

Title	A01 Record Keeping and Document Retention
Version Number	3
Last reviewed	11/06/26
Last amended	11/06/2026
Next review	June 27
Author	Mark Wheatley reviewed by J Walker

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 should be used in conjunction with the following policies:

1. A-02 - Data Security and Protection
2. A-03 - Data Breach
3. A-05 - Clear Desk
4. A-06 - Cyber Security
5. A-07 - Caldicott Guardian
6. A-10 CCTV and Digital Capture.

This policy will ensure that the people we support 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

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
- Common Law Duty of Confidentiality
- Public Records Act 1958

Section 2 - Scope

This policy includes in its scope all data which we process either in hard or digital copy and covers team members, the people we support 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 regarding 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 regulations 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

4.1 Data Retention

As a general principle, Moorview Care will not keep (or otherwise process) any personal data for longer than is necessary. If we no longer require the personal data once we have finished using it for the purposes for which it was obtained, we will delete the personal data unless it is required by law to retain the data for an additional period of time.

4.2 We may have legitimate business reasons to retain the personal data for a longer period. This may include, for example, retaining personnel records in case a claim arises relating to personal injury caused by Moorview Care that does not become apparent until a future date. Moorview Care will consider the likelihood of this arising when it determines its retention periods - the extent to which medical treatment is provided by Moorview Care will, for example, affect the likelihood of Moorview Care needing to rely on records at a later date. A link to the NHSX Records Management Code of Practice 2021 is available in the Underpinning Knowledge section. It is a guide in relation to the practice of managing records, with minimum retention periods for different types of records relating to health and care.

4.3 We may be required to retain personal data for a specified period of time to comply with legal or statutory requirements. These may include, for example, requirements imposed by HMRC in respect of financial documents, or guidance issued by UK Visas and Immigration and Immigration Enforcement in respect of the retention of right-to-work documentation.

4.4 Moorview Care understands that claims may be made under a contract for six years from the date of termination of the contract, and that claims may be made under a deed for a period of twelve years from the date of termination of the deed. We will therefore retain contracts and deeds as well as documents and correspondence relevant to those contracts and deeds for the duration of the contract or deed, plus six and twelve years, respectively.

4.5 Moorview Care will consider how long it needs to retain HR records. We have considered separating HR records into different categories of personal data (for example, health and medical information, holiday and absence records, next of kin information, emergency contact details, financial information) and specifying different retention periods for each category of personal data.

Moorview Care recognises that determining separate retention periods for each element of personal data may be more likely to comply with UK GDPR.

The period of time that is appropriate may depend on the likelihood of a claim arising in respect of that team member in the future. If, for example, Moorview Care is concerned that a team member may suffer personal injury as a result of their employment, it may choose to retain its HR records for a significant period of time. If any such claim is unlikely, we may choose to retain files for six or twelve years (depending on whether the arrangement entered into between Moorview Care and the team member is a contract or a deed).

4.6 Moorview Care will consider the following advice and guidelines when deciding how long to retain HR data for. We acknowledge that the suggested retention periods below are based on guidance within relevant legislation and, in some cases, reflect statutory requirements. We may choose to retain records for a longer period of time in case a dispute arises. For example, data that is potentially relevant to pay disputes may be retained for seven years after the team member ends, despite a shorter statutory retention period:

- **Recruitment records** - Six months after notifying candidates of the outcome of the recruitment exercise

- **Immigration checks** - Two years after the termination of employment. Moorview Care may consider retaining for a further year to enable the fact of any dispute to reach the attention of Moorview Care after the statutory two-year period has ended
- **PAYE records** - At least three years after the end of the tax year to which they relate
- **Payroll and wage records for companies** - Six years from the financial year-end in which payments were made
- **Records in relation to hours worked and payments made to workers** - Six years beginning with the day on which the pay reference period immediately following that to which they relate ends
- **Records required by the Working Time Regulations:**
 - Working time opt-out - Three years from the date on which they were entered into
 - Compliance records - Three years after the relevant period
 - Health assessment records for night workers - Three years after the relevant period
- **Maternity records** - Three years after the end of the tax year in which the maternity pay period ends. Moorview Care may consider retaining for a further year to enable the fact of any dispute to reach the attention of Moorview Care after the statutory three-year period has ended
- **Accident records** - At least three years from the date the report was made, or potentially longer if deemed appropriate given the possibility of ongoing relevance of the records. Moorview Care may consider retaining for a further year to enable the fact of any dispute to reach the attention of Moorview Care after the statutory three-year period has ended

4.7 Moorview Care will consider how long it is required to keep records relating to the people being supported. In doing so, Moorview Care will consider the data retention guidelines provided. Moorview Care will determine an appropriate retention policy for the people being supported's personal data. Moorview Care may choose to retain personal data for at least six years from the end of the provision of services to the people being supported, in case a claim arises in respect of the services provided.

4.8 Irrespective of the retention periods chosen by Moorview Care, Moorview Care will ensure that all personal data is kept secure and protected for the period in which it is held. This applies in particular to special categories of data.

4.9 Moorview Care must record all decisions taken in respect of the retention of personal data. If the ICO investigates the policies and procedures at Moorview Care, a written record of the logic and reasoning behind the retention periods adopted must be available.

4.10 Moorview Care will implement processes for effectively and securely destroying and/or deleting personal data at the end of the relevant retention period. Moorview Care will consider whether personal data stored on computers, including in emails, is automatically backed up and how to achieve deletion of those backups or ensure that the archived personal data is automatically deleted after a certain period of time. Moorview Care will also consider circulating guidance internally to encourage team members to regularly delete emails. Moorview Care will introduce policies relating to the destruction of hard copies of documents, including using confidential waste bins or shredding them.

4.11 Data Security

Moorview Care will take steps to ensure that the personal data it processes is secure, including by protecting the personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

4.12 Moorview Care understands that all health and care organisations, as detailed below, are required to comply with the Data Security and Protection Toolkit. A link to an explanatory guidance note is included in the Underpinning Knowledge section. Compliance with the Data Security and Protection

Toolkit facilitates compliance with UK GDPR. Moorview Care understands that all organisations that have access to NHS patient data and systems must use the Data Security and Protection Toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

4.13 Moorview Care will implement and embed the use of policies and procedures to ensure that personal data is kept secure. The suggestions below apply in addition to the steps Moorview Care is required to take pursuant to the Data Security and Protection Toolkit, if the toolkit applies to Moorview Care. Moorview Care will bear in mind the following principles when deciding how to ensure that personal data is kept secure:

- **Confidentiality** - ensuring that personal data is accessible only on a need-to-know basis
- **Integrity** - ensuring that there are processes and controls in place to make sure personal data is accurate and complete
- **Availability** - ensuring that personal data is accessible when it is needed for the business purposes of Moorview Care
- **Resilience** - ensuring that personal data can withstand and recover from threats

For paper documents, these will include, where possible:

- Keeping the personal data in a locked filing cabinet or locked drawer when it is not in use
- Adopting a "clear desk" policy to ensure that personal data is not visible or easily retrieved
- Ensuring that documents containing personal data are accessible only by those who need to know/review the documents and the personal data contained within them
- Redacting personal data from documents where possible
- Ensuring that documents containing personal data are placed in confidential waste bins or shredded at the end of the relevant retention period
- Minimising the transfer of personal data from outside of business premises and, where such transfer cannot be avoided, ensuring that the paper documents continue to be kept confidential and secure

For electronic documents, the measures taken by Moorview Care will include, where possible:

- Password protection or, where possible, encryption
- Adopting a 'clear screen' policy where users lock screens when they are away from their computers
- Ensuring that documents containing personal data are accessible only by those who need to know/review the documents and the personal data contained within them
- Ensuring ongoing confidentiality, integrity and reliability of systems used online to process personal data (this may require a review of IT systems and software currently used by Moorview Care)
- The ability to quickly restore the availability of and access to personal data in the event of a technical incident (this may require a review of IT systems and software currently used by Moorview Care)
- Taking care when transferring documents to a third party, ensuring that the transfer is secure and the documents are sent to the correct recipient

Moorview Care will ensure that all business phones, computers, laptops and tablets are password-protected. At no point should information be downloaded and stored on removable storage devices.

4.14 Moorview Care will implement guidance relating to the use of business phones and messaging apps. Moorview Care understands that all personal data sent via business phones, computers, laptops

and tablets may be captured by UK GDPR, depending on the content and context of the message. As a general rule, Moorview Care will ensure that team members only send personal data by text or another messaging service if they are comfortable that the content of the messages may be captured by UK GDPR and may need to be provided pursuant to a Subject Access Request (team members should refer to the Subject Access Requests Policy and Procedure at Moorview Care for further details).

4.15 Moorview Care will ensure that all team members are aware of the importance of keeping personal data secure and not disclosing it on purpose or accidentally to anybody who should not have access to the information. To achieve this, Moorview Care will:

- Provide training to team members where necessary on the security of personal data
- Consider, in particular, the likelihood that personal data (including special categories of data) will be removed from the premises of Moorview Care.
- Control access to the premises
- Ensure that all team members understand the importance of maintaining the confidentiality of personal data away from the premises
- Take care to ensure that the personal data is not left anywhere it could be viewed by a person who should not have access

4.16 Moorview Care will adopt policies and procedures in respect of recognising, resolving and reporting security incidents, including breaches of UK GDPR. Moorview Care understands that it may need to report breaches to the ICO and to affected Data Subjects, as well as through 'Respond to an NHS Cyber Alert' if it is required to comply with the Data Security and Protection Toolkit.

4.17 Moorview Care will adopt processes to regularly test, assess and evaluate the security measures it has in place for all types of personal data.

4.18 Privacy by Design

Moorview Care will take into account the UK GDPR requirements around privacy by design, particularly in terms of data security.

4.19 Moorview Care understands that privacy by design is an approach set out in UK GDPR that promotes compliance with privacy and data protection from the beginning of a project. Moorview Care will ensure that data protection and UK GDPR compliance are always at the forefront of the services it provides, and that it will not be treated as an afterthought.

4.20 Moorview Care will comply with privacy by design requirements by, for example:

- Identifying potential data protection and security issues at an early stage in any project or process, and addressing those issues early on
- Ensuring that the default position in projects involving personal data is privacy centres, i.e. privacy by default; and
- Increasing awareness of privacy and data protection across Moorview Care, including in terms of updated policies and procedures adopted by Moorview Care

4.21 Moorview Care will conduct Data Protection Impact Assessments to identify and reduce the privacy and security risks of any project or processing carried out by Moorview Care. A template Data Protection Impact Assessment, along with the circumstances in which a Data Protection Impact Assessment should be conducted, is available within the Data Protection Impact Assessment (DPIA) Policy and Procedure at Moorview Care.

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 the people we support 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 on the 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 any 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 usable – 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

5.1 Moorview Care must consider data retention and data security issues and concerns at the beginning of any project (whether the project is the introduction of a new IT system, a new way of working, the processing of a new type of personal data or anything else that may affect the processing activities at Moorview Care). Moorview Care appreciates that this is key for complying with the privacy by design requirements in the UK GDPR.

5.2 Moorview Care will review the periods for which it retains all the personal data that it processes.

5.3 Moorview Care will, if necessary, adopt new policies and procedures in respect of data retention and will circulate those policies and procedures to all team members. Moorview Care will also consider providing training to team members in respect of data retention.

5.4 Moorview Care will review the security measures currently in place in respect of all the personal data it processes.

5.5 Moorview Care will document the decisions it takes and the logic and reasoning behind those decisions, in respect of both data retention and data security. Moorview Care will keep a record of all policies and procedures it implements to demonstrate its compliance with UK GDPR.

Record-keeping procedures – creation and use of records

When we create records, we use standardised structures and layouts for the contents of records. These include a standard file structure and naming convention.

These folders have been created to ensure that most elements are taken into account, and no new folders should be created.

Client Folders	HR Folders
Client Onboarding	Absence
Finance	Archive
Medication	ID & ISA

Client Folders	HR Folders
Support Planning	Induction
Risk Assessment	Misc
Meetings & Reviews	Payroll
Health & Wellbeing	Performance Review
Accommodation	Recruitment
Legal	Restricted Information
Notifications	Training
Archive	Supervision & Ad Hoc

As part of this new folder structure, we are introducing a new naming convention, which is designed to help make files quicker for the systems to find and easier to spot where information is in the incorrect place. The title is built on 3 key areas. The first is the date that the document was created; however, this is written in the following format YYYYMMDD, so for example, 1st March 2025 would be written as 20250301.

The next part is the person we support's unique identifier, which is present on the profile screen of MVCX. Finally is the document title, this needs to be written in a short format but needs to be clear as to the document, e.g., Support Plan, Risk Assessment, Hospital Letter.

Examples of the document titles:

20250226_JM34_careplan

20250301_MW86_Hospital App Letter

20240403_FF99_DWP review

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.

Team members' and the people we support's 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 the 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 (Basic)

Document Type	Retention Period
PERSONNEL	
Maternity, Paternity & Adoption Leave	3 years
Parental Leave	18 years from the date of birth of the child or 6 years after the 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 from 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 the warning expired, then retained in the personnel file, as spent for 6 years after employment ceases
Redundancy	6 years from the 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 the date on which they were made
Employee Files	6 years from the 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-18s, 5 years after their 18 th birthday
Accident reports/ incident reports HS03	5 years from the last entry or the end of investigation if later
Incidents notified to CQC	3 years
CLIENTS	
Client files	8 years from the leave date
Any social care records for adults	8 years from the 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 the settlement
Contracts	6 years
Employer's Liability Certificates	40 years
Audit Records	5 years
Subject Access Requests	3 years

Further retention periods can be found in the resources section.

Further Reading

ICO - Records Management and Security (Retention Schedule):

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/records-management-and-security/>