Approved by ELHA Board 21/08/25

ELHA POLICY

Date Issued	August 2025
Department	Corporate
Title	Records Management Policy
Objective	**To provide a framework for the effective management of records**
Responsible	Chief Executive
Next Review Date	**August 2030**

1.0 Introduction

1.1 East Lothian Housing Association creates, handles and uses records of information to support its functions and operations as a Registered Social Landlord in Scotland.

1.2 Our Records Management policy outlines how we handle our information throughout its lifecycle, from creation to disposal, ensuring compliance with legislation, regulatory requirements and supporting business needs. It provides a framework for effective records management within the Association, as well as guidance to staff on the proper management and protection of records, including the storage retrieval, retention and eventual disposal.

2.0 Legal & Regulatory Framework

2.1 Managing records appropriately reduces the costs and risks associated with retaining unnecessary information and is core to complying with legal and regulatory requirements, including:

- General Data Protection Regulations
- Data Protection Act 2018
- Freedom of Information (Scotland) Act 2002
- Environmental Information (Scotland) Regulations 2004
- Human Rights Act 1998

2.2 We will also comply with the Scottish Ministers' Code of Practice on Record Management issued under Section 61 of the Freedom of Information (Scotland) Act 2002. The Code recommends that the Association has a Record Management policy and organisational arrangements in place that supports record management.

2.3 This policy operates alongside the following ELHA publications:

- Privacy Policy
- Freedom of Information Policy
- Freedom of Information Guide to Information
- Data & Digital Strategy
- ICT Security policy
- Data Retention Schedule
- Subject Access Request Procedure

3.0 Scope

3.1 This policy applies to all records created, received, or maintained by staff, contractors, board members, and agents of East Lothian Housing Association in the course of their duties.

3.2 A record can be defined as 'recorded information, regardless of format or medium that is created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business'. It covers:

- Paper documents
- Emails
- Digital files (Word, PDF, excel, etc)
- Audio and/or video recordings
- Photographs
- Social media communications
- Metadata associated with files or databases

For example:

- Tenancy files
- Administrative - meeting minutes, memo's, internal reports
- Financial - invoices, purchase orders, audit logs
- Legal / contractual – contracts, licences, consent forms
- Personnel / HR – job applications, training records
- Maintenance and repair records
- Governance documents

3.3 These records may be held within our premises or by third parties on our behalf, including consultants and professional advisers. Records created by staff in the course of their employment with the Association belong to the Association not the member of staff who created them.

4.0 Responsibilities

4.1 The Chief Executive has overall accountability for records management.

4.2 The Senior Management Team with the Data Protection Officer and Compliance Team established the policy, oversee compliance with data protection and advise on data retention and security.

4.3 The Management Team develop and implement procedures, train staff, conduct reviews and liaise with internal and external stakeholders.

4.3 Staff have a responsibility to effectively manage the Association's records in accordance with the law, best practice and this policy, maintaining the quality, integrity, completeness, accessibility, reliability, accuracy and security of the records and for promoting a culture that values, protects and uses records for the benefit of the Association and its service users. Staff with their Manager, are also responsible for the regular review of the records held within their departments.

5.0 Record Management

5.1 Records management can be described as the efficient and systematic control of the planning, creation, receipt, maintenance, use, distribution, storage and disposal / permanent preservation of records throughout their life cycle.

5.2 Records management ensures that evidence of, and information about our activities and transactions, is captured in our record keeping systems and maintained as viable records. It concerns placing controls around each stage of a record's lifecycle, at the point of creation or receipt, during its maintenance and use, and ultimate disposal. Through such controls we can ensure our records demonstrate the key features of authenticity, reliability, integrity and accessibility.

5.3 The main benefits of good records management are:

- Promoting the creation of storage of accurate and reliable records in a managed environment, which provides an audit trail of actions that can support us in the event of, for example, regulatory intervention

- Increasing organisational and administrative effectiveness common efficiency and service delivery through improved access to and retrieval of high quality records

- Helping enhance information security by facilitating improved confidentiality, integrity and availability of records

- Improving working environments and more economical use of physical and service space through reducing the tension of irrelevant, duplicate and out of date records

- Promoting our physical and intellectual control of all records by knowing what records we have and how and where to retrieve them easily

- Ensuring that we identify and retain records of historical and evidential value to us as a corporate memory, and to assist in managing future recurrences of specific events

- Helps to maintain audit trails relating to access and alteration of records

- Improving information sharing and the provision of easy and timely access to the correct information at the right time, resulting in better quality decision making and thereby facilitating transparency and accountability for all actions

- Managing business continuity risks by helping to identify records that are essential to the continued operation which, if lost or destroyed, would seriously impair or disrupt our operations

- Assisting in compliance with all legal and regulatory obligations including responding to requests for information and personal data made to the Association

5.4 The risks to the Association in not maintaining effective records management are:

- Poor quality decisions being made on the basis of inaccurate, incomplete or out of date records
- Levels of service to our customers being inconsistent due to records of previous actions being unavailable
- Financial, legal or reputational loss if the necessary evidence of an activity or transaction is not available or cannot be relied upon in the event of, for example, regulatory intervention
- Non-compliance with legal or regulatory requirements
- Failure to identify, protect and retain records that are critical to business continuity
- Failure to handle confidential information with an appropriate level of security
- Unnecessary costs incurred in storing records for longer than needed
- Wasted time and resources in searching for records in response to a request received
- Wasted time considering issues that have previously been addressed and resolved
- Loss of reputation as a result of all the above

6.0 Receipt and Creation of Records

6.1 Staff must act responsibly, lawfully and professionally when receiving and creating records, and must comply with the following principles:

- **Adequate** - records must be sufficient for the purposes for which they are held
- **Authentic** - records must be reliable and accurate, contain the information that was used for a particular activity, and it must be possible to identify who created them and when

- **Accessible and Usable** - records must be capable of being readily accessed, used and relied upon by those with appropriate authorisation for as long as they are required (this includes ensuring the longevity of records held in paper and electronic formats where there is a risk of papers deteriorating or electronic files being deleted)

- **Complete** - records must be sufficient in content, context and structure to permit reconstruction of the relevant business activity (records must be complete, and it must be possible to identify any alterations made to them after creation, together with the identity of the staff who made the alterations to protect against unauthorised alteration)

- **Comprehensive** - records must be capable of being easily understood and provide clear information about the relevant business activity

- **Compliant** - records must comply with relevant legal and regulatory requirements

- **Retention** - records must be kept for as long as they are required to support and evidence the relevant business activity

- **Proportionate** - the contents of records should be proportionate and appropriate to the relevant business activity and should not be excessive for the activity

- **Secure** - records should only be accessible to those who need to have access for a relevant business activity and appropriate physical and technological measures must be in place to keep them secure and to prevent accidental or unauthorised alteration, copying, movement or deletion, which could put the reliability of the records at risk

6.2 The Association prohibits staff from creating records that are misleading, false, fraudulent, sexually explicit, abusive, offensive, harassing, discriminatory, profane, libellous, defamatory, unethical, or that violates any legal or regulatory requirements so stop if such records are created by staff, the release of any information contained in such records in response to a request made to the Association under access to information or data protection laws could have a significant reputational, regulatory and legal consequences for us.

7.0 Storage and Access

7.1 Records must be stored securely at our premises or at a secure location in accordance with our Privacy Policy and ICT Security Policy to minimise the risk of damage, loss or unauthorised access to the records.

7.2 All records must be stored within our file structure, housing management system or These Homes, and must not be stored by staff in their personal drives on computers or in personal paper files or notebooks. When storing records, staff must give records titles that reflect that specific nature and contents. This ensures more universal availability of records and helps with finding them more easily. It also facilitates the audit process, allows us to determine the types of records we hold and where they are held, and the identification of records for disposal at the end of their relevant retention period.

7.3 Staff should dispose of brief or temporary records on a routine basis. For example:

- Hard copies of electronic documents, which have been printed for a meeting
- Trivial emails or communications that should be deleted after being read such as promotional emails or communications
- Draft documents once the final version is approved
- Duplicate copies of documents kept for convenience

In general, all documents which have short term usefulness, no legal or regulatory retention requirement and not part of the official record or decision making trail should be deleted. This will reduce the likelihood of duplicates and unnecessary records being stored within the file structure.

7.4 Staff should only have access to records on a strict need to know basis, depending on the nature of a record and its relevance to the work of staff.

7.5 To ensure continuity of records in situations where the Association is procuring a new document management system, we will integrate records management into the specification, particularly in relation to ensuring that existing electronic records are migrated and remain accessible via the new system. We will also take into consideration the advice and guidance of our Data Protection Officer and the characteristics of a good records system contained within the Scottish Ministers, Section 61 Code of Practice on Records Management.

8.0 Removal of records

8.1 Staff may remove records from our premises only for legitimate business purposes, such as visiting tenants at home or attending a meeting with an external agency. Staff must return records when there are no longer needed off site for business purposes.

8.2 Staff must handle records removed from our premises in accordance with the ICT Security policy.

9.0 Retention and Disposal

9.1 We must keep records for as long as they are required by relevant laws and regulatory purposes, and our business needs particularly for reference in accountability purposes. Destruction at the end of this period ensures that office and server space are not used unnecessarily, and costs are not incurred in maintaining records that are no longer required. It also ensures that we comply with the fifth data protection principle for records containing personal information; 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes'.

9.2 Our Data Retention Schedule sets out how long each record type will normally be held and when they will be destroyed. We will regularly review and update the Data Retention Schedule with additional record types that we use in the course of carrying out our functions and operations.

9.3 We will not destroy or dispose of records before the relevant retention period expires. The retention period specified in the Data Retention Schedule does not mandate that records must be disposed of or destroyed after this period. Rather, expiry of the retention period provides staff with an opportunity to review the record and decide if there are special reasons to justify longer retention.

9.4 Staff must not generally retain records for longer than the relevant retention period unless there are special reasons for doing so, for example, where the records are required for the purposes of litigation in which we are or are likely to be involved or in the case of a request for information, all relevant complaint and appeal provisions have been exhausted. In such circumstances, staff must not alter, dispose of or destroy any relevant records required for the litigation or information request until the Data Protection Officer has advised that the retention and disposal of such records should resume in line with the Data Retention Schedule. Special reasons may also exist in the case of those records which we have selected for permanent preservation.

9.5 A record cannot be considered to have been completely disposed of or destroyed until all copies, including backup copies, have been destroyed.

9.6 If a record type is not listed in the Data Retention Schedule, or if staff have questions or concerns about retaining any records beyond the specified retention periods, they must contact our Data Protection Officer for guidance.

9.7 Some of our records are likely to be retained permanently and archived, these are also listed in the Data Retention Schedule. We will follow the Scottish Ministers Code of Practice which sets out arrangements that apply to the review and transfer of records to public archives. The Data Protection Compliance Team will transfer documents to the public archives when required in an orderly manner and with a level of security appropriate to the confidentiality of the records.

9.8 We will destroy records scheduled for destruction in a secure manner, in particular documents containing personal information will be destroyed by professional contractors to prevent unauthorised access.

10.0 Digital Records and E-mail

10.1 Emails containing business critical or personal data must be stored in the appropriate system not left in personal inboxes.

10.2 Staff should avoid using personal devices or e-mail accounts for business purposes unless authorised.

11.0 Monitoring and Compliance

11.1 The Data Protection Compliance Team will monitor adherence to this policy through:

- Regular audits
- Staff training and awareness sessions
- Reports to the Senior Management Team

11.2 The Management Team and Data Protection Compliance Team will review the Data Retention Schedule annually and ensure the disposal or archiving of records. We will keep details of destruction of records, either as part of the audit trail metadata, or separately. At the very least we will, as part of routine records management processes, record the:

- Type of record
- Age range
- Specified provision of the Data Retention Schedule

Recording the disposal provides evidence to explain why records specified in a court order, for example, cannot be provided, or to defend ourselves against any charge under section 65 of FOISA that records were destroyed in order to prevent their disclosure in response to a request for information.

11.3 We take compliance with this policy very seriously. To not comply puts both staff and the Association at risk. Therefore, failure to comply with any requirement of this policy may lead to disciplinary action for a member of staff, and this action may result in dismissal for gross misconduct.

12.0 Training and Awareness

12.1 All staff will receive training on records management, data protection and secure handling of information at induction and regularly throughout their employment with the Association.

13.0 Policy Review

13.1 This policy will be reviewed by the Chief Executive every five years, or sooner if required by changes in legislation or organisational practice. Any material changes will be submitted to the ELHA Board for approval.