



DATA RETENTION POLICY

Governance and Business Improvement Manager

Contents

1. Introduction	3
2. Guiding Principles	3
3 Role and responsibilities	3
4. Recommended retention periods.....	4
5. Disposal and destruction of data	4
6. Consequences of failure to comply.....	5
7. Equality, Diversity & Inclusion.....	5
8. Data Protection	5
9. Policy Review	6
10. Associated Policies & Guidance	6
11. Responsibilities Chart.....	6
Policy Assessment Checklist.....	8
Health & Safety Assessment	8
Equality Impact Assessment	8
Data Protection Impact Assessment.....	9
RECOMMENDED DATA RETENTION PERIODS	11

r

Policy	Data Retention Policy								
Version reference	1.0								
Approved by	Board of Management								
Date of Approval	December 2024								
Review Period	3 years								
Review Due	December 2027								
Policy Review	Director of Finance & Business Support								
Who this policy affects	Board	X	Customers	X	Contractors	X	Members of the Public	X	
Where this policy affects	General needs		X	Supported		X	Office / staff base		X

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. Managers/Directors of departments are responsible for ensuring 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.
- 4.4 If records do not contain personal data, they can be kept for longer for example building surveys without personal data.

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.
- Paper documents must be disposed of in a timely manner in accordance with the retention periods specified in AHA's Retention Schedule.
 - Documentation that is to be disposed of is to be checked before disposal and any documents that contain personal data or sensitive information must be treated as confidential waste.
 - Confidential waste must not be left in areas accessible to the public or in areas where there are people who are not entitled to see it, for example, corridors, open-plan offices, unlocked offices, the reception area or anywhere in view of members of staff/visitors/public who should not have access to that information.
 - Any documents containing personal data must be disposed of as follows:
 - *By placing in confidential waste bins or bags*
 - *By shredding*
 - *By burning / incineration*
 - *By secure collection for disposal by specialist contractors, e.g., Shred-it*
 - Prior to disposal, hard copy documents are to be removed from folders, plastic/ paper wallets, box files, poly pockets etc. and paper clips, staples and treasury tags are to be removed.

- Recycling bins are available for paper documents that do not contain personal data or other sensitive data which doesn't require secure disposal or destruction.
- Electronic documents must be disposed of in a timely manner in accordance the retention periods specified in AHA's Retention Schedule.
- All electronic media devices including PCs, laptops, tablets, hard drives, removable hard drives, data sticks and mobile phones should be returned to the IT Department for destruction / disposal in an appropriate manner when they are no longer required.
- AHA uses a specialist company to dispose of electronic equipment. They will provide AHA with a Certificate of Secure Data Destruction which specifies the method of destruction. This will include the serial number(s) of any equipment they have disposed of.
- For the disposal and destruction of disks, DVDs, CDs, USBs, audio or video tapes (including CCTV footage if applicable), these should be passed to the ICT Manager who will record that they have been received and securely destroyed or disposed of.
- For documents, including emails, that are to be permanently deleted, i.e., put beyond use, the person deleting the document must do all that is reasonably and practicably possible to ensure that deletion has been done in such a way that the document cannot be recovered. For example, emails should also be deleted from the 'Deleted Items' folder.
- If any data subject exercises their right to Correct, Erase or Restrict the processing of any personal data held by AHA , we must ensure that this is also corrected on any backup drives or systems, whether they be AHA 's drives/systems or a data processors'.

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. This decision should be recorded by the DPO.

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. Equality, Diversity & Inclusion

- 7.1 Almond aims to ensure that equality, fairness, dignity and respect are central to the way we work and how we treat our customers. We support diversity and uphold equal opportunities in all areas of our work as an employer and service provider.
- 7.2 Almond will not discriminate against tenants, staff, visitors, suppliers or others based on their age, sex, sexual orientation, race, disability, religion or belief, marital status, pregnancy and maternity or gender reassignment (collectively referred to as 'protected characteristics' in the Equality Act 2010).

8. Data Protection

- 8.1 Our policies and procedures foster an approach of 'data protection by design and by default'. What this means in practice is that:
- Policies and procedures consider data protection issues, i.e. how to protect the data subject served by the policy or procedure;

- New systems, services, products and business practices involving personal data are designed and implemented to ensure personal data is protected by default;
- That the Data protection principles and safeguarding of individuals' rights (such as data minimisation, pseudo anonymisation, and purpose limitation) are clear in the policy or procedure;
- And that if the policy or procedure aims to provide service to vulnerable groups (e.g. children) that the personal data is treated with extra protection.

What this requires users of this policy to do is:

- Make sure that staff understand why data protection is important for the implementation of this policy, for instance via training or by reading the data protection policies;
- If we are undertaking a review of the policy, change to process or change to system, that we must consider doing a Data Protection Impact assessment, if the change is likely to result in a high risk to individuals.
- It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

We will consult our data protection officer, if there is doubt over these requirements.

9. Policy Review

- 9.1 This policy will be reviewed every three years or as required due to legislative or regulatory change. The review will be completed by the Governance and Business Improvement Manager and circulated to the Board of Management for approval.

10. Associated Policies & Guidance

- 10.1 This Policy takes account of the following documents:

- Rules of Almond Housing Association
- Equity, Diversity and Inclusion Policy
- Data Protection Policy
- Records Management Policy
- Document Management (Off site Storage) Procedure
- Scottish Federation of Housing Association's Code of Conduct for Governing Body Members
- Scottish Housing Regulatory Standards of Governance & Financial Management

11. Responsibilities Chart

- 11.1 The chart below illustrates the responsibilities of all staff in relation to this policy.

	Board	CEO	Director of Finance & Business Support	Governance Manager	All Staff
To Implement the policy		✓		✓	✓
Ensure Almond HA staff have an understanding of Policy				✓	
Policy Review			✓	✓	
Ensure Policy Reviewed	✓			✓	

Ensure Equality & Diversity guidance is adhered to					✓
Appeals process	✓				

Policy Assessment Checklist

Health & Safety Assessment

Does this policy have the potential to affect:

	Yes	No
Lone Working	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Safety and/or wellbeing of customers	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Safety and/or wellbeing of staff	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Equality Impact Assessment

Does this policy have the potential to affect:

	Yes	No
Age	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Disability	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Gender reassignment	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Marriage and Civil Partnership	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Pregnancy and Maternity	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Religion or belief	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Sex	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Sexual orientation	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Race	<input type="checkbox"/>	<input checked="" type="checkbox"/>

If you have answered 'Yes' to any of these points, please complete a full Equality Impact Assessment. If you have answered 'No', you need take no further action in completing an Equality Impact Assessment.

Data Protection Impact Assessment

Carrying out a Data Protection Impact Assessment [DPIA] will be useful to any project – large or small – that:

- Involves personal or sensitive data about individuals
- May affect our customers' reasonable expectations relating to privacy
- Involves information that may be used to identify or target individuals

A Data Protection Impact Assessment [DPIA] must be completed if the policy involves one or more of the following (please tick each that apply to this policy):

Evaluation or scoring	<input type="checkbox"/>
Automated decision-making with significant effects;	<input type="checkbox"/>
<i>Systematic monitoring</i>	<input type="checkbox"/>
<i>Processing of sensitive data or data of a highly personal nature</i>	<input checked="" type="checkbox"/>
<i>Processing on a large scale</i>	<input checked="" type="checkbox"/>
<i>Processing of data concerning vulnerable data subjects</i>	<input checked="" type="checkbox"/>
<i>Innovative technological or organisational solutions</i>	<input type="checkbox"/>
<i>Processing that involves preventing data subjects from exercising a right or using a service or contract</i>	<input type="checkbox"/>
<i>Use systematic and extensive profiling or automated decision-making to make significant decisions about people</i>	<input type="checkbox"/>
<i>Process special-category data or criminal-offence data on a large scale</i>	<input type="checkbox"/>
<i>Systematically monitor a publicly accessible place on a large scale</i>	<input type="checkbox"/>
<i>Use of new technologies involving significant innovation</i>	<input type="checkbox"/>
<i>Use profiling, automated decision-making or special category data to help Make decisions on someone's access to a service, opportunity or benefit</i>	<input type="checkbox"/>
<i>Carry out profiling on a large scale</i>	<input type="checkbox"/>
<i>Process biometric or genetic data</i>	<input type="checkbox"/>
<i>Combine, compare or match data from multiple sources</i>	<input type="checkbox"/>
<i>Process personal data without providing a privacy notice directly to the individual</i>	<input type="checkbox"/>
<i>Process personal data in a way that involves tracking individuals' online or offline location or behaviour</i>	<input type="checkbox"/>
<i>Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them</i>	<input type="checkbox"/>
<i>Process personal data that could result in a risk of physical harm in the event of a security breach</i>	<input type="checkbox"/>
<i>There is a change to the nature, scope, context or purposes of our processing</i>	<input type="checkbox"/>

If a DPIA is not carried out, please summarise the reasons below

In adhering to this policy, we are adhering to the principles of UK GDPR. Data processing within the context of this policy is a requirement to comply with GDPR.

Appendix 1

SCHEDULE

RECOMMENDED DATA RETENTION PERIODS

(Note – records that do not contain any personal data can be retained for longer than detailed below where required to be retained longer for business purposes)

Type of data	Recommended retention period	Format	Responsible
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	Electronic and may also be hard copy	Chief Executive
<ul style="list-style-type: none"> • Applications for membership 	5 years from date of end of membership	Electronic and may also be hard copy	Director of Finance and Business Support
<ul style="list-style-type: none"> • Full membership register • Abbreviated membership register • Register of share certificates • Register of tenant organisations 	Permanent	Electronic	Chief Executive
<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	Electronic	Director of Finance and Business Support
<ul style="list-style-type: none"> • Governing Body (and AGM and SGM) minutes and resolutions (including special resolutions) 	Permanent	Electronic and may also be hard copy	Chief Executive
<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	Electronic	Chief Executive

Type of data	Recommended retention period	Format	Responsible
<ul style="list-style-type: none"> Register of Governing Body members 	Permanent	Electronic	Director of Finance and Business Support
<ul style="list-style-type: none"> Register of payments and benefits Register of gifts and hospitality 	10 years from date of register entry	Electronic	Director of Finance and Business Support
<ul style="list-style-type: none"> Annual return on the Scottish Social Housing Charter, including supporting information 	5 years from date of submission	Electronic	Chief Executive
<ul style="list-style-type: none"> Annual return to the FCA 	Permanent	Electronic and may be also be hard copy	Director of Finance and Business Support
<ul style="list-style-type: none"> Business plans and supporting documentation Business continuity plans 	5 years from date of completion	Electronic	Chief Executive
<ul style="list-style-type: none"> Risk registers 	Permanent	Electronic and may be also be hard copy	Chief Executive
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 assignations, 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 	6 years from date of end of tenancy (including moves)	Electronic and may be also be hard copy	Director of Housing Management

Type of data	Recommended retention period	Format	Responsible
reinstatement claims), consent mandates and correspondence to and from local authority Housing Benefit department <ul style="list-style-type: none"> • 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 			
<ul style="list-style-type: none"> • Correspondence to and from DWP 	2 years	Electronic	Director of Housing Management
<ul style="list-style-type: none"> • Correspondence to and from local authority Social Work department • Occupational therapists' reports 	6 years from end of tenancy	Electronic	Director of Housing Management
<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	Electronic	Director of Housing Management
<ul style="list-style-type: none"> • Abandonment files 	6 years from the date of end of tenancy	Electronic	Director of Housing Management
<ul style="list-style-type: none"> • Unsuccessful housing applications 	6 years after notification of outcome of application	Electronic	Director of Housing Management
<ul style="list-style-type: none"> • Tenant general (non-repair) satisfaction surveys and consultations 	6 years from date of completion	Electronic	Director of Housing Management

Type of data	Recommended retention period	Format	Responsible
<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	Electronic and may be also be hard copy	Director of Housing Management
Maintenance and Works			
<ul style="list-style-type: none"> Gas records 	6 years from date of inspection	Electronic	Director of Asset Management
<ul style="list-style-type: none"> Decanting records Inspection / complaint file notes 	6 years from date of end of tenancy	Electronic and may be also be hard copy	Director of Asset Management
<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	Electronic and may also be hard copy	Director of Asset Management
<ul style="list-style-type: none"> Works orders 	Permanent	Electronic	Director of Asset Management
<ul style="list-style-type: none"> Stock condition surveys 	2 years from date of survey (if does not contain personal data can be kept as long as necessary)	Electronic	Director of Asset Management
<ul style="list-style-type: none"> Electrical records 	6 years from date of inspection	Electronic	Director of Asset Management
<ul style="list-style-type: none"> Insurance claims 	Life of company	Electronic and may also be hard copy	Director of Asset Management
<ul style="list-style-type: none"> Tenant repair satisfaction surveys and consultations 	6 years from date of completion	Electronic	Director of Asset Management
<ul style="list-style-type: none"> Alterations and Improvement applications 	6 years from date of approval	Electronic	Director of Asset Management
<ul style="list-style-type: none"> Tender / contract documentation for contracts 	3 years from date of contract completion	Electronic	Director of Asset Management
Factoring			

Type of data	Recommended retention period	Format	Responsible
<ul style="list-style-type: none"> Factoring agreement and Written Statement of Services 	6 years from date of termination of factoring agreement	Electronic and may also be hard copy	Director of Housing Management
<ul style="list-style-type: none"> Communal work requests 	6 years from the date of termination of factoring agreement	Electronic and may also be hard copy	Director of Housing Management
<ul style="list-style-type: none"> Change of ownership records in owner sale 	6 years from date of sale	Electronic	Director of Housing Management
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	Electronic	Director of Finance and Business Support
<ul style="list-style-type: none"> Signed versions of accounts Grant funding (HAG, etc.) 	Permanent	Electronic and may also be hard copy	Director of Finance and Business Support
<ul style="list-style-type: none"> Tax returns 	10 years from the end of the relevant financial year	Electronic	Director of Finance and Business Support
<ul style="list-style-type: none"> Tenant financial information, including bank details 	6 years after end of tenancy from the date of final payment	Electronic and may also be hard copy	Director of Finance and Business Support

Type of data	Recommended retention period	Format	Responsible
<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	Electronic and may also be hard copy	Director of Finance and Business Support
<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 • 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 	6 years from date of termination of employment	Electronic and may also be hard copy	Director of Finance and Business Support

Type of data	Recommended retention period	Format	Responsible
<ul style="list-style-type: none"> Pension actuarial valuation reports Returns of pension fund contributions Annual reconciliations of pension fund contributions 	Permanent	Electronic and may also be hard copy	Director of Finance and Business Support
<ul style="list-style-type: none"> Documentation relating to retirement benefits 	6 years from end of scheme or other notifiable event taken place	Electronic	Director of Finance and Business Support
<ul style="list-style-type: none"> Current and former insurance policies and certificates 	Permanent	Electronic and may also be hard copy	Director of Finance and Business Support
<ul style="list-style-type: none"> Annual insurance schedules 	Permanent	Electronic and may also be hard copy	Director of Finance and Business Support
Information Requests and Complaints			
<ul style="list-style-type: none"> Data Governance general 	<ul style="list-style-type: none"> Email 12 months CCTV – 14 days Call recordings – 30-90 days 	Electronic	ICT Manager
<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	Electronic	Governance & Business Improvement Manager
<ul style="list-style-type: none"> GDPR subject access request case files, personal data provided, including legal advice and internal communications regarding request. Environmental information request case file, including record of correspondence with applicant and information provided 	12 months from date of response / last contact (can keep for longer if anonymised)	Electronic	Governance & Business Improvement Manager

Type of data	Recommended retention period	Format	Responsible
<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	Electronic	Governance & Business Improvement Manager
<ul style="list-style-type: none"> GDPR general compliance records 	2 years	Electronic	Governance & Business Improvement Manager
<ul style="list-style-type: none"> Data security incident and breach register 	6 years	Electronic	Governance & Business Improvement Manager
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	Electronic and may also be hard copy	Director of Asset Management
<ul style="list-style-type: none"> Health and safety statutory notices 	6 years after compliance	Electronic	Director of Asset Management
<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	Electronic	Director of Asset Management
<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 	Depends on the requirements of the insurer (but minimum of 25 years)	Electronic	Director of Asset Management

Type of data	Recommended retention period	Format	Responsible
investigations and the accident book)			
<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	Electronic and may also be hard copy	Director of Asset Management
<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>	Electronic and may also be hard copy	Director of Asset Management
<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	Electronic	Director of Asset Management
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 	6 months from date of notification of rejection	Electronic	People and Culture Manager

Type of data	Recommended retention period	Format	Responsible
checks, interview notes, assessment and psychometric test results and correspondence concerning application			
<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	Electronic	People and Culture Manager
<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>	Electronic	People and Culture Manager

Type of data	Recommended retention period	Format	Responsible
<ul style="list-style-type: none"> • Copies of identification documents • Identification documents of foreign nationals (including right to work) 	Review and destroy once checked	Electronic	People and Culture Manager
<ul style="list-style-type: none"> • Emergency contact details / next of kin 	Upon termination	Electronic	People and Culture Manager
<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	Electronic and may also be hard copy	People and Culture Manager
<ul style="list-style-type: none"> • Disciplinary investigations, including warnings 	6 months after conclusion of investigation or expiry of warning	Electronic	People and Culture Manager
<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	Electronic	People and Culture Manager
<ul style="list-style-type: none"> • Trade union agreements 	10 years after ceasing to be effective	Electronic	People and Culture Manager
<ul style="list-style-type: none"> • Occupational health records 	40 years after completion of assessment	Electronic	People and Culture Manager

Type of data	Recommended retention period	Format	Responsible
<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	Electronic	People and Culture Manager
Contracts and Procurement			
<ul style="list-style-type: none"> Transfer Agreement 	30 years after the date of stock transfer	Electronic and may also be hard copy	Chief Executive
<ul style="list-style-type: none"> Contracts executed under seal 	20 years after the end of the contract	Electronic and may also be hard copy	Relevant department Director/Manager
<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 is no continuing maintenance or similar requirement Licensing agreements Rental and hire purchase agreements Indemnities and guarantees 	6 years after the end of the contract	Electronic	Relevant department Director/Manager
<ul style="list-style-type: none"> Loan agreements Right to buy sale documents 	Permanent	Electronic and may also be hard copy	Chief Executive
<ul style="list-style-type: none"> Forms of tender 	6 years after notification of award decision	Electronic	Relevant department Director/Manager
<ul style="list-style-type: none"> Document relating to unsuccessful tenderers 	2 years after notification	Electronic	Relevant department Director/Manager
<ul style="list-style-type: none"> Documents relating to successful tenderers 	6 years after the end of the contract	Electronic	Relevant department Director/Manager
Property Records			

Type of data	Recommended retention period	Format	Responsible
<ul style="list-style-type: none"> Leases and titles to property 	12 years after the end of the lease / ownership ceases	Electronic	Director of Housing Management
<ul style="list-style-type: none"> Development documentation 	Permanent	Electronic and may also be hard copy	Director of Asset Management
<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	Electronic and may also be hard copy	Director of Asset Management
<ul style="list-style-type: none"> Property maintenance records 	6 Years	Electronic	Director of Asset Management
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	Electronic	Director/Manager of department that manages vehicles
PR, Communications and Website			
<ul style="list-style-type: none"> Newsletter distribution lists (post) 	Until the recipient opts out of receiving the newsletter	Electronic	People and Culture Manager
<ul style="list-style-type: none"> Social media posts 	2 years	Electronic	People and Culture Manager
<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,	Electronic	People and Culture Manager

Type of data	Recommended retention period	Format	Responsible
	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	Electronic	People and Culture Manager
Office and Administration			
<ul style="list-style-type: none"> Visitor book entries 	6 months from date of visit	Electronic or hard copy	Director of Housing Management