

Data & Document Retention & Disposal Policy



Policy Name	Data & Document Retention & Disposal Policy
Effective Date	1 st August 2025
Approved By	Harbour Light Board
Approval Date	1 st August 2025
Policy Owner/Dept	Information & Data Governance
Policy Author	Peter McEleavey
Review Date	1 st August 2028
Version Number	1.0

Version	Date	Changes	Approver

Relevant National Standards or Regulations	• ICO guidance on storage limitation and secure disposal. • NHF guidance/briefings on records retention schedules. • RSH regulatory framework expectations on governance, risk and control (record-keeping)
---	---

Relevant Legislation	• UK GDPR (Article 5(1)(e) – storage limitation). • Data Protection Act 2018. • Limitation Act 1980 (civil claim time limits guiding retention). • Companies Act 2006 / HMRC rules for accounting records (e.g., 6-year retention). • Health & safety record duties where applicable (e.g., Control of Asbestos Regulations/RIDDOR - long-term retention of exposure/incident records)
-----------------------------	--



Data & Document Retention & Disposal Policy

1. Purpose

This policy sets out how Harbour Light Assisted Living CIC manages the retention of records and the secure disposal of data and documents. Its purpose is to ensure that we keep information for only as long as necessary and then dispose of it safely, in compliance with the storage limitation principle of the UK GDPR and other legal requirements. By implementing this policy, the Organisation ensures compliance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018, and relevant guidance from the National Housing Federation (NHF) and the Information Commissioner's Office (ICO). This policy also helps us meet regulatory expectations for good governance and information management, including requirements of the Regulator of Social Housing and best practices for social landlords. It supports accountability and efficiency by preventing excessive retention of data and reducing the risk of data breaches related to old or unnecessary records.

2. Scope

This policy applies to **all records and data** held by Harbour Light Assisted Living CIC, whether in physical (paper) form or in electronic systems. It covers all types of documents and data, including but not limited to tenant files, tenancy agreements, financial records, correspondence, emails, reports, HR/employment records, safeguarding records, maintenance and health & safety logs, CCTV footage, and any other documents containing personal or business information. The policy is applicable across all departments of the Organisation.

Who is covered: All employees, agency staff, contractors, volunteers, and third-party service providers who create, receive, or manage Harbour Light Assisted Living CIC documents or data are required to follow this policy. It also extends to any external data processors handling information on our behalf (such as IT backup providers or document disposal companies), who must act according to our retention and disposal guidelines.

By defining the scope broadly, this policy ensures that **all organisational information assets** are managed consistently from creation to destruction. It aims to prevent keeping records longer than necessary and to promote secure disposal, thereby upholding individuals' privacy rights and maintaining compliance with UK GDPR.

3. Responsibilities

Proper enforcement of the retention and disposal policy is critical. The following roles have specific responsibilities:

- **Data Protection Manager (Mark Adams):** Responsible for maintaining and overseeing this policy and the master Document Retention Schedule (Appendix A). The Data Protection Manager will monitor legislative changes or guidance updates (e.g. new ICO or NHF advice on retention) and will initiate policy revisions as needed. He also provides advice and training to staff on retention requirements and audits compliance with retention periods.
- **Department Leads/Managers:** Each department head is responsible for implementing the retention schedule within their area of work. They must ensure that their team members know the required retention periods for the records they handle and that records are not kept beyond those periods. Department leads should periodically review the records held in their business area (both electronic and paper) and coordinate secure disposal of any information that has met its retention timeline. They also ensure any third-party contractors under their



Data & Document Retention & Disposal Policy

remit (e.g. a shredding service or off-site storage provider) are aware of and adhere to this policy.

- **All Staff and Data Users:** Every staff member (and anyone processing data on our behalf) must comply with the retention and disposal procedures. This includes appropriately labelling and filing documents to facilitate easy retrieval and timely disposal, not hoarding records longer than allowed, and securely disposing of records when instructed or when the retention period expires. Staff must report to their manager or the Data Protection Manager if they suspect any records are being kept too long or if they discover records that should have been destroyed. Additionally, any **data breach** or incident (such as lost files or improper disposal) must be reported immediately so that appropriate action can be taken.

These responsibilities ensure clear ownership of the retention process at all levels. Management oversight combined with day-to-day staff diligence helps maintain an effective records management culture. The Board of Directors holds ultimate accountability for ensuring the Organisation meets its legal obligations for data retention and disposal, and will receive periodic assurance (for example, via audit reports or Data Protection Manager updates) that this policy is being followed.

4. Legislation and Regulations

This Retention & Disposal Policy is informed by the following key legislation, regulations, and standards:

- **UK General Data Protection Regulation (GDPR)** (EU 2016/679, as retained in UK law) – Particularly the “**storage limitation**” principle under Article 5, which requires that personal data be kept no longer than necessary for the purposes for which it is processed.
- **Data Protection Act 2018** – National law that supplements GDPR, including provisions on exemptions and enforcement related to data retention.
- **Limitation Act 1980** – Sets statutory limitation periods for legal claims (e.g. contractual claims, personal injury, debt recovery) which inform how long certain records (like contracts or accident reports) should be kept in case of litigation.
- **Regulatory Framework for Social Housing in England (Regulator of Social Housing)** – Contains governance and viability standards expecting registered providers to have effective systems for managing and safeguarding information, including proper record-keeping and disposal in compliance with law. Keeping records too long or failing to produce them when required (e.g. for health and safety checks or complaints) could breach regulatory expectations.
- **ICO Guidance on Storage Limitation and Data Disposal** – Guidance from the Information Commissioner’s Office on how organisations should implement retention rules and securely destroy data that is no longer needed. This includes best practices like not keeping data “just in case” beyond its purpose and ensuring secure destruction methods.
- **NHF (National Housing Federation) Briefing: GDPR and Document Retention** – Sector-specific guidance from the NHF about recommended retention periods for housing associations. We use this as a reference, alongside our legal obligations, to set retention periods that reflect housing sector best practice.
- **Other Relevant Laws and Standards:** Depending on the type of record, other laws can dictate retention. For example:
 - **Companies Act 2006 and Finance (No. 2) Act 2017** – govern retention of financial and accounting records (6 years for accounts).
 - **Housing Benefit Regulations** – may require us to keep certain tenant financial records for audit by local authorities.



Data & Document Retention & Disposal Policy

- **Health and Safety regulations** (e.g. Control of Asbestos Regulations 2012, RIDDOR) – require lengthy retention of safety and maintenance records (such as 40 years for asbestos-related documents).
- **Employment legislation** – influences retention of HR files (e.g. 6 years after employment ends, aligning with time limits for tribunal claims).
- **Safeguarding guidance** – serious incident reports or safeguarding records may be kept for extended periods (often 10 years or more) due to the sensitive nature and potential for long-term follow-up.

Status Note: This policy is considered **Statutory/Regulatory** as it is essential for compliance with data protection law and various regulatory standards. Adhering to these rules protects the rights of individuals and ensures we can demonstrate accountability for how long we keep information.

5. Procedures

5.1 Lawful Retention Principles

Harbour Light Assisted Living CIC follows strict principles to decide how long to keep each type of document or data. We will **only retain documents and personal data** under the following conditions:

- **Legal, Contractual, or Regulatory Requirement:** We keep records for a duration that is required or clearly justified by law, regulation, or contract. For example, we retain tenancy agreements and related documents for at least 6 years after a tenancy ends, because of the Limitation Act 1980 (the period in which former tenants could bring certain claims). Similarly, we keep financial records for 6 years after the financial year to comply with tax and accounting laws.
- **Necessary for Business Purpose:** We retain personal data only as long as needed for the purpose it was collected or for other legitimate business purposes that are not overridden by the individual's rights. We determine necessity by considering the ongoing use of the data – once a record's purpose is fulfilled, we should archive or delete it.
- **Defined Retention Period:** Each category of record has a defined retention period or review interval per our Retention Schedule (Appendix A). We adhere to these defined periods. If a record's retention period is extended (for instance, due to ongoing legal action or an open inquiry), the reason will be documented, and the record will be deleted once that reason no longer applies.

In summary, **no data should be kept indefinitely “just in case.”** We actively enforce retention deadlines. Keeping data longer than necessary increases the risk of it becoming inaccurate, irrelevant, or causing a data breach, and it violates GDPR principles. By sticking to lawful retention principles, we demonstrate respect for individuals' privacy and good information governance.

5.2 Retention Periods

Specific retention periods for key types of documents are set out in **Appendix A – Document Retention Schedule** at the end of this policy. This schedule covers categories such as tenancy records, financial documents, human resources files, health, and safety records, and more. A few key examples include:

- **Tenancy Agreements and Tenant Files:** Retained for 6 years after a tenancy ends (this covers tenancy contracts, rent payment records, and related correspondence). This period aligns



Data & Document Retention & Disposal Policy

with the statute of limitations for contract claims, ensuring records are available if former tenants raise issues or if we need to pursue debts.

- **Financial Records:** Retained for 6 years after the end of the financial year. This includes invoices, receipts, accounts, and audit documents, meeting HMRC requirements and company law.
- **Safeguarding and Serious Incident Records:** Retained for a longer period, typically **10 to 15 years**, reflecting best practice in the sector. This accounts for the possibility of long-term follow-up or legal actions in sensitive cases.
- **Health and Safety Documentation:** Certain records, like asbestos surveys, fire risk assessments (FRA), accident reports, or equipment inspection certificates, are kept for extended durations. For example, asbestos records may be kept for **40 years** due to health risk latency and legal duties.
- **HR/Personnel Files:** For former employees, kept for 6 years after employment ends (covering personnel records, contracts, disciplinary records, etc.), aligning with timeframes for potential employment tribunal claims or references.
- **CCTV Footage:** Routine surveillance footage is kept for a **maximum of 30 days** (one month) unless needed longer for a specific investigation. After 30 days, footage is overwritten or deleted unless flagged for an incident.

Staff should refer to **Appendix A** for the full list of retention periods applicable. If a document type is not listed in the schedule, the default approach is to consult the Data Protection Manager for guidance, who will determine a retention period based on legal requirements and business need.

We perform periodic checks and audits to identify records that have reached their disposal date. For electronic systems, automated retention rules or tags may be applied where feasible (for example, email archives or SharePoint document libraries might have retention labels). For paper records, departments maintain storage with clear labels (including destruction dates where possible) to facilitate timely destruction.

Importantly, when an official request or legal hold is in place (e.g. a subject access request or litigation hold), relevant records will **not** be destroyed even if their retention date has passed until the hold is lifted. This ensures we do not dispose of information that is needed for an ongoing matter.

5.3 Secure Disposal

When records reach the end of their retention period (or are identified as no longer needed), they must be disposed of promptly **and securely**. Secure disposal is critical to prevent any unauthorised access to sensitive information during or after the destruction process. Harbour Light Assisted Living CIC employs the following disposal methods:

- **Paper Records:** Physical documents containing personal or confidential information are destroyed by cross-cut shredding or placed in locked “confidential waste” bins, which are collected by an accredited shredding service. Shredded material is then usually recycled or incinerated by the disposal contractor under secure conditions. Under no circumstances should paper records simply be thrown in regular rubbish or recycling bins intact.
- **Electronic Records:** For digital files, we use secure deletion methods. This can include using authorised software tools to permanently erase files (ensuring they cannot be recovered) or, for removable media, physically destroying the media if it is no longer needed. Simply deleting a file or email is not always sufficient, so IT will ensure data is truly wiped according to our



Data & Document Retention & Disposal Policy

procedures. For example, old hard drives are securely wiped or degaussed, and if that is not possible, they are destroyed.

- **Backup Data:** We also address data held in system backups or archives. If personal data has been deleted from live systems, we ensure that backup copies are either automatically purged after a retention period or are securely wiped if restoring them. Our IT team manages backup retention policies so that outdated personal data is not stored indefinitely in backup systems.
- **Cloud Services:** If any personal data is stored with third-party cloud services, we will ensure that those services have robust deletion procedures. When we delete cloud-held data, we obtain confirmation that it has been fully removed from all servers, including replicas and backups, according to the service agreement.
- **Special Cases:** For certain specialised records (like old CCTV DVRs, ID cards, or biometric data, if any), we follow industry guidelines for destruction. For instance, CCTV hard drives will be wiped or physically destroyed when decommissioned. Any item that might contain personal data (USB drives, CDs, printed photos, etc.) is treated as confidential and destroyed securely.

All disposals of records containing personal data should be **logged in the Data Disposal Register** maintained by the Data Protection Manager or IT Department. The log entry notes what was destroyed, when, and by whom (or which contractor). This creates an audit trail for accountability and helps demonstrate compliance with our policy.

Staff must coordinate with their line managers or the Data Protection Manager before disposing of any large sets of documents to ensure no overriding reason exists to keep them (such as ongoing investigations or legal considerations). If in doubt, consult the Data Protection Manager.

By following these secure disposal procedures, we mitigate the risk of data leaks and uphold our legal obligations to securely destroy personal data. **Remember:** retention and disposal go hand-in-hand it is not enough to know when to delete; we must also delete in a manner that leaves no trace of the personal data.

5.4 Storage & Classification

Organising and classifying documents properly during their life cycle aids effective retention management. Harbour Light Assisted Living CIC utilises a structured approach to storing records:

- All documents (especially electronic files) should be stored in the appropriate location within our approved **SharePoint structure and metadata taxonomy** (or other designated document management systems). This means files are saved in the correct departmental library or folder, with metadata tags (such as document type, date, tenant name, etc.) filled in as required. Consistent use of the folder structure and metadata makes it easier to apply retention rules and locate files when review or deletion is due.
- We classify records by category (e.g., tenancy, finance, HR, maintenance) and assign retention rules to each category. This classification is reflected in Appendix A. Staff should be aware of the category of the documents they handle and ensure those documents are stored in the corresponding repository, which enforces the appropriate retention policy.
- Access controls are applied so that only authorised personnel can access sensitive records. This not only protects data but also helps track where records are – for example, personnel files are in a secure HR area, incident reports in a safeguarding folder, etc. This segregation supports easier review of groups of records when the retention period is up.
- **Avoid Duplication:** Staff should refrain from keeping multiple copies of the same record in different places (for instance, downloading a report and storing it in personal drives or email).



Data & Document Retention & Disposal Policy

A single “source of truth” copy should be kept in the central system. Duplicates make it harder to manage retention since one copy might be deleted while others linger. Our policy is that the official copy of a record is retained, and all duplicates or locally stored versions should be deleted promptly when no longer needed for active work.

- **Email and Communications:** Emails can contain important records. Staff should either capture important information from emails into our systems (e.g., save attachments or key decisions to SharePoint) or apply retention tags to email folders. We discourage using email inboxes as long-term storage. Periodically, emails older than a certain timeframe should be archived or deleted, unless they serve as official records that need retention (in which case, they should be moved to the proper repository).
- Our IT systems may implement automated retention policies (for example, auto-deletion of emails after X years or mandatory review of documents after Y years). Staff should not attempt to circumvent these controls. If a retention control deletes something that is still needed, staff should inform IT/DPM immediately – do not rely on personal backups or undeleting without consultation.

By maintaining organised storage and clear classification, we simplify the eventual disposal process. It allows the Data Protection Manager and department leads to run reports or checks on what is due for deletion. Additionally, good classification is essential for responding to data subject requests or audits, since we can easily find what data, we hold. All employees have a role in ensuring that records are stored correctly and cleaned up regularly.

5.5 Data Subject Rights and Deletion Requests

Under GDPR, individuals (data subjects) have the **right to request deletion** of their personal data (the “right to be forgotten”) in certain circumstances. This policy works in tandem with those rights:

- If we receive a **deletion (erasure) request** from an individual, the Data Protection Manager will evaluate it promptly. We will honour valid deletion requests and erase the individual’s personal data from our systems, provided that the data is not required to be retained for a legal or contractual reason. For instance, if a former tenant requests deletion of their data and we have no ongoing reason to keep it, we will remove their records from our active systems and archives.
- Situations where we might **refuse or defer deletion** include:
 - We have a legal obligation to keep the data (e.g., financial transaction records for HMRC, or records required by safeguarding laws).
 - The data is needed for the establishment, exercise, or defence of legal claims (for example, the individual owes a debt or has a dispute pending, so we must retain relevant information).
 - The deletion request applies to information in active use necessary for performing a contract or providing a service the individual still uses (in which case deletion might mean we can’t fulfil our agreement; we would explain this to the individual and might offer to cease the service if they insist on deletion).
- When a deletion request is fulfilled, the Data Protection Manager will ensure all copies of the personal data are erased – including from live databases, file shares, and, where feasible, from backups (or that backups are set not to restore the deleted data). We will also inform any third parties who have the data (due to sharing as per our Privacy Policy) about the deletion, if required, so they can also erase their copies.
- We will respond to the individual to confirm deletion has taken place or provide a justified refusal if we cannot delete some or all requested data. In case of refusal, we will inform the

Data & Document Retention & Disposal Policy



data subject of the specific reason and their right to complain to the ICO. For example, “We are unable to delete your tenancy records for an additional 2 years because they are needed to satisfy our legal obligation under the Housing Act...” etc.

It is important to note that our **scheduled retention and disposal processes will often proactively remove personal data** as soon as it is no longer needed, potentially obviating the need for individuals to request deletion. In effect, by following our retention schedule, we minimise the amount of outdated or irrelevant personal data we hold, thereby upholding individuals’ rights automatically. Deletion requests will be incorporated into our retention workflows – if someone requests deletion and it is approved, we will update our records (or retention schedule) to mark those items for immediate destruction rather than waiting for the standard time limit.

In summary, **Harbour Light Assisted Living CIC will honour deletion requests** to the fullest extent possible, **unless** there is an overriding legal or regulatory requirement to retain the data. Our Data Protection Manager maintains documentation of any deletion requests and their outcomes as part of demonstrating GDPR compliance.

6. Review and Updates

This Data & Document Retention & Disposal Policy will be reviewed on a **three-year cycle**, or sooner if required due to changes in legislation or operational needs. The next scheduled review will be in **August 2028**. Reviews will assess whether retention periods remain appropriate (for example, if laws change or if internal experience shows a need for longer/shorter retention for certain records) and whether disposal procedures are effectively implemented.

Updates to this policy (including Appendix A – Retention Schedule) will be approved by senior management. When updates occur, the revised policy version will be distributed to all staff and relevant contractors, with training or briefing provided if there are significant changes to procedures.

Version history will be logged in the document control section of the policy. This document is **Version 1.0** as of the effective date. Any changes (e.g., revision to Version 1.1 or 2.0) will be noted along with the date and a summary of changes.

By regularly reviewing this policy, Harbour Light Assisted Living CIC ensures continuous alignment with current laws (such as UK GDPR) and best practices in records management. The review process also considers feedback from audits, any data incidents related to retention/disposal, or user input to improve practicality. Ultimately, keeping this policy up-to-date helps protect the organisation and its stakeholders by preventing both excessive retention and premature disposal of important records.



Data & Document Retention & Disposal Policy

Appendices: The following appendix is an integral part of this policy and will be updated in line with policy reviews:

Appendix A – Document Retention Schedule

Document Type	Retention Period	Notes / Legal Basis
Tenancy Agreements	6 years after tenancy end	Limitation Act 1980 – contract claims (6-year limit)
Tenancy Files (support, rent, complaints)	6 years after tenancy end	UK GDPR legitimate interests; allows time to resolve post-tenancy issues
Financial Records (ledgers, invoices, bank statements)	6 years after the fiscal year end	Companies Act 2006; Finance laws (required for audits, tax)
Safeguarding Reports & Serious Incident Records	10–15 years (from date of closure)	Best practice reflects safeguarding duty and potential long-term inquiries
Health and Safety Records (e.g. building safety certificates, asbestos surveys, accident reports)	40 years (or as specified by regulation)	E.g. Control of Asbestos Regulations (40 yrs); RIDDOR for incidents
HR / Personnel Files (employee records, contracts, performance, etc.)	6 years after employment end	Statutory claims period for employment tribunals/discrimination claims
CCTV Footage	30 days maximum	Automatically overwritten unless required for an ongoing investigation
Board & Committee Minutes	Permanent (or minimum 10 years)	Governance best practice; historic record of decisions

Notes: The retention periods above are general guidelines. “After tenancy end” or “after employment end” means counting from the date the tenancy or employment formally ended. “Fiscal year end” for financial records usually means 31 March or 5 April for the UK tax year, depending on context, or our own accounting year end if different.

If any applicable law prescribes a longer retention for a specific document, that law overrides the schedule (for example, certain financial or health & safety documents might need longer retention under future regulations). The Organisation will update the schedule as needed to remain compliant.

For documents not explicitly listed, consult the Data Protection Manager. In cases of ongoing disputes, investigations, or legal proceedings, retain records until the matter is fully resolved, even if the standard period has passed – then dispose securely.

By adhering to this retention schedule, Harbour Light Assisted Living CIC demonstrates compliance with legal mandates and ensures information is available when needed and disposed of when it is not, thereby balancing operational needs with data protection responsibilities.