2018, Access to Medical Records Act 2000 and Freedom of Information Act 2000
- Organisational and miscellaneous audits
- Improvements in service delivery through research
- Organisational Governance
- Reduction in aspects of risk

- Records management, through the proper control of the content, storage, and volume of records, reduces vulnerability to legal challenge or financial loss and promotes best value in terms of human and space resources through greater coordination of information and storage systems.

3. Definitions

Data Protection Officer – a person who ensures, in an independent manner, that an organisation applies the laws protecting individuals' personal data.

Senior Manager – a person who is either the Chief Executive Officer or Manager

Data Security and Protection Toolkit - an online self-assessment tool provided by NHS Digital that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. All organisations that have access to NHS patient data and systems must use this Toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

Data Subject – an identifiable natural person, a person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Duty of Confidence - a duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It arises from common law.

General Data Protection Regulation (GDPR) - A regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area.

Information Governance – a combination of legal requirements, policy and best practice designed to ensure all aspects of information processing are conducted appropriately, confidentially, securely and to the highest standards.

Personal Data Breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Third Party(ies) or Contractor(s) – applies to any person(s) undertaking work for or on behalf of the The Old Needleworks Foundation such as wellbeing coaches, counsellors and volunteers.

4. Scope

This policy relates to all service records. Service records are defined as information, created or received in the course of business, and captured in a readable form in any medium, providing evidence of the functions, activities and transactions. They include:

- Administrative records (including personnel, estates, financial and accounting records, contract records, litigation and records associated with complaint-handling)
- Service user records, including those concerning all speciality services within the organisation.
- Audio and video tapes, cassettes, CD's
- Records in all electronic formats e.g. email, electronic service user records

All records created in the course of the business of the organisation are corporate records and are public records under the terms of the Public Records Acts 1958 and 1967. This includes electronic messages such as email, text messages and WhatsApp messages.

The organisation must ensure that it adheres to all legislation and guidance in relation to Records Management. The organisation should:

- Ensure there are strict guidelines in the formation of records and information, whether it is manual or computerised.
- Maintain, archive and track these records to ensure their use and validity.
- Ensure all procedures and policies in relation to the completion of records are regularly updated and staff are suitably trained with new updates.
- Store and preserve records in an environment where they are not susceptible to damage or destruction.
- Dispose of unwanted records, ensuring correct procedures are in place to uphold confidentiality. An unwanted record is classed as a record no longer required under retention guidelines.
- Comply with and ensure all organisational employees, coaches and counsellors know the importance of security and confidentiality of information and records by offering training in our services.
- Understand and comply with legislation and keep up to date on current issues relating to records management.

This document will provide guidelines for the creation, maintenance, archiving and disposal of records. The chief executive and trustees should ensure there are local procedures in place for employees, coaches and counsellors work in line with this document. This policy highlights the need for accurate record keeping, the secure storage of records and the relevant disposal of records once they have exceeded their retention period.

In addition to this policy, all employees, coaches and counsellors working for and behalf of the organisation, should adhere to other organisational record keeping guidance, and in particular the guidelines laid down by appropriate professional regulatory bodies.

This policy is mandatory for all employees, coaches and counsellors working within the organisation.

5. Training/Competencies

All employees, coaches and counsellors are responsible for ensuring they complete annual mandatory Information Governance Awareness training as this covers relevant data protection and confidentiality requirements.

- Every employee's, coach's, and counsellor's Service Level Agreement clearly identifies individual responsibilities for compliance with information governance requirements – i.e. legislation, regulations, common law duties and professional codes of practice.
- To further encourage integration of the management of risk throughout the organisation, it is the responsibility of all staff to consider risks around Records Management and notify the Chief Executive. Where appropriate, the issues will be identified within the organisational Risk Register and rectifying action taken.

6. Responsibilities and Duties

Board of Trustees

- Setting policy for the organisation through powers delegated to the trustees.
- Ensuring policy is implemented through agreed management arrangements.
- Ensuring they are alerted to relevant issues arising that may affect policy.

Chief Executive

- Ensuring that arrangements are in place so that employees, coaches, and counsellors are fully aware of their statutory, organisational and professional responsibilities and that they are fulfilled.
- Ensuring that the arrangements in support of policy are fully implemented through inclusion in work stream reviews.
- For this responsibility to be effectively discharged, Trustees and senior colleagues will have specific delegated responsibility to support the Chief

Executive in this process. The Chief Executive has delegated responsibility for records management and archiving to the trustee – Data Protection Officer.
- The quality of records management across the organisation and work streams delivered.

Responsibility of all Employees

- All employees, coaches, and counsellors are responsible for any records they may create or use. This responsibility is established and defined by the law. Any records created by employees are public records.
- They must ensure that the records are kept up-to date and in good condition to have any real value to the organisation.
- Every person working for, or within the organisation, who records, uses, stores or otherwise comes across information, has a personal common law duty of confidence as well as adhering to the GDPR / DPA 2018.
- Personal information (e.g. about an employee or service user) processed or left for any purpose should not be kept for any longer than is necessary for that purpose.
- Service user / personal information must be processed in accordance with the requirements of the GDPR / DPA18 and the common law duty of confidentiality. Further details can be found in the organisation's Data Protection and Confidentiality Policy.

Personal / Professional Integrity

All The Old Needleworks Foundation staff have a legal duty of care; record keeping should be able to demonstrate:

- A full account of all assessments and the care planned and provided.
- Relevant information about the condition of the service user at any given time and the measures taken to respond to their needs.
- Evidence that the duty of care has been understood and honoured and that all reasonable steps to care for the service user have been taken and that any actions or omissions have not compromised their safety in any way.

Professionals are accountable for ensuring that any duties, which they delegate to volunteers, are undertaken to a reasonable standard. For instance, if a professional delegates record keeping to a volunteer, they must ensure that they are adequately supervised and that they are competent to perform the task and work to locally agreed protocols.

Professionals are accountable for the consequences of entries made by unqualified

members of staff or volunteers.

.

Responsibilities of Third Parties

Anybody undertaking work for or with the organisation such as employees, coaches, and counsellors, volunteers, and visiting maintenance craftsmen must have contracts that detail the obligations on confidentiality and restrictions on the use of personal information, including those specified by The Old Needleworks Foundation Records Management Policy and the GDPR / DPA18. The contract must require that service user information is treated and stored accordingly, and is used only for purposes consistent with the terms of the contract. Action that will be taken in the event of confidence being breached (e.g. termination of contract) should be specified within the contract.

7. Policy/Guideline

7.1 Legal and professional obligations

All records are accessible Public Records under the Public Records Acts and must be kept in accordance with statutory guidance, in particular:

- Public Records Acts 1958 and 1967
- European Union General Data Protection Regulation / Data Protection Act 1998 (GDPR / DPA18)
- Freedom of Information Act 2000
- The Caldicott Principles
- Care Quality Commission
- Audit Commission, Setting the Record Straight, 1995
- Common Law Duty of Confidentiality
- Independent Inquiry into Child Sexual Abuse (IICSA) 2016

Where records are to be shared with other organisations (e.g. social services) this must be done in accordance with documented and agreed information sharing protocols.

7.2 Policy objectives

The main objectives of this policy are:

Accountability – that adequate records are maintained to account fully and transparently for all actions and decisions in particular:

- To protect legal and other rights of staff or those affected by those actions.
- To facilitate audit or examination.
- To provide credible and authoritative evidence.

Quality – that records are complete and accurate and the information they contain is reliable and its authenticity can be guaranteed.

Accessibility – that records and those with a legitimate right of access can efficiently retrieve the information within them, for as long as the records are held by The Old Needleworks Foundation.

Security – that records will be secure from unauthorised or inadvertent alteration or erasure, that access and disclosure will be properly controlled, and audit trails will track all use and changes. Records will be held in a robust format, which remains readable for as long as records are required.

Retention and disposal – that there are consistent and documented retention and disposal procedures to include provision for permanent preservation of archival records.

Training – that all staff are made aware of their record-keeping responsibilities through generic and specific training programmes and guidance.

In addition, this policy aims to provide guidance on:

Performance measurement – that the application of records management procedures is regularly monitored against agreed indicators and action taken to improve standards as necessary.

Records are available when needed – from which the organisation 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 can be interpreted – the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records.

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, that access and disclosure are properly controlled, and audit trails will track all use and changes. To ensure that 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.

Staff are trained – so that all staff are made aware of their responsibilities for record-keeping and record management in line with the GDPR/DPA18 which seta out the legal requirements and duties placed on all Data Controllers (i.e. the organisation) and Data Processors when processing personal information.

7.3 Setting an organisational standard aligned to NHS standards.

A systematic and planned approach to the management of records within the organisation, from the moment they are created to their ultimate disposal, ensures that the organisation can:

- Control both the quality and the quantity of the information that it generates.
- Dispose of the information efficiently when it is no longer required. This applies to all records whether manual or computerised.

Records are valuable because of the information they contain, and that information is only usable if:

- It is correctly and legibly recorded in the first place.
- It is then kept up to date.
- It is easily accessible when needed.

Good record keeping ensures that:

- Employees work with maximum efficiency without having to waste time hunting for information.
- There is an ‘audit trail’, which enables any record entry to be traced to a named individual at a given date/time with the secure knowledge that all alterations can be similarly traced.
- New staff can see what has been done, or not done, and why.
- Any decisions made can be justified or reconsidered at a later date.
- Good Records Management is essential for:
- Providing high quality service delivery
- Continuity of care

- Effective communication and dissemination of information
- An accurate account of continuous assessment, service delivery and evaluation
- The ability to detect problems, such as changes in the client's circumstances or condition at an early stage
- Corporate memory
- Historical purposes
- Purchasing and contract service agreement management
- Financial accountability
- Disputes or legal action

It is therefore important to ensure:

- Important and relevant information is recorded and completed
- Handwritten records are legible, written in black ink, and can be easily read and reproduced when required
- Information/records are easily accessible and kept up to date
- Personal identifiable information is shared rather than copied to reduce risks to confidentiality
- Records are disposed of as soon as possible subject to national and local retention periods (Records Management Code of Practice for Health and Social Care 2016) or locally determined retention periods
- Records are shredded or disposed of in line with The Old Needleworks Foundation procedure

A systematic and planned approach to the management of records within the organisation, from the moment they are created to their ultimate disposal, ensures that the organisation can:

- Control both the quality and the quantity of the information that it generates.
- Maintain the information in a manner that effectively services its needs, those of government and of the citizen.
- Dispose of the information efficiently when it is no longer required. This applies to all records whether manual or computerised.

Records are valuable because of the information they contain, and that information is only usable if:

- It is correctly and legibly recorded in the first place.
- It is then kept up to date.

- It is easily accessible when needed.

Good record keeping ensures that:

- Employees, coaches, and counsellors and volunteers, work with maximum efficiency without having to waste time hunting for information,
- There is an ‘audit trail’, which enables any record entry to be traced to a named individual at a given date/time with the secure knowledge that all alterations can be similarly traced.
- Employees, coaches, and counsellors can see what has been done, or not done, and why.
- Any decisions made can be justified or reconsidered at a later date.

Good Records Management is essential for:

- Providing high quality service provision
- Continuity of care
- Effective communication and dissemination of information between employees, coaches, counsellors and volunteers and members of external multi-disciplinary health and social care teams
- The ability to detect problems, such as changes in the service user’s condition or circumstances, at an early stage.
- Corporate memory
- Clinical liability
- Historical purposes
- Purchasing and contract service agreement management
- Financial accountability
- Disputes or legal action

It is therefore important to ensure:

- Important and relevant information is recorded and completed.
- Handwritten records are legible, written in black ink, and can be easily read and reproduced when required.
- Information/records are easily accessible and kept up to date.
- Personal identifiable information is shared rather than copied in order to reduce risks to confidentiality.

- Records are disposed of as soon as possible subject to national and local retention periods (Records Management Code of Practice for Health and Social Care 2016) or locally determined retention periods.
- Records are shredded or disposed of in line with the organisation's procedure.

What needs to be done to achieve best standards?
All employees need to ensure that staff are aware of their personal responsibilities under the GDPR / DPA 18 and familiar with the organisation's procedures for access to service user information.
Senior staff should ensure that staff are suitably trained in record keeping, security and storage of information/records (manual and computerised).

Records may be required as evidence:

- Before a Court of Law
- The Health Service Ombudsman
- The Information Commissioner
- In order to investigate a complaint at a local level
- By Professional Conduct Committees e.g. NMC, which considers complaints about professional misconduct.

7.4 Creating records and record keeping standards.

A record, whether it is in paper format or electronic, is a structured document which contains information, which has been created or gathered as a result of any aspect of the work of the organisation's employees, coaches and counsellors. These records must be continually updated to ensure their validity and use, unless the information contained in the record becomes obsolete.

All records should have a unique file name or number and be part of a structured filing system. For example:

A service user's record will be identifiable by their allocated number.
An employee's personal file must be identifiable by the personnel number.
All records must have clear and precise formats.

They must be structured in the same way that files of the same description are structured with an easy-to-follow standardised index (either numerical, by date or

alphabetically), so that information can be retrieved quickly and easily (for example all service user and employee files).

Senior staff should ensure that this is the practice within their own departments and relevant guidance is in place.

Updating Records
Senior staff should ensure that all records are regularly updated and maintained in a practical order.

Employees, coaches, and counsellors should be vigilant when storing both electronic and paper files, to ensure their confidentiality, security and availability.

Records which are no longer required should be considered for archiving or disposal, depending on their statutory minimum retention period.

For paper records, regular checks on the status of the record container, whether it is a binder, paper folder or box file, should be undertaken to ensure no damage has occurred, or if it has, to replace it quickly before it is further damaged.
Concise and easy to follow procedures, whether they are paper or electronic systems, should back up all record keeping practices.

Senior staff should ensure all staff are correctly trained.

7.5 Records storage and retrieval.

The organisation has a responsibility for ensuring the effective and efficient operation of all storage facilities within the organisation. This includes the safekeeping, accessibility and retention of records for as long as required, the transfer of those records selected for permanent preservation, and the timely destruction of records no longer required. Storage should also be in a suitable environment, which has easy access and appropriate safety to ensure the records are not damaged or destroyed. All records storage areas should meet with Health and Safety requirements.

7.6 Confidentiality and accessing records.

Levels of confidentiality bind all employees, coaches, counsellors and volunteers. Senior staff must ensure that all staff are trained in data protection and are aware of the implications if confidentiality is breached. The impact of a breach of confidentiality could be any of the following:

- Threat to personal safety or privacy
- Embarrassment for the organisation and possibly external partners.
- Legal obligation or penalty
- Financial loss
- Disruption of activities and provision of patient services

The organisation is committed to multi-disciplinary working procedures, and this requires all key professionals to work together and share information, to the benefit of the service user. Service users have an expectation that information held relating to them is confidential and will be held securely.

7.7 Sharing information with other health and social care providers – Continuity of Care.

All health and adult social care providers are subject to the statutory duty under section 251B of the Health and Social Care Act 2012 to share information about service users for their direct care. This duty is subject to the GDPR, the DPA18 and the Common Law Duty of Confidentiality. This will apply when sharing information about a service user with another health care provider for continuity of care purposes.

For common law purposes, sharing information for direct care is based on implied consent, which may also cover administrative purposes where the service user has been informed or it is otherwise within their reasonable expectations that their personal information will be shared.

Under the GDPR, for the processing of personal data in the delivery of direct care and for administrative purposes, the Article 6 condition for lawful processing that is available to all publicly funded health and/or statutory health and social care organisations in the delivery of their functions is:

- 6(1)(e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…'

Personal Data Concerning Health is a special category of personal data; the most appropriate Article 9 condition under the GDPR for direct care and for administrative purposes is:

- 9(2)(h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems'

These conditions will also be the most appropriate basis for local administrative purposes such as: activity monitoring, local clinical audit and local clinical supervision.

7.8 Sharing information with other health and social care providers – Continuity of Care.

Whilst the original record remains the property of the originating organisation, there will be occasions where the organisation is asked to share all or parts of the record with another party, in some cases the service user. The organisation is obliged by the General Data Protection Regulation / Data Protection Act 2018 to process these requests within one calendar month. The organisation has an 'Access to Records Request' process for staff to follow to deal with such requests and a standard operating procedure (SOP) has been developed to guide staff through the various stages of managing requests. See Subject Access Request – Standard Operating Procedure for detailed guidance on how to manage, process and deal with these requests in a timely manner.

7.9 Disposal of records.

The length of the retention period depends upon the type of record and its importance to the business and services of the organisation. The Information Governance Alliance Records Management Code of Practice for Health and Social Care 2021 gives guidance on the retention and disposal of records (see summary in Appendix A). There may be additions to or deletions from the schedule to suit the needs of the organisation.

Process for disposal
The organisation holds an inventory for all records stored, which identifies all records, their date of creation, and where they are stored.

It is the responsibility of the senior managers to identify the records, which may be appropriate for review.

The process of deciding what to do with records when their business use has ceased is called review. No record or series can be automatically destroyed or deleted.

Once the records have been identified, then the decision should be made by the relevant chief executive officer in discussion with the data protection officer what to do:

Steps to follow when reviewing records for disposal:

- Has the service user re-engaged into support since the paper record you are appraising for disposal. If so, you need to make a note of the date last seen, as this is the commencement date when calculating most retention periods.
- Do the records relate to a deceased/living patient as different retention periods can apply if service users are deceased?
- Are the records likely to pose a high or low risk of being required for any enquiry e.g. the Independent Inquiry into Child Sexual Abuse 2016 Inquiry?

- Has the minimum retention period been reached, please refer to the organisation's Records Management Policy – Retention & Disposal Schedule, and is there any reason why this should be extended?

There will be one of three outcomes from review:

- Destroy / delete records.
- Keep for a longer period.

If because of review, a decision is made to destroy a record there must be evidence of the decision. **See Appendix B TONF / Records Inventory.**

- Records should be destroyed completely if there is no reason to retain for a longer retention period.
- The scanning option may be beneficial in some cases if the record needs to be retained for a longer retention period as the destruction of paper records is irreversible and cannot be rectified later.
- A list should be kept indefinitely of all disposed of records for audit purposes (Appendix B).

For all archived records the chief executive officer must sign the disposal of records list (Appendix B) to confirm that the destruction of the records is approved, and the details of the actual disposal date must be countersigned by the data protection officer for records management and retained for future reference by the organisation and Audit. The Board of Trustees should be updated on a six-monthly basis.

Schedule for retention

The Information Governance Alliance Records Management Code of Practice for Health and Social Care 2021 has a suggested schedule showing the minimum retention periods for records held by the organisation (Appendix A).

7.10 Confidentiality and security of records.

Everyone working for or with the organisation who records, handles, stores or otherwise accesses patient information has a personal common law duty of confidence to service users and to their employer.
The guidelines contained within this policy underpin the principles of the GDPR / DPA18 and ensures that personal information is accurate, up to date and retrievable in a timely manner.
The organisation must also ensure that information is shared “on a need to know” basis and that it is continuously improving confidentiality and security procedures governing access to and storage of clinical information.
Senior managers must ensure that all staff are made aware of their responsibilities regarding confidentiality and security of records. Support and guidance can be provided by the organisation’s Data Protection Officer.

8. Monitoring Implementation

This Policy will be reviewed every three years, or earlier if appropriate, to take into account any changes to legislation that may occur, and/or guidance from the Department of Health and Social Care and/or the Information Commissioners Office.

9. References

- General Data Protection Regulation 2016
- Data Protection Act 2018
- Access to Health Records Act
- Access to Medical Records Act 2000
- Freedom of Information Act 2000
- Public Records Acts 1958 and 1967
- Mental Health Act
- Records management Code of Practice for Health & Social Care 2021

10. Associated

11. Documentation

- Subject Access Request Standard Operating Procedure

12. Appendices

Appendix A – Brief Summary of Retention and Disposal Periods for key documents and records

Type of Record – Health Records	Minimum Retention Period	Notes
Referral forms for support and corresponding session notes including WEMWBS scores	8 years after conclusion of service or death. Check for any other involvement that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions.	All must be reviewed prior to destruction talking into account any serious incident retentions or requirements of the IICSA Inquiry
Group registers and sign in books	8 years after conclusion of service. Check for any other involvement that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions	To be reviewed prior to destruction
Records relating to learners attending TONF courses	8 years after conclusion of service. Check for any other involvement that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions	To be reviewed prior to destruction

Risk Assessment Records	Retain the latest risk assessment until it is superseded	Destroy under confidential conditions

Type of Record – Corporate Records	**Minimum Retention Period**	**Notes**
Accident forms and Register	10 years if not serious incidents	Destroy under confidential conditions
Agendas of board meetings, committee, sub-committees (master copies, including associated papers)	Open Board Meetings – Transfer to a Place of Deposit before 20 years as soon as practically possible. Closed Board Meetings – Transfer to a Place of Deposit after 20 years.	FOI exemptions should be noted or duty of confidence indicated
Agendas (other)	2 years	Destroy under confidential conditions
Annual/Corporate reports	3 years, except final annual accounts reports which should be transferred to a Place of Deposit as soon as practically possible with Board Papers.	
Business plans, including local delivery plans	Life of the organisation plus 6 years.	
Complaints Correspondence, investigation and outcomes	10 years from completion of action.	Destroy under confidential conditions
Health and Safety documentation	6 years	Review and destroy under confidential conditions
History of organisation or predecessors, its organisation and procedures (e.g. establishment order)	Life of organisation plus 6 years.	
Incident forms non serious Incident forms - serious	10 years from the date of non-serious incidents 20 years from the date of serious incidents.	Destroy under confidential conditions

Manuals – policy and procedure (administrative and clinical, strategy documents)	10 years after life of the system (or superseded) to which the policies or procedures refer	Destroy (policies may have archival value)
Meetings and minutes papers of Trustees (master copies)	Before 20 years but as soon as practically possible.	
Service user Surveys (re access to services)	2 years	Destroy under confidential conditions
Press Releases	6 years	
Quality assurance records (e.g. regulatory, NHS partners, Lottery, Investors in People)	12 years	Destroy under confidential conditions
Receipts for registered and recorded mail	2 years following the end of the financial year to which they relate	Destroy under confidential conditions
Reports (major)	30 years	Likely to have archival value
Subject Access Requests– records of requests	3 years after closure of SAR. 6 years after closure where there has been a subsequent appeal.	Review and destroy under confidential conditions

Type of Record – Financial Records	Minimum Retention Period	Notes
Accounts – annual (final – one set only)		Transfer to a Place of Safety
Accounts – minor records (pass books, paying-in slips, cheque counterfoils, cancelled/discharged cheques (for cheques bearing printed receipts, see Receipts), accounts of petty cash expenditure minor vouchers, duplicate receipt books, income records, laundry lists and receipts) travel and subsistence accounts,	2 years from completion of audit Close of financial year 6 years.	 Review and confidentially destroy
Audit reports – internal and external (including management letters, value for money reports and systems/final accounts memoranda)	2 years after formal completion by statutory auditor	Review and confidentially destroy
Contracts – financial	Approval files – 15 years, Approved suppliers lists – 11 years	Review and confidentially destroy
Invoices	6 years after end of financial year to which they relate	Review and confidentially destroy
Payments	6 years after year end	Review and confidentially destroy

Type of Record – Personnel Records	Minimum Retention Period	Notes
Job advertisements	Retain on the personal file of the successful candidate in line with staff record summary retention periods.	Review and confidentially destroy
Job applications (successful)	Keep until 75th birthday, or 6 years after cessation of employment if aged over 75 years at the time	Review and confidentially destroy
Job applications (unsuccessful)	1 year	Review and confidentially destroy
Job descriptions	Retain on the personal file of the successful candidate in line with staff record summary retention periods.	Review and confidentially destroy
Leavers' dossiers (Staff Record Summary)	6 years after individual has left Summary (see Code of Practice for Health and Social Care 2021) to be retained until individuals 75th birthday, or 6 years after cessation of employment if aged over 75 years at the time.	Review and confidentially destroy
Letters of appointment	6 years after individual has left Summary to be retained until individuals 75th birthday, or 6 years after cessation of employment if aged over 75 years at the time.	Review and confidentially destroy
Pension forms (all)	Although pension information is routinely retained until 100th birthday by the NHS Pensions Agency employers must retain a portion of the staff record until the 75th birthday.	Review and confidentially destroy
Personnel/human resources records – major (e.g. personal files, letters of	6 years after individual leaves service, at which time a summary of the file must be	Review and confidentially destroy

appointment, contracts, references and related correspondence, registration authority forms, training records, equal opportunity monitoring forms (if retained)	kept until the individual's 75th birthday Summary should be retained until individuals 75th birthday or until 6 years after cessation of employment if aged over 75 years at the time. (see Code of Practice for Health and Social Care 2021)	
Personnel/human resources records – minor (e.g. attendance books, annual leave records, duty rosters, clock cards, turnaround)	2 years	Review and confidentially destroy
Timesheets	2 years	Review and confidentially destroy
Training Records	Records of significant training must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member's role. The IGA recommends: **Clinical training records** - to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer **Statutory and mandatory training records** - to be kept for ten years after training completed **Other training records -** keep for six years after training completed	Review and confidentially destroy

Appendix B – TONF / Records Inventory

Example:

The Old Needleworks Foundation / Records Inventory List - REFERENCE									
Surname	Forename	Date of Birth	NHS Number / TONF Reference	Volume Number	Storage Reference / Box Number	Deceased?	Actual Date Patient Last Seen	Actual Date Retention Expiry Date	Retention Expiry Date (Mth / Year) (Based on Last Seen Date)

TONF_Inventory%20Records%20Log_V(