RECORDS MANAGEMENT POLICY

Reference	CS-CC-08
Information Classification	Public
Review Frequency	3 years
Date Reviewed/Approved	March 2026
Next Review Due Date	March 2029
Applicable Committee(s)	SMT
Owner - role	Compliance Advisor

Record of Updates/Changes			
Current Version	**Date Approved**	**Approved By**	**Changes**
V2		SMT	Changes to Section 8
V3			Updates to Appendix 1 (Maintenance of Records section) – to reflect system changes

1. INTRODUCTION

Records management is vital to the delivery of Castlehill Housing Association (CHA)'s services in an orderly, efficient and accountable manner.

Records contain information, which is a valuable resource and operational asset. Effective records management helps ensure CHA has the right information at the right time to make the right decisions.

2. SCOPE

This Policy applies to the management of all documents and records, in all formats, created or received by CHA.

This Policy applies to all staff, Management Committee Members, contractors, consultants and third parties who are given access to CHA documents and records and information processing facilities.

3. DEFINITIONS

A record is a document (created or received) which facilitates and supports the work of CHA and which is retained for a defined period to provide evidence of CHA's activities or transactions. A record may be in printed or digital format.

Records Management is the efficient and systematic control of the creation, receipt, maintenance, use, storage, revision, retrieval, retention and disposal of records in a way that is administratively sound and legally compliant, meets the needs of CHA and preserves an adequate historical record.

4. PRINCIPLES OF RECORDS MANAGEMENT

Effective records management will ensure that the records being created and held by CHA are being managed and maintained in such a way that they:

- Are accurate, created for a specific purpose, organised and maintained up to date
- Meet all the internal business needs of CHA
- Provide evidence of transactions and business processes
- Enable the content of the record to be accessed, used and reused in a controlled and efficient manner
- Are held securely according to CHA and legislative requirements and thereafter appropriately and securely disposed of
- Comply with all regulatory and statutory requirements.

5. STATUTORY AND REGULATORY FRAMEWORK

CHA is a data controller with obligations set out in the Data Protection Act 2018 and designated as a Scottish public authority with obligations under the Freedom of Information (Scotland) Act 2002.

The legal and regulatory framework for records management includes:

- UK GDPR and The Data Protection Act 2018
- The Freedom of Information (Scotland) Act 2002
- Privacy and Electronic Communications Regulations 2003
- The Environmental Information (Scotland) Regulations 2004

6. POLICY REQUIREMENTS

CHA will:

- Ensure a consistent approach to managing information is adopted across CHA and covers the lifecycle of information (creation, filing, storage, processing, retention and disposal)
- Develop and instil a culture which acknowledges the value and benefits of effective records management within CHA
- Ensure information is accurate, up to date and readily accessible to those who need it and also held according to CHA's record retention periods, in an organised and secure environment
- Provide appropriate guidance and training in relation to records management

CHA's Records Management Procedures, as detailedin Appendix 1 set out specific requirements regarding how records must be managed, including:

- Creation of records – including consistent file naming conventions
- Secure storage of records – including managing shared drives by defining access rights and consistent filing
- Regular disposal of records, in accordance with CHA's record retention periods

7. DUTIES AND RESPONSIBILITIES

CHA has a responsibility to ensure that our records are managed well. Specific record management roles and responsibilities are set out below.

The **Chief Executive** has overall responsibility for this Policy.

The **Senior Management Team** have operational responsibility for implementation of this Policy.

Line Managers are responsible for ensuring that information held within their departments or their area of responsibility is managed in compliance with this Policy and procedures.

The **Compliance Advisor** is responsible for undertaking regular compliance audits.

All staff and Committee Members are responsible for ensuring they act in accordance with this Policy and procedures.

8. POLICY COMPLIANCE AND AUDIT

The Compliance Advisor must verify compliance with this Policy and procedures.

The Compliance Advisor will keep a record of all Data Sharing Arrangements between the organisation and third parties that are not otherwise covered by the Association's Fair Processing Notice.

The Compliance Advisor or an individual appointed by the Compliance Advisor will on a quarterly basis:

- Conduct a clear desk audit.
- Audit a sample of former tenant files across all systems handling tenant data to ensure compliance with data retention periods.
- Audit a sample of former staff files to ensure compliance with data retention periods.

The Compliance Advisor or an individual appointed by the Compliance Advisor will on an annual basis:

- Liaise with Managers to ensure expired contract documentation is held for no longer than six years.

Any queries regarding the implications of this Policy or how it may apply, should be directed to CHA's Compliance Advisor.

APPENDIX 1 -PROCEDURES

These Procedures have been developed, in accordance with CHA's Records Management Policy, to ensure a consistent and effective approach to records management across CHA.

CREATION OF RECORDS

- The file name of all electronic records should start with the creation date e.g. for a file created on 1st April 2020, the file name should be '200401 Letter from CHA regarding X'.
- Draft versions must be clearly marked as draft. If there are multiple drafts and a final version, clear and consistent version control must be used.

MAINTENANCE OF RECORDS

- Electronic records, including scanned records, must be securely stored in CHA information management systems (Homemaster and/or PeopleHR) and/or on SharePoint.
- Paper records must only be stored when legally required. Any necessary paper records must be securely stored in appropriate CHA storage facilities.
- Payroll records should be securely stored in Paycircle cloud storage and/or on SharePoint.
- Scanned records must be quality checked to ensure reliability before the original paper is destroyed.

INFORMATION SHARING

- Information and records are an asset to which all staff may have access, except where the nature of the information requires restrictions, such as personal information. Restrictions should not be imposed unnecessarily.
- For information sharing with third parties, please refer to CHA's Data Protection Policy.

DESTRUCTION OF RECORDS

- Records scheduled for destruction must be approved by the relevant Line Manager responsible for the activities covered by the records.
- In the event that a record is not covered by CHA's record retention periods, please refer to CHA's Compliance Advisor.

In the event that records are mistakenly destroyed or lost following a disaster, every effort must be made to recover them. In the first instance, by contacting our IT Managed Support Provider and, if considered necessary, in accordance with CHA's IT Disaster Recovery Policy.