RECORDS MANAGEMENT POLICY 2024

1 Introduction

1.1 The Association creates, handles and uses records of information to support its functions and operations as a registered social landlord in Scotland. These records contain information that is an invaluable resource and a significant operational asset to support such functions and operations. A systematic approach to records management is necessary to protect and preserve records to support the Association's functions and operations and provide evidence of events, activities and transactions.

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

1.2.1 General Data Protection Regulation;

1.2.2 Data Protection Act 2018;

1.2.3 Freedom of Information (Scotland) Act 2002;

1.2.4 Environmental Information (Scotland) Regulations 2004; and

1.2.5 Human Rights Act 1998.

1.3 The Association will also comply with the Scottish Ministers' Code of Practice on Records Management issued under Section 61 of the Freedom of Information (Scotland) Act 2002. The Code recommends that the Association have a records management policy and organisational arrangements in place that support records management.

1.4 This policy is an organisational commitment to effective records management at the Association. It will help staff to properly manage the Association's records with regard to how they create, store, remove, retain and destroy them and highlights the importance of effective records management to the Association's functions and operations.

2 Responsibility and scope

2.1 The Association's Data Protection Officer (DPO) is responsible for this policy, assisting staff in maintaining appropriate information audits for their departments, providing guidance on records retention and delivering staff training on records management.

2.2 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 are also responsible for the regular review of the records held within their departments.

2.3 Records are documents (including written and typed documents and annotated copies), computer files, paper files, communications (including voicemails and SMS messages) and other material in all recorded formats, including electronic, paper, film, video (including CCTV footage), audio and others available through existing and emerging technologies.

2.4 For records to be covered by this policy, they must be created, received or maintained by the Association in the course of carrying out its functions and operations and relate to a business-related event, activity or transaction or other legal, regulatory or compliance purpose. These records may be held within the Association's premises or by third parties on its 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.

3 Records management

3.1 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 lifecycle. It ensures that evidence of, and information about, the Association's activities and transactions is captured in its 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 at ultimate disposal. Through such controls, the Association can ensure its records demonstrate the key features of authenticity, reliability, integrity and accessibility.

3.2 The main benefits of good records management at the Association are:

3.2.1 promotes the creation and storage of accurate and reliable records in a managed environment, which provide an audit trail of actions that can

support the Association in the event of, for example, regulatory intervention;

3.2.2 increases organisational and administrative effectiveness, efficiency and service delivery through improved access to and retrieval of high-quality records;

3.2.3 helps enhance information security by facilitating improved confidentiality, integrity and availability of records;

3.2.4 improves working environments and more economical use of physical and server space through reducing the retention of irrelevant, duplicate and out-of-date records;

3.2.5 promotes the Association's physical and intellectual control of all records by knowing what records it has and how and where to retrieve them easily;

3.2.6 ensures that the Association identifies and retains records of historical and evidential value to the Association as a "corporate memory" and to assist in managing future recurrences of specific events;

3.2.7 helps to maintain audit trails relating to access and alteration of records;

3.2.8 improves 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;

3.2.9 manages business continuity risks by helping to identify records that are essential to continued operation which, if lost or destroyed, would seriously impair or disrupt the Association's operations; and

3.2.10 assists in compliance with all legal and regulatory obligations, including responding to requests for information and personal data made to the Association.

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

3.3.1 poor quality decisions being made on the basis of inaccurate, incomplete or out-of-date records;

3.3.2 levels of service to service users being inconsistent due to records of previous actions being unavailable;

3.3.3 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;

3.3.4 non-compliance with legal or regulatory requirements applicable to the Association;

3.3.5 failure to identify, protect and retain records that are critical to business continuity;

3.3.6 additional costs incurred in storing records for longer than necessary; and

3.3.7 wasted time and resources in searching for records in response to a request received.

4 Receipt and creation of records

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

4.1.1 adequate: records must be sufficient for the purposes for which they are held;

4.1.2 authentic: records must be reliable and accurate, contain the information that was used by the Association for a particular activity and it must be possible to identify who created them and when;

4.1.3 accurate: records must accurately reflect the business activity carried out by the Association and must be created at the time of the activity by staff who were involved in the activity;

4.1.4 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;

4.1.5 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;

4.1.6 comprehensive: records must be capable of being easily understood and provide clear information about the relevant business activity;

4.1.7 compliant: records must comply with relevant legal and regulatory requirements;

4.1.8 retention: records must be kept for as long as they are required to support and evidence the relevant business activity;

4.1.9 proportionate: the content of records should be proportionate and appropriate to the relevant business activity and should not be excessive for that activity; and

4.1.10 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.

4.2 The Association prohibits staff from creating records that are misleading, false, fraudulent, sexually explicit, abusive, offensive, harassing, discriminatory, profane, libellous, defamatory, unethical, or that violate any legal or regulatory requirements. 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 significant reputational, regulatory and legal consequences for the Association.

5 Storage of and access to records

5.1 Records must be stored securely at the Association's premises or at a secure location in accordance with the Association's Privacy Policy and Information Security Policy to minimise the risk of damage, loss or unauthorised access to the records.

5.2 All records must be stored within the Association's document management or paper filing systems and must not be stored by staff in "personal drives" on computers or in personal paper files or notebooks. When storing records, staff must give records titles that accurately reflect their specific nature and contents. This ensures more universal availability of records within the Association and is conducive to their easy retrieval. It also facilitates the audit process, allows the Association to determine the types of records that it holds and where they are held and the identification of records for disposal at the end of their relevant retention periods.

5.3 Staff should dispose of ephemeral records on a routine basis. This includes hard copies of electronic documents, which have been printed by staff for a meeting or trivial e-mails or communications that should be deleted after being read, such as promotional e-mails or communications. This will reduce the

likelihood of duplicate and unnecessary records being stored within the Association's document management and paper filing systems.

5.4 Staff 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.

5.5 To ensure continuity of records in situations where the Association is procuring a new document management system, the Association 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. The Association will also take into consideration the advice and guidance of the DPO and the characteristics of a good records system contained within the Scottish Ministers' Code of Practice on Records Management issued under Section 61 of the Freedom of Information (Scotland) Act 2002.

5.6 When archiving paper records within the Association's storage facility, staff must clearly label storage boxes or folders.

6 Removal of records

6.1 Staff may remove records from the Association's premises only for legitimate business purposes, such as visiting service users at home or attending a meeting with an external agency. Staff must return records when they are no longer needed off-site for business purposes.

6.2 Staff must handle records removed from the Association's premises in accordance with the Information Security Policy.

7 Retention and destruction of records

7.1 Records must be kept for as long as they are required by relevant laws and for regulatory purposes and the Association's business needs, particularly for reference and accountability purposes.

7.2 The Association's Data Retention Policy sets out how long records will normally be held and when they will be destroyed. The Association will regularly review and update the Data Retention Policy with additional record types that it uses in the course of carrying out its functions and operations.

7.3 Records should not be disposed of or destroyed before the relevant retention period expires. The retention period specified in the Data Retention Policy 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. 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 the Association is, or is likely to be, involved. In such circumstances, staff must not alter, dispose of or destroy any relevant records required for the litigation until the DPO has advised that the retention and disposal of such records should resume in line with the Data Retention Policy. Special reasons may also exist in the case of those records which the Association has selected for permanent preservation.

7.4 A record cannot be considered to have been completely disposed of or destroyed until all copies (including back-up copies) have been destroyed.

7.5 If a record type is not listed in the Data Retention Policy or if staff have questions or concerns about retaining any records beyond the specified retention periods, staff must contact the DPO for guidance.

8 Failure to comply

8.1 The Association takes compliance with this policy very seriously. Failure to comply puts both staff and the Association at risk.

8.2 Due to the importance of this policy, failure to comply with any requirement of it may lead to disciplinary action for a member of staff, and this action may result in dismissal for gross misconduct.

8.3 Any questions or concerns about this policy should be directed to the DPO.

9 Review and updates to this policy

The Association will review and update this policy in accordance with its legal obligations and may amend, update or supplement it from time to time and at least every 3 years or earlier, if required by changes in legislation or technology underlying its document management systems.

Anne Smith
Chief Executive

October 2024

Policy Review Consultation Process

Considered by the Management Team on	25th October 2024
APPROVED BY THE FINANCE, AUDIT AND CORPORATE GOVERNANCE COMMITTEE ON	**7th November 2024**
APPROVED BY THE BOARD OF MANAGEMENT COMMITTEE ON	**28th November 2024**
Date of Next Review	**October 2027**