

Title	A01 Record Keeping and Document Retention
Version Number	2.0
Last reviewed	April 2025
Last amended	April 2025
Next review	January 2026
Author	Mark Wheatley

A01 - RECORD KEEPING AND DOCUMENT RETENTION

This statement is a written record that demonstrates that we have shown due regard to the need to eliminate unlawful discrimination, advance equality of opportunity and foster good relations with respect to the characteristics protected by equality law.

Section 1 - Purpose

The Moorview Care Record Keeping Policy relates to the safekeeping of all records from their creation to disposal.

This policy will ensure that client and personnel records are properly created, of good quality, accessible and available for use and that they are disposed of in a secure and timely fashion. It provides team members with guidance regarding individual responsibility for accuracy and appropriate storage of records.

To support the meeting of the Quality Statements:

Key Questions	Quality Statements
EFFECTIVE	QSE2: Delivering evidence-based care and treatment QSE3: How team members and services work together
EFFECTIVE	QSE3: How team members and services work together
SAFE	QSS3: Safeguarding
WELL LED	QSW5: Governance, Management and Sustainability

Relevant legislation:

- Freedom of Information Act 2000
- The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- Access to Health Records Act 1990
- Data Protection Act 2018
- UK GDPR

- ~~Nursing and Midwifery Council (NMC) Legislation~~
- Common Law Duty of Confidentiality
- Public Records Act 1958
- ~~Section 123 and 124 of the Police Act 1997~~

Section 2 - Scope

This policy includes in its scope all data which we process either in hardcopy or digital copy and covers employees, clients and external parties.

Section 3 - Objectives

To enable Moorview Care to ensure that its data retention and data security policies are UK GDPR compliant.

To enable team members in whatever capacity they have in regard to record keeping to work according to best practice principles and within the law.

To support the development of clear accountability and establish effective working practices through improved record keeping and the use of documented communication systems.

To support the effective evaluation, review, clinical audit, research, resource allocation and performance planning through improved management and recording of information

To ensure that records are disposed of, stored and archived in line with regulation and legislation.

- UK General Protection Regulation
- Records Management Code of Practice 2021
- ICO Employment Practices Codes of Practice
- NHS Data Security and Protection Toolkit

To ensure team members understand their responsibilities regarding the storage of personal information and the importance of maintaining it in line with regulations, best practice and insurance requirements. Section 4 - Policy

Section 4 - Policy

We are committed to the continuous improvement of our records management systems, recognising the significant organisational benefits this brings. These include:

- More efficient use of physical and digital storage space,
- Better allocation of team time,
- Enhanced control over valuable information assets,
- Compliance with legal and regulatory standards,
- Accurate maintenance of a Data Asset Information Register
- Overall cost reduction

All records will be archived and stored securely, in accordance with statutory, regulatory and insurance requirements. Documents will be easily retrievable and accessible only to authorised personnel, in line with the procedures outlined in this policy. Disposal of records,

documents and other media will be carried out in a manner that ensures confidentiality is maintained.

All team members will be made aware of their responsibilities regarding the storage, archiving and management of documents during induction and will receive ongoing reminders through training and regular updates. Any security breaches related to archiving, storage or disposal will be fully investigated and reported in accordance with our policies and procedures

The Data Protection Act

The Data Protection and Security policy A02 outlines the requirements relating to the correct and lawful treatment of personal data and should be read in conjunction with this policy.

Under Article 5 of the GDPR, the principles require that personal data shall:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you, and not used in a way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

This means deleting from Google Drive, or shredding hard copies, of any personal data that is no longer needed, inaccurate or out-of-date in line with section 8 of this policy.

Data Quality

Good quality, accurate records are vital for the safety of our clients and the safe and responsible running of the organisation.

When a record is created or updated it is important to ensure the information entered has the following characteristics:-

- a) It is authentic – i.e. the data is what it claims to be. You can make sure it is authentic by properly signing off records you have updated with your name and marking the time and date.
- b) It is reliable – You should make sure you record data which is complete and accurate and that you write it down as soon after the (or during) the event as possible.
- c) It has integrity – If you need to change and information, make sure that it is clearly marked and that you can be identified as the person who has changed the record.

- d) It is useable – Make sure that records are stored correctly according to the local procedure for hard copy and the Electronic Filing procedure for digital records

Section 5 - Procedure

Record keeping procedures – creation and use of records

When we create records, we use standardised structures and layouts for the contents of records.

All records are kept in accessible but protected locations. The location of these records is documented in the Information Asset Register (IAR). The security procedures around access to records are detailed in the Data Security Policy.

Employee and client records should be stored in the individual's file in a locked drawer or cabinet or in the electronic file.

Hard copy files should contain the items listed on the file index. Where documents are replaced annually only the most up to date should be kept in the file. Documents being removed should be scanned and kept in the electronic file.

Records are only retained while they are necessary for the purposes for which they were originally collected. We will ensure that all records are retained and destroyed in-line with the Retention and Disposal Procedures detailed within this document.

We will audit our record keeping procedures annually to ensure that they are adequate and continue to keep our records to the highest standards.

Information handling procedures

Information handling procedures ensure that personal information is protected and that it is not disclosed inappropriately, either by accident or design, whilst in use or when it is being transferred.

In line with Data Protection legislation, personal information is not processed without a lawful basis being identified. The Record of Processing Activities (ROPA) records all processing of personal data and identifies the legal basis for it being processed.

Retention schedule and disposal procedures

We will adhere to the retention timelines determined by the Information Governance Alliance (IGA) in Appendix 3 of Records Management Code of Practice for Health and Social Care 2016.

At the end of their lifespan, the records will go through an appraisal process. This process will determine if there is a continuing legal basis for keeping the record. The Data Protection Lead will have final responsibility for determining whether the record will be destroyed or retained. A record will be maintained of all retention or disposal decisions.

In the instance that hard copy records are destroyed, this will be by using secure disposal containers supplied by an approved, secure destruction service.

Storage periods for electronic files are the same as for paper documents. Old documents should be moved into the archive section in each electronic file until the required destruction date.

Fig 1 – Retention Schedule

Document Type	Retention Period
PERSONNEL	
Maternity, Paternity & Adoption Leave	3 years
Parental Leave	18 years from date of birth of the child or 6 years after leave date – whichever is less
Application Forms & interview notes of unsuccessful applicants	6 months
DBS Disclosures	Up to 6 months at Head Office only – must not be kept locally
DBS Disclosure Seen form EP 05	3 years or until renewed
Personnel Files	6 years after employment ceases
Training Records	6 years after employment ceases
Disciplinary and Capability Records	6 years after employment ceases

Formal Warnings	Until warning expired, then retained in personnel file as spent for 6 years after employment ceases
Redundancy	6 years from date of redundancy
Life Assurance expression of wish forms	6 years after employment ceases or death
Duty Rosters	6 years after the date to which they relate
Records relating to Working Time	2 years from date on which they were made
Employee Files	6 years from leave date
FINANCE	
Accounting documents (Limited Company)	7 years
VAT Records	7 years
Tax Records	7 years
Payroll Records to include timesheets, sick pay	7 years
Customers financial records & audits	3 years after they have left
Timesheets and expenses	6 years (File alphabetically within each month)
HEALTH & SAFETY	

Serious Accident reports (where person injured)	5 years For under 18's, 5 years after their 18 th birthday
Accident reports/ incident reports HS03	5 years from last entry or end of investigation if later
Incidents notified to CQC	3 years
CLIENTS	
Client files	8 years from leave date
Any social care records for adults	8 years from leave date
FUNDRAISING (AHMT)	
Records relating to Gift Aid	6 years
GOVERNANCE	
Board Meeting Minutes	10 years
GENERAL	
Records relating to any Litigation	3 years after settlement
Contracts	6 years
Employer's Liability Certificates	40 years
Audit Records	5 years
Subject Access Requests	3 years