



DATA RETENTION POLICY

Adopted: November 2019

Last Reviewed: 16.2.23

Next Review Due: Feb 2026

This policy document can be produced in various formats, for instance, in larger print or audio-format; and it can also be translated into other languages, as appropriate.

1 Introduction

- 1.1 Our corporate information, records and data are important to how we conduct business and manage employees.
- 1.2 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our business operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our business.
- 1.3 This Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.
- 1.4 Failure to comply with this Policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.
- 1.5 This Policy covers all data that we hold or have control over. This includes physical data, such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data, such as e-mails and electronic documents. It applies to both personal data and non-personal data. In this Policy, we refer to this information and these records collectively as “data”.
- 1.6 This Policy also covers data that is held by third parties on our behalf, for example, cloud storage providers or offsite data storage.

2 Guiding principles

- 2.1 Through our data retention practices, we aim to meet the following commitments:
 - 2.1.1 We comply with legal and regulatory requirements to retain data.
 - 2.1.2 We comply with our data protection obligations, in particular, to keep personal data no longer than is necessary for the purposes for which it is processed.
 - 2.1.3 We handle, store and dispose of data responsibly and securely.
 - 2.1.4 We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good business reason.
 - 2.1.5 We allocate appropriate resources, roles and responsibilities to data retention.
 - 2.1.6 We regularly remind employees of their data retention responsibilities.
 - 2.1.7 We regularly monitor and audit compliance with this Policy and update this Policy when required.

3 Role and responsibilities

- 3.1 We aim to comply with the laws, rules, and regulations that govern our organisation and with recognised good practices. All employees must comply with this Policy. Failure to do so may subject us to serious civil and / or criminal liability.
- 3.2 Managers in conjunction with our Data Protection Officer (DPO) are responsible for identifying the proper period of retention for our data and for providing guidance and training to employees in relation to this Policy. Employees are, however, responsible for handling the destruction of data whose retention period has expired.

4 Recommended retention periods

- 4.1 Certain data is more important to us and is therefore listed in the recommended retention periods set out in the Schedule to this Policy as being required to be retained permanently. This may be because we have a legal requirement to retain it permanently (so that we can produce it in the future), or because we may need it as evidence of our transactions, or because it is important to the running of our business. The period specified for any personal data is the maximum and the period specified for any non-personal data is the minimum retention period.
- 4.2 Some data may be discarded or deleted once it has served its useful purpose or the period for bringing any claims against us has expired. The recommended retention periods set out in the Schedule to this Policy specify time periods for the retention of such data. Such data should not be retained beyond this period, unless a valid and strong business reason justifies its continued retention. If employees are unsure whether to retain certain data beyond the recommended retention period, they should consult the DPO.
- 4.3 If data is not listed in the recommended retention periods set out in the Schedule to this Policy, employees should consult the DPO for guidance.

5 Disposal and destruction of data

- 5.1 Hard copy data must be destroyed by shredding via the external contractor and electronic data must be deleted securely in a manner that it cannot be reconstituted after it has been deleted. Hard disk drives must be securely destroyed. No hard copy data should be destroyed by recycling.
- 5.2 Data must not be destroyed if the DPO confirms that its continued retention is relevant and necessary for the purposes of legal proceedings in which we are involved.

6 Consequences of failure to comply

- 6.1 We take compliance with this Policy very seriously. Failure to comply with the Policy may lead to disciplinary action.
- 6.2 Any questions or concerns about this Policy should be directed to Managers or the DPO.

7 Review and updates to this Policy

We will review and update this Policy in accordance with our data protection obligations and we may amend, update or supplement it from time to time and at least every 3 years or earlier, if required by changes in legislation.

APPENDIX 1 – RECORDS MANAGEMENT STRATEGY

Date this version 16.2.23

1 Introduction

- 1.1 OTHA 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. OTHA will adopt a systematic approach to records management. This is necessary to protect and preserve records to support OTHA's functions and operations and provide evidence of events, activities and transactions.
- 1.2 Guidance on the appropriate records management approach is detailed in OTHA's Records Management Strategy and is part of the overall OTHA's Retention Policy.
- 1.3 Managing records appropriately reduces the costs and risks associated with retaining unnecessary information and is core to complying with legal and regulatory requirements, including:
 - 1.3.1 UK General Data Protection Regulation;
 - 1.3.2 Data Protection Act 2018;
 - 1.3.3 Freedom of Information (Scotland) Act 2002;
 - 1.3.4 Environmental Information (Scotland) Regulations 2004;
 - 1.3.5 Equalities Act 2010
- 1.4 OTHA will comply with the Scottish Ministers' Code of Practice on Records Management recommendations, issued under Section 61 of the Freedom of Information (Scotland) Act 2002.
- 1.5 This strategy, as part of the Data Retention Policy, is an organisational commitment to effective records management at OTHA.

2 Responsibility and scope

- 2.1 Managers are responsible for implementing this strategy, assisting staff in maintaining appropriate information audits for their departments, providing guidance on records retention and training staff on records management.
- 2.2 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.

3 Records management strategy

Good records management relies on an effective strategy which is clear on how records should be held.

For OTHA this would be "DIGITAL FIRST" – reducing reliance on paper records and holding digital records in the appropriate location. This supports the principles of Data Minimisation and Accuracy of Data in the UK GDPR principles.

The following table sets out the high level strategy by department

Action	Paper records	Emails	Digital records
What to do	All paper records to be scanned and stored in the relevant department system such as SDM, HR System or share drives.	All emails and their attached files to be stored in the relevant section of the system or share drive.	Held in relevant system or share drive, in line with retention schedule and with suitable access controls in place
Follow up action	Paper record will then be shredded as soon as scan has been checked for accuracy.	Emails can be deleted in line with Retention Schedule of 12 months	Back ups and other data resilience solutions will be in line with the Retention schedule
Exemptions	Exemptions would be insurance and other certificates of incorporation and as required under relevant laws.	Possible exemptions would be where there is a requirement to hold for a legal requirement – such as criminal court case, tribunal	Review of certain records may require them to be held for longer and as an exemption to the retention schedule – examples would be due to legal requirements, legitimate interest, consent from data subject.

4 Records management principles

- 4.1 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, OTHA'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, OTHA can ensure its records demonstrate the key features of authenticity, reliability, integrity and accessibility.
- 4.2 The main benefits of good records management at OTHA are:
- 4.2.1 promotes the creation and storage of accurate and reliable records in a managed environment, which provide an audit trail of actions.
 - 4.2.2 increases organisational and administrative effectiveness, efficiency and service delivery through improved access to and retrieval of high quality records;
 - 4.2.3 helps enhance information security by facilitating improved confidentiality, integrity and availability of records;
 - 4.2.4 improves working environments and more economical use of physical and server space through reducing the retention of irrelevant, duplicate and out-of-date records;
 - 4.2.5 promotes OTHA's physical and intellectual control of all records by knowing what records it has and how and where to retrieve them easily;
 - 4.2.6 ensures that OTHA identifies and retains records of historical and evidential value to OTHA as a "corporate memory" and to assist in managing future recurrences of specific events;
 - 4.2.7 helps to maintain audit trails relating to access and alteration of records;
 - 4.2.8 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;
 - 4.2.9 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 OTHA's operations; and
 - 4.2.10 assists in compliance with all legal and regulatory obligations, including responding to requests for information and personal data made to OTHA.

4.3 The risks to OTHA in not maintaining effective records management are:

- 4.3.1 poor quality decisions being made on the basis of inaccurate, incomplete or out-of-date records;
- 4.3.2 levels of service to service users being inconsistent due to records of previous actions being unavailable;
- 4.3.3 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;
- 4.3.4 non-compliance with legal or regulatory requirements applicable to OTHA;
- 4.3.5 failure to identify, protect and retain records that are critical to business continuity;
- 4.3.6 additional costs incurred in storing records for longer than necessary; and
- 4.3.7 wasted time and resources in searching for records in response to a request received.

5 Storage of and access to records

- 5.1 Records must be stored securely at OTHA's premises or at a secure location in accordance with the OTHA's Data Protection Policy to minimise the risk of damage, loss or unauthorised access to the records.
- 5.2 Staff should only access records on a strict "need to know" basis, depending on the nature of a record and its relevance to the work of staff.

6 Retention and destruction of records

OTHA's Data Retention Policy sets out how long records will normally be held and when they will be destroyed. OTHA 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 Failure to comply

- 7.1 OTHA takes compliance with this strategy very seriously. Failure to comply puts both staff and OTHA at risk.
- 7.2 Due to the importance of this policy, failure to comply with any requirement of it may lead to disciplinary action.
- 7.3 Any questions or concerns about this policy should be directed to the Manager or the DPO.

8 Review and updates to this strategy

OTHA will review and update this strategy 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.

Appendix 2
SCHEDULE
RECOMMENDED DATA RETENTION PERIODS

Type of data	Recommended retention period
Governance and Management	
<ul style="list-style-type: none"> • Certificate of registration as a registered social landlord from SHR • Confirmation of registration as a Scottish charity from OSCR • Confirmation of charitable status from HMRC • Certificate of registration as a registered society with the FCA • Rules and Standing Orders 	Permanent
<ul style="list-style-type: none"> • Applications for membership 	5 years from date of end of membership
<ul style="list-style-type: none"> • Full membership register • Abbreviated membership register • Register of share certificates • Register of tenant organisations 	Permanent
<ul style="list-style-type: none"> • Governing Body member declarations of interest • Governing Body member documents, including appointment letters and bank details 	6 years from end of membership
<ul style="list-style-type: none"> • Governing Body (and AGM and SGM) minutes and resolutions (including special resolutions) 	Permanent
<ul style="list-style-type: none"> • Governing Body (and AGM and SGM) papers (including notice of Governing Body meetings, AGMs and SGMs) 	10 years from date of issue
<ul style="list-style-type: none"> • Register of Governing Body members 	Permanent
<ul style="list-style-type: none"> • Register of payments and benefits • Register of gifts and hospitality 	10 years from date of register entry
<ul style="list-style-type: none"> • Annual return on the Scottish Social Housing Charter, including supporting information 	5 years from date of submission
<ul style="list-style-type: none"> • Annual return to the FCA 	Permanent
<ul style="list-style-type: none"> • Business plans and supporting documentation • Business continuity plans 	5 years from date of completion

Type of data	Recommended retention period
<ul style="list-style-type: none"> Risk registers 	Permanent
Housing Management and Financial Inclusion / Income Maximisation	
<ul style="list-style-type: none"> Housing application form (including equalities and medical information) Tenancy offer letters Tenant visit records Tenancy agreement Correspondence to and from tenants Tenants' contact details Pet permissions Alterations permissions Changes to tenancy, including assignments, changes to joint tenancy, mutual exchange requests, sublets and succession forms and letters Powers of attorney / mandates of authority Guardianship documentation Tenancy reference requests (received and provided) Housing Benefit related documentation, including applications, claims (including reinstatement claims), consent mandates and correspondence to and from local authority Housing Benefit department Universal Credit related documentation Referrals for money and benefits advice Correspondence to and from support agencies Occupational therapists' reports End of tenancy form Eviction case files Void process documentation Communications with local authority regarding allocations Diary notes on document management system Court letters, documents and notices of proceedings, court reports, correspondence with solicitors and correspondence to and from Shelter 	6 years from date of end of tenancy (including moves)
<ul style="list-style-type: none"> Correspondence to and from DWP 	2 years
<ul style="list-style-type: none"> Correspondence to and from local authority Social Work department Occupational therapists' reports 	6 years

Type of data	Recommended retention period
<ul style="list-style-type: none"> Anti-social behaviour incidents, including Police reports, complaints, witness statements and noise recordings 	2 years or until the end of legal action
<ul style="list-style-type: none"> Abandonment files 	6 years from the date of end of tenancy
<ul style="list-style-type: none"> Unsuccessful housing applications 	6 years after notification of outcome of application
<ul style="list-style-type: none"> Tenant general (non-repair) satisfaction surveys and consultations 	6 years from date of completion
<ul style="list-style-type: none"> Advice regarding benefits, debts arrears reduction and income maximisation, including details of referrals to, and contact with, other agencies 	6 years from the date of end of tenancy
Maintenance and Works	
<ul style="list-style-type: none"> Gas records 	6 years from date of inspection
<ul style="list-style-type: none"> Decanting records Inspection / complaint file notes 	6 years from date of end of tenancy
<ul style="list-style-type: none"> Affordable Housing Supply Programme Funding documentation for adaptations Correspondence with tenant re: works and adaptations 	6 years from date of completion of works
<ul style="list-style-type: none"> Works orders 	Permanent
<ul style="list-style-type: none"> Stock condition surveys 	2 years from date of survey
<ul style="list-style-type: none"> Electrical records 	6 years from date of inspection
<ul style="list-style-type: none"> Insurance claims 	Life of company
<ul style="list-style-type: none"> Tenant repair satisfaction surveys and consultations 	6 years from date of completion
<ul style="list-style-type: none"> Alterations and Improvement applications 	6 years from date of approval
<ul style="list-style-type: none"> Tender / contract documentation for contracts 	3 years from date of contract completion
Factoring	
<ul style="list-style-type: none"> Factoring agreement and Written Statement of Services 	6 years from date of termination of factoring agreement

Type of data	Recommended retention period
<ul style="list-style-type: none"> Communal work requests 	6 years from the date of termination of factoring agreement
<ul style="list-style-type: none"> Change of ownership records in owner sale 	6 years from date of sale
Finance, Pensions and Insurance	
<ul style="list-style-type: none"> Accounting records (including cheque counterfoils, bank statements and reconciliations and charitable donations made) Auditing records Balance sheets and supporting documents VAT records and correspondence Invoices Credit and debit notes Cash records, including petty cash Creditor and debtor accounts Orders and delivery notes Budgets and internal financial reports 	7 years from the end of the relevant financial year
<ul style="list-style-type: none"> Signed versions of accounts Grant funding (HAG, etc.) 	Permanent
<ul style="list-style-type: none"> Tax returns 	10 years from the end of the relevant financial year
<ul style="list-style-type: none"> Tenant financial information, including bank details 	6 years after end of tenancy from the date of final payment
<ul style="list-style-type: none"> Rent payments, rent statements and rent refunds Arrears correspondence Debt recovery, earnings and bank arrestments Bankruptcy information 	6 years from date of end of tenancy
<ul style="list-style-type: none"> Employee salary records, records of overtime, bonuses and benefits in kind Pay As You Earn (PAYE) records, including wage sheets, deductions, working sheets, calculations of the PAYE income of employees and relevant payments to them, the deduction of tax from, or accounting for tax in respect of, such payments 	6 years from date of termination of employment

Type of data	Recommended retention period
<ul style="list-style-type: none"> Copies of notices to employees (e.g. P45, P60) HMRC correspondence in relation to tax codes, pay and tax details Travel and subsistence payments (including expense claims and payments), season ticket advances and loans to employees Employee income tax records Records of income on which National Insurance contributions are payable Records of employer's and employee's National Insurance contributions Correspondence with HMRC National minimum wage requirements records, including hours worked Statutory sick, maternity, paternity and shared parental pay records, calculations, certificates or other evidence Leave records 	
<ul style="list-style-type: none"> Pension actuarial valuation reports Returns of pension fund contributions Annual reconciliations of pension fund contributions 	Permanent
<ul style="list-style-type: none"> Documentation relating to retirement benefits 	6 years from end of scheme or other notifiable event taken place
<ul style="list-style-type: none"> Current and former insurance policies and certificates 	Permanent
<ul style="list-style-type: none"> Annual insurance schedules 	Permanent
Information Requests and Complaints	
<ul style="list-style-type: none"> Data Governance general 	<ul style="list-style-type: none"> Email 12 months CCTV – 30 days BWV – 30 days Call recordings – 30-90 days
<ul style="list-style-type: none"> GDPR subject access request register Third party disclosure register Environmental information request register 	6 years from date of register entry
<ul style="list-style-type: none"> GDPR subject access request case files, personal data provided, including legal advice and internal communications regarding request 	12 months from date of response / last contact

Type of data	Recommended retention period
<ul style="list-style-type: none"> Environmental information request case file, including record of correspondence with applicant and information provided 	
<ul style="list-style-type: none"> Complaints to the Information Commissioner (GDPR) and the Scottish Information Commissioner (environmental information) Complaints (including stage 2 complaints, correspondence with the SPSO and complaints performance reports) Data security incident and breach investigation documentation 	6 years from date of last action / report production / end of investigation
<ul style="list-style-type: none"> GDPR general compliance records 	2 years
<ul style="list-style-type: none"> Data security incident and breach register 	6 years
Health and Safety	
<ul style="list-style-type: none"> Health and safety assessments Health and safety policy statements Records of consultations with safety representatives 	Permanent
<ul style="list-style-type: none"> Health and safety statutory notices 	6 years after compliance
<ul style="list-style-type: none"> Records of reportable injuries, diseases or dangerous occurrences, including reportable incidents, reportable diagnoses and injury arising out of accident at work (and associated investigations and the accident book) 	5 years from date of the entry
<ul style="list-style-type: none"> Records of reportable injuries, diseases or dangerous occurrences, including reportable incidents, reportable diagnoses and injury arising out of accidents involving children (and associated investigations and the accident book) 	Depends on the requirements of the insurer (but minimum of 25 years)
<ul style="list-style-type: none"> Record of employees exposed to asbestos dust, including health records of each employee Medical records and details of biological tests under the Control of Lead at Work Regulations Medical records specified by the Control of Substances Hazardous to Health Regulations (COSHH) 	40 years from the date of the last entry made in the record

Type of data	Recommended retention period
<ul style="list-style-type: none"> Records of monitoring of exposures to hazardous substances (where exposure monitoring is required under COSHH) 	<p>Where the record includes the personal exposures of identifiable employees, 40 years from the date of the last entry made in the record.</p> <p>Otherwise, 5 years from the date of the last entry made in the record.</p>
<ul style="list-style-type: none"> Records of tests and examinations of control systems and protective equipment under COSHH 	5 years from the date on which the record was made
Recruitment and Human Resources	
<ul style="list-style-type: none"> Rejected job applicant records, including application letters or forms (including equal opportunities monitoring forms), CVs (including copies of qualifications), references and other pre-employment checks, interview notes, assessment and psychometric test results and correspondence concerning application 	6 months from date of notification of rejection
<ul style="list-style-type: none"> Application records of successful candidates, including application letters or forms (including equal opportunities monitoring forms), CVs (including copies of qualifications), references and other pre-employment checks, interview notes, assessment and psychometric test results and correspondence concerning employment 	6 years from date of termination of employment
<ul style="list-style-type: none"> Criminal records requirement assessments for a particular post, consisting of criminal records information forms and the recorded outcomes of Disclosure Scotland checks 	<p>12 months after the assessment was last used</p> <p>All other information, as soon as practicable after the check has been completed and the outcome recorded, unless the DPO assesses – in exceptional circumstances – that retention is relevant to the ongoing employment relationship, in which case, maximum retention period of 6 months after the check has been completed</p>

Type of data	Recommended retention period
<ul style="list-style-type: none"> Copies of identification documents Identification documents of foreign nationals (including right to work) 	Review and destroy once checked
<ul style="list-style-type: none"> Emergency contact details / next of kin 	Upon termination
<ul style="list-style-type: none"> Employment contracts, including personnel and training records, written particulars of employment and changes to terms and conditions of employment Employee performance and conduct records, probationary period reviews, review meeting and assessment interviews, appraisals and evaluations and promotions and demotions Death benefit nomination and revocation forms Resignation, termination and retirement records Grievances Collective workforce agreements Records concerning temporary employees 	6 years from date of termination of employment
<ul style="list-style-type: none"> Disciplinary investigations, including warnings 	6 months after conclusion of investigation or expiry of warning
<ul style="list-style-type: none"> Records relating to and / or showing compliance with Working Time Regulations, including registration of work and rest periods and working time opt-out forms 	2 years from the date on which the record was made
<ul style="list-style-type: none"> Trade union agreements 	10 years after ceasing to be effective
<ul style="list-style-type: none"> Occupational health records 	40 years after completion of assessment
<ul style="list-style-type: none"> Redundancy records 	6 years from date of redundancy if less than 20 redundancies/ 12 years if 20 or more redundancies
Contracts and Procurement	
<ul style="list-style-type: none"> Transfer Agreement 	30 years after the date of stock transfer
<ul style="list-style-type: none"> Contracts executed under seal 	20 years after the end of the contract
<ul style="list-style-type: none"> Contracts for the supply of goods or services, including professional services Documentation relating to small one-off purchases of goods and services where there 	6 years after the end of the contract

Type of data	Recommended retention period
<ul style="list-style-type: none"> is no continuing maintenance or similar requirement Licensing agreements Rental and hire purchase agreements Indemnities and guarantees 	
<ul style="list-style-type: none"> Loan agreements Right to buy sale documents 	Permanent
<ul style="list-style-type: none"> Forms of tender 	6 years after notification of award decision
<ul style="list-style-type: none"> Document relating to unsuccessful tenderers 	2 years after notification
<ul style="list-style-type: none"> Documents relating to successful tenderers 	6 years after the end of the contract
Property Records	
<ul style="list-style-type: none"> Leases and titles to property 	12 years after the end of the lease / ownership ceases
<ul style="list-style-type: none"> Development documentation 	Permanent
<ul style="list-style-type: none"> Wayleaves, licences and servitudes 	12 years after the rights that were granted or received cease to exist
<ul style="list-style-type: none"> Planning and building control permissions Title searches undertaken prior to purchase of property 	20 years after ownership ceases
<ul style="list-style-type: none"> Property maintenance records 	6 Years
Vehicles	
<ul style="list-style-type: none"> Ownership and registration documentation Maintenance records, including MOT tests and servicing Mileage records 	2 years after the date of disposal of vehicle
PR, Communications and Website	
<ul style="list-style-type: none"> Newsletter distribution lists (post) 	Until the recipient opts out of receiving the newsletter

Type of data	Recommended retention period
<ul style="list-style-type: none"> Social media posts 	2 years
<ul style="list-style-type: none"> Website contact forms / requests / enquiries / complaints 	Delete as soon as the form / request / enquiry / complaint has been transferred to the document management system, although the original may be retained for audit trail purposes for 2 years
<ul style="list-style-type: none"> Photographs (including consent forms, where available) 	Until the subject of the photograph objects to their photograph being used
Office and Administration	
<ul style="list-style-type: none"> Visitor book entries 	6 months from date of visit

