

CLYDESDALE HOUSING ASSOCIATION LIMITED

Policy:	Privacy Policy
Date:	24 June 2026
Lead Officer:	Chief Executive
Review Date:	24 June 2029

Regulatory Requirements:

- 3.5 Landlords must ensure that they meet all of their legal duties and responsibilities and that they adhere to relevant guidance and the requirements of other regulators.

Regulatory Standards:

Standard 1

Regulatory Guidance 1.3

The governing body ensures the RSL complies with its constitution and its legal obligations. Its constitution adheres to these Standards and the constitutional requirements set out below.

Standard 2

Regulatory Guidance 2.3

The governing body is open and transparent about what it does, publishes information about its activities and, wherever possible, agrees to requests for information about the work of the governing body and the RSL.

Regulatory Guidance 2.5

The RSL is open, co-operative, and engages effectively with all its regulators and funders, notifying them of anything that may affect its ability to fulfil its obligations. It informs the Scottish Housing Regulator about any significant events such as a major issue, event or change as set out and required in the notifiable events guidance.

Clydesdale Housing Association will provide this policy on request at no cost, in large print, in Braille, in audio or other non-written format, and in a variety of languages.



CONTENTS

1.	Introduction	3
2.	Legislation	3
3.	Data.....	3
4.	Processing of Personal Data	4
5.	Data Sharing	5
6.	Data Storage and Security	6
7.	Breaches	7
8.	Data Protection Officer (“DPO”).....	7
9.	Data Subject Rights.....	8
10.	Privacy Impact Assessments (“PIAs”)	10
11.	Archiving, Retention and Destruction of Data	10
Appendix 1: List of Related Policies.....		11
Appendix 2: Table of Duration of Retention of certain Data.....		12

1. Introduction

- 1.1 Clydesdale Housing Association Limited (hereinafter referred to as the “Association”) is committed to ensuring the secure and safe management of data held by the Association in relation to customers, staff and other individuals. The Association’s staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals’ data in accordance with the procedures outlined in this policy and documentation referred to herein.
- 1.2 The Association needs to gather and use certain information about individuals. These can include customers (tenants, factored owners etc.), employees and other individuals that the Association has a relationship with. The Association manages a significant amount of data, from a variety of sources. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the GDPR).
- 1.3 This Policy sets out the Association’s duties in processing that data, and the purpose of this Policy is to set out the procedures for the management of such data.
- 1.4 Appendix 1, which is attached, details the Association’s related policies.
- 1.5 The Data (Use and Access) Act 2025 (“**DUA**”) and associated legislation/regulation will make changes to data protection law meaning that the functions of the Information Commissioner will be transferred to the Information Commission. At the time of preparing this Policy these changes are yet to come into force. Until such time as these changes come into force references in this Policy to the “Information Commission” (and any associated expressions) should be treated as a reference to the Information Commissioner.

2. Legislation

- 2.1 It is a legal requirement that the Association process data correctly; the Association must collect, handle and store personal information in accordance with the relevant legislation.
- 2.2 The relevant legislation in relation to the processing of data is:
 - (a) the UK General Data Protection Regulation (“the GDPR”);
 - (b) the Privacy and Electronic Communications (EC Directive) Regulations 2003;
 - (c) the Data Protection Act 2018 (“the 2018 Act”) and
 - (d) any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the UK GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003 or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union

3. Data

- 3.1 The Association holds a variety of Data relating to living individuals, including customers and employees (referred to as Data Subjects). Data which can identify Data Subjects and relates to them is known as Personal Data. The Personal Data held and processed by the Association is detailed within a Fair Processing Notice and the Data Protection Addendum of the Terms of and Conditions of Employment which is provided to all employees.

- 3.1.1 “Personal Data” is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by the Association and which relates to individuals.
- 3.1.2 The Association also holds Personal Data that is sensitive in nature (i.e. relates to or reveals a Data Subject’s racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is “Special Category Personal Data” or “Sensitive Personal Data”. The Secretary of State may designate further categories of Special Category Personal Data and if this occurs the Association shall treat any such designated data accordingly.

4. Processing of Personal Data

4.1 The Association is permitted to process Personal Data on behalf of Data Subjects provided it is doing so on one of the following grounds:

- Processing with the consent of the Data Subject (see clause 4.4 hereof);
- Processing is necessary for the performance of a contract between the Association and the Data Subject or for entering into a contract with the Data Subject;
- Processing is necessary for the Association’s compliance with a legal obligation;
- Processing is necessary to protect the vital interests of the Data Subject or another person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the Association’s official authority;
- Processing is necessary for the purposes of legitimate interests pursued by the Association or by a third party; or
- Processing is necessary for the purposes of a recognised legitimate interest.

4.2 Fair Processing Notice

4.2.1 The Association has produced a Fair Processing Notice (FPN) which it is required to provide to all customers whose Personal Data is held by the Association. That FPN must be provided to the customer from the outset of processing their Personal Data and they should be advised of the terms of the FPN when it is provided to them. If the Association receives personal data about an individual from another source (so not from the individual direct) the Association will provide the required privacy information in accordance with the requirements of Data Protection Law.

4.2.2 The Fair Processing Notice sets out the Personal Data processed by the Association and the basis for that Processing. This document is provided to all of the Association’s customers at the outset of processing their data

4.3 Employees

4.3.1 Employee Personal Data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by the Association. Details of the data held and processing of that data is contained within the

Employee Fair Processing Notice which is provided to Employees at the same time as their Contract of Employment.

- 4.3.2 A copy of any employee's Personal Data held by the Association is available upon written request by that employee from the Association's Data Protection Officer subject to certain exceptions.

4.4 Consent

- 4.4.1 Consent as a ground for processing will require to be used from time to time by the Association when processing Personal Data. It should be used by the Association where no other alternative ground for processing is available. In the event that the Association requires to obtain consent to process a Data Subject's Personal Data, it shall obtain that consent in writing (unless extenuating circumstances apply). The consent provided by the Data Subject must be freely given and the Data Subject will be required to sign a relevant consent form if willing to consent (again, subject to extenuating circumstances such as the Data Subject being unable to write). Any consent to be obtained by the Association must be for a specific and defined purpose (i.e. general consent cannot be sought). Where consent is being relied on, Data Subjects are free to withhold their consent or withdraw it at any future time.

4.5 Processing of Special Category Personal Data or Sensitive Personal Data

- 4.5.1 In the event that the Association processes Special Category Personal Data or Criminal Offence Data, the Association must rely on an additional ground for processing in accordance with one of the special category grounds. These include, but are not restricted to, the following:

- The data subject has given explicit consent to the processing of this data for a specified purpose;
- Processing is necessary for carrying out obligations or exercising rights related to employment, social security, or social protection law;
- Processing is necessary for health or social care
- Processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity; and
- Processing is necessary for reasons of substantial public interest under law.

- 4.5.2 All the grounds for processing sensitive personal data are set out in the GDPR and expanded on in the Data Protection Act 2018.

5. Data Sharing

- 5.1 The Association shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with the Association's relevant policies and procedures. In order that the Association can monitor compliance by these third parties with Data Protection laws, the Association will require the third party organisations to enter into an Agreement with the Association governing the processing of data, security measures to be implemented and responsibility for breaches. There is a Model Data Sharing Agreement which the

association may use in such scenarios. However the Association will determine on a case-by-case basis what the most appropriate contract terms (if required) shall be.

5.2 Data Processors

- 5.2.1 A Processor is a third party entity that processes Personal Data on behalf of the Association, and are frequently engaged if certain of the Association's work is outsourced (e.g. payroll, maintenance and repair works).
- 5.2.2 A Data Processor must comply with Data Protection laws. The Association's Processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify the Association if a data breach is suffered.
- 5.2.3 If a Processor wishes to sub-contact their processing, prior written consent of the Association must be obtained. Upon a sub-contracting of processing, the Processor will be liable in full for the data protection breaches of their sub-contractors.
- 5.2.4 Where the Association contracts with a third party to process Personal Data held by the Association, it shall require the third party to enter into a written contract with the Association with such contract outlining, amongst other things, how personal data will be kept safe and secure. The Association has a Model Data Protection Addendum which can be used in these scenarios. But the Association may, on a case-by-cases basis, determine the other contract wording is appropriate.

6. Data Storage and Security

- 6.1 All Personal Data held by the Association must be stored securely, whether electronically or in paper format.

6.2 Paper Storage

- 6.2.1 If Personal Data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. Employees should make sure that no Personal Data is left where unauthorised personnel can access it. When the Personal Data is no longer required (and the Association has a Retention Policy which sets out the expected timescales for holding various personal categories of personal data) it must be disposed of by the employee to ensure its destruction. If the Personal Data requires to be retained on a physical file then the employee should ensure that it is affixed to the file which is then stored in accordance with the Association's storage provisions.

6.3 Electronic Storage

- 6.3.1 Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should be password protected when being sent internally or externally to the Association's Processors or those with whom the Association has entered in to a Data Sharing Agreement. If Personal Data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be encrypted and stored securely at all times when not being used. Personal Data should not be saved directly to mobile devices and should be stored on designated drives and servers.

7. Breaches

7.1 A data breach can occur at any point when handling Personal Data and the Association has reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the Data Subjects who are the subject of the breach require to be reported externally in accordance with Clause 7.3 of this policy.

7.2 Internal Reporting

7.2.1 The Association takes the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as the breach or potential breach has occurred, the Association's Data Protection Officer must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any Data Subject(s);
- The Association must seek to contain the breach by whatever means available;
- The Data Protection Officer must consider whether the breach is one which requires to be reported to the Information Commission and to the Data Subjects affected and do so in accordance with this clause 7;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements, Data Processing Agreements or equivalent contract terms.

7.3 Reporting to the Information Commission and to Data Subjects

7.3.1 The Data Protection Officer will require to report any breaches which pose a risk to the rights and freedoms of the Data Subjects who are subject of the breach to the Information Commission within 72 hours of the breach occurring or the Association becoming aware of the breach. The Data Protection Officer must also consider whether it is appropriate to notify those Data Subjects affected by the breach.

7.3.2 Where a breach poses a high risk to the rights and freedoms of the Data Subjects impacted by the breach, the Association must, in addition to notifying the Information Commission, promptly notify the Data Subjects in question.

8. Data Protection Officer ("DPO")

8.1 The Association's Corporate Services Officer is our DPO. The DPO is an individual who has an over-arching responsibility and oversight over compliance by the Association with Data Protection laws. The Association has elected to appoint a Data Protection Officer whose details are noted on the Association's website and contained within the Fair Processing Notice.

8.2 The DPO will be responsible for:

- monitoring the Association's compliance with Data Protection laws and this Policy and advising on compliance as needed;
- co-operating with and serving as the Association's contact for discussions with the Information Commission;

- reporting breaches or suspected breaches to the Information Commission and Data Subjects in accordance with Part 7 of this policy.

9. Data Subject Rights

9.1 Certain rights are provided to Data Subjects under Data Protection Law:

- 9.1.1 a right to be informed about the collection and use of their personal data, (typically fulfilled by providing individuals with a Fair Processing Notice).
- 9.1.2 a right to access and receive a copy of their personal data, plus other supplementary information (the “right of access”);
- 9.1.3 a right to have inaccurate personal data rectified and incomplete personal data completed (the “right to rectification”);
- 9.1.4 a right to have personal data erased (the “right to erasure”);
- 9.1.5 the right to request the restriction or suppression of personal data (the “right to restrict”);
- 9.1.6 the right to obtain and reuse certain personal data across different providers (the “right to data portability”);
- 9.1.7 the right, in certain circumstances, to object to the processing of their personal data (the “right to object”);
- 9.1.8 the right to make a complaint about how their personal data has been processed (the “right to complain”); and
- 9.1.9 rights to protect individuals against automated decision making or profiling (“rights related to automated decision making”).

9.2 These rights are notified to the Association’s tenants and other customers in the Association’s Fair Processing Notice. Such rights are subject to qualification and are not absolute.

9.3 The Right of Access: Subject Access Requests

9.3.1 Data Subjects are permitted to view their data held by the Association through making a request to do so (a Subject Access Request – subject to certain exemptions). Upon receipt of a request by a Data Subject, the Association must respond to the Subject Access Request within one month from the date of receipt of the request (unless the Association is entitled under the relevant legislation to increase this timescale). The Association:

- must provide the Data Subject with an electronic or hard copy of the Personal Data requested, unless any exemption to the provision of that data applies in law.
- where the Personal Data comprises data relating to other Data Subjects, the Association shall only release that data where: the Association has obtained consent from those Data Subjects OR the Association determines it is reasonable to disclose said data without consent, or
- where the Association does not hold the Personal Data sought by the Data Subject, must confirm that to the Data Subject as soon as practicably

possible, and in any event, not later than one month from the date on which the request was made.

9.4 The Right to be Erasure

- 9.4.1 A Data Subject can exercise their right to erasure (otherwise known as the right to be forgotten) by submitting a request to the Association seeking that the Association erase their Personal Data in its entirety.
- 9.4.2 Each request received by the Association will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the Data Subject's request in accordance with clause 9.4 and will respond in writing to the request.
- 9.4.3 Requests for Erasure will be considered and responded to by the Association by one month from the day after the date we receive the request, unless the Association is entitled to increase the timescales under relevant legislation.

9.5 The Right to Restrict or Object to Processing

- 9.5.1 A Data Subject may request that the Association restrict its processing of the Data Subject's Personal Data, or object to the processing of that data.
- 9.5.2 In the event that any direct marketing is undertaken from time to time by the Association, a Data Subject has an absolute right to object to processing of this nature by the Association, and if the Association receives a written request to cease processing for this purpose, then it must do so immediately.
- 9.5.3 Each request received by the Association will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the Data Subject's request in accordance with clause 9.5 and will respond in writing to the request.

9.6 The Right to Rectification

- 9.6.1 A Data Subject may request the Association to have inaccurate Personal Data rectified. If appropriate, a Data Subject may also request the Association to have incomplete Personal Data completed.
- 9.6.2 Each request received by the Association will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the Data Subject's request in accordance with clause 9.6 and will respond in writing to the request.

9.7 The Right to Data Portability

- 9.7.1 A Data Subject may ask for their personal data which they have provided to the Association to be provided in a structured, commonly used, machine readable format or the Data Subject may ask for this data to be transmitted directly to another organisation. This is subject to certain exemptions.
- 9.7.2 Each request received by the Association will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or

refusing the Data Subject's request in accordance with clause 9.7 and will respond in writing to the request.

9.8 The Right to Complain

9.8.1 A Data Subject may complain to the Association if they consider their personal data has been processed by the Association in contravention of Data Protection Law.

9.8.2 Any such complaint shall be handled in accordance with the Association's Complaints Policy.

9.9 Rights Related to Automated Decision Making

9.9.1 Should the Association utilise any automated decision making it shall follow the requirements set down in Data Protection Law to protect the Data Subjects in question

10. Privacy Impact Assessments ("PIAs")

10.1 These are a means of assisting the Association in identifying and reducing the risks that our operations have on personal privacy of Data Subjects. Whilst this policy uses the term PIAs, it is also recognised that these assessments are also commonly referred to as "Data Protection Impact Assessments" or similar.

10.2 The Association shall:

10.2.1 Carry out a PIA before undertaking a project or processing activity which poses a "high risk" to an individual. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing Personal Data; and

10.2.2 In carrying out a PIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the Personal Data.

10.3 The Association will require to consult the Information Commission in the event that a PIA identifies a high level of risk which cannot be reduced. The DPO will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the DPO within five (5) working days.

11. Archiving, Retention and Destruction of Data

11.1 The Association cannot store and retain Personal Data indefinitely. It must ensure that Personal Data is only retained for the period necessary. The Association shall ensure that all Personal Data is archived and destroyed in accordance with the periods specified within the table shown in Appendix 2.

Approved by the Committee of Management on:	
Signed:	Signed:
Secretary/Chairperson	Chief Executive/Senior Staff Member

Appendix 1: List of Related Policies

Policy Name	Policy Category
Age Retirement	Human Resources
Alcohol, Drugs and Substance Misuse	Human Resources
Allocations	Housing Management
Annual Leave	Human Resources
Anti-Social Behaviour	Housing Management
Asbestos Management	Technical Services
Attendance Management	Human Resources
Bad Debts	Finance
Committee Appraisal	Governance
Committee Members Expenses	Governance
Committee Recruitment	Governance
Complaints	Governance
Conflicts of Interest	Governance
Entitlements, Payments and Benefits	Governance
Equal Opportunities	Governance
Estate Management	Housing Management
Factoring Services	Technical Services
Flexible Working	Human Resources
Induction	Human Resources
Learning and Development	Human Resources
Leasing	Housing Management
Membership	Governance
Mental Wellbeing and Resilience	Human Resources
Personal Relationships at Work	Governance
Pets	Housing Management
Rechargeable Repairs	Technical Services
Recruitment and Selection	Human Resources
Rent Arrears	Housing Management
Repairs and Maintenance	Technical Services
Shared Ownership	Housing Management
Shared Parental Leave	Human Resources
Staff Appraisal	Human Resources
Stage 3 Adaptations	Technical Services
Tenancy Sustainment	Housing Management
Unacceptable Behaviour	Governance
Void Management	Housing Management
Whistleblowing	Governance

Appendix 2: Table of Duration of Retention of certain Data

The table below sets out retention periods for Personal Data held and processed by the Association. It is intended to be used as a guide only. The Association recognises that not all Personal Data can be processed and retained for the same duration, and retention will depend on the individual circumstances relative to the Data Subject whose Personal Data is stored.

Topic	Type of record	Suggested retention time
Human Resources	Personal files including training records and notes of disciplinary and grievance hearings	5 years to cover the time limit for bringing any civil legal action, including national minimum wage claims and contractual claims
	Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of the redundancy
	Job Application forms, interview notes	Minimum 6 months to a year from date of interviews. Successful applicants' documents should be transferred to personal file.
	Documents proving the right to work in the UK	2 years after employment ceases.
	Facts relating to redundancies	6 years if less than 20 redundancies. 12 years if 20 or more redundancies.
	Payroll	Current financial year plus previous 6 years
	Income tax, NI returns, correspondence with tax office	Current financial year plus previous 6 years
	Retirement benefits schemes – notifiable events, e.g. relating to incapacity	6 years from end of the scheme year in which the event took place
	Pensioners records	12 years after the benefit ceases
	Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence	Current financial year plus previous 6 years

Topic	Type of record	Suggested retention time
Human Resources (continued)	Parental Leave	18 years
	Statutory Sick Pay records, calculations, certificates, self-certificates	Current financial year plus previous 6 years
	Wages/salary records, expenses, bonuses	Current financial year plus previous 6 years
	Records relating to working time	2 years from the date they were made
	Accident books and records and reports of accidents	3 years after the date of the last entry
	Health and Safety assessments and records of consultations with safety representatives and committee	Permanently
	Health records	During employment and 3 years thereafter if reason for termination of employment is connected to health
Governance	Membership records	5 years after last contact
	Committee Members' Documents	5 years after cessation of membership
	Committee meetings/residents' meetings	Permanently
Technical Services	Documents relation to successful tenders	5 years after end of contract
	Documents relating to unsuccessful form of tender	5 years after notification
	Minute of factoring meetings	Duration of appointment as factor
	Property Repairs Records	Duration of property ownership and 5 years after ownership termination
Housing Management	Applicants for accommodation	5 years
	Benefits Notifications	Duration of Tenancy
	Tenancy files	Duration of Tenancy
	Former tenants' files (key information)	5 years
	Third Party documents, e.g. regarding care plans	Duration of Tenancy
	Records regarding offenders. Ex-offenders (sex offender register)	Duration of Tenancy
	Lease documents	5 years after lease termination
	Anti-Social Behaviour case files	5 years/end of legal action
	Office CCTV recordings	6 months