Clydesdale Housing Association	
Policy name & number	**Privacy Policy**
Date approved	**25 April 2018**
Date for review	**April 2021**
Policy by	**Joe Gorman - Chief Executive**
Responsible Officer	**Depute Chief Executive**

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

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.

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).

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.

Appendix 1, which is attached, details the Association's related policies.

2. Legislation

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.

The relevant legislation in relation to the processing of data is:

(a) the General Data Protection Regulation (EU) 2016/679 ("the GDPR");

(b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and

(c) any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications 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 individuals, including customers and employees (referred to as Data Subjects in the rest of this policy) which 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.

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".

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; or
- Processing is necessary for the purposes of legitimate interests.

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.

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 Depute Chief Executive.

4.4 Consent

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. 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. Any consent to be obtained by the Association must be for a specific and defined purpose (i.e. general consent cannot be sought).

4.5 Processing of Special Category Personal Data or Sensitive Personal Data

In the event that the Association processes Special Category Personal Data or Sensitive Personal Data, the Association must do so in accordance with one of the following grounds of processing:

- 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 or social security;

- 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.

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 in to an Agreement with the Association governing the processing of data, security measures to be implemented and responsibility for breaches.

5.2 Data Sharing

5.2.1 Personal Data is from time to time shared amongst the Association and third parties who require to process Personal Data that the Association process as well. Both the Association and the third party will be processing that data in their individual capacities as Data Controllers.

5.2.2 Where the Association shares in the processing of Personal Data with a third party organisation (e.g. for processing of the employees' pension), it shall require the third party organisation to enter in to a Data Sharing Agreement with the Association in accordance with the terms of the Model Data Sharing Agreement set out in the Scottish Federation of Housing Associations' (SFHA) GDPR Model Documentation & Guidance Notes (the SFHA Guidance).

5.3 Data Processors

A Data 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).

5.3.1 A Data Processor must comply with Data Protection laws. The Association's Data 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.

5.3.2 If a Data Processor wishes to sub-contact their processing, prior written consent of the Association must be obtained. Upon a sub-contracting of processing, the Data Processor will be liable in full for the data protection breaches of their sub-contractors.

5.3.3 Where the Association contracts with a third party to process Personal Data held by the Association, it shall require the third party to enter in to a Data Protection Addendum with the Association in accordance with the terms of the Model Data Protection Addendum set out in the SFHA Guidance.

6. Data Storage and Security

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

6.1 Paper Storage

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 it must be disposed of by the employee so as 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.

6.2 Electronic Storage

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 Data 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 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 drivers 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 subject of the breach require to be reported externally in accordance with Clause 7.3 of this policy.

7.2 Internal Reporting

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, and in any event no later than six (6) hours after it has occurred, the 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 Commissioner's Office and 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

7.3 Reporting to the Information Commissioner's Office (ICO)

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 ICO within 72 hours of the breach occurring. The Data Protection Officer must also consider whether it is appropriate to notify those Data Subjects affected by the breach.

8. Data Protection Officer ("DPO")

8.1. A 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:

8.2.1 monitoring the Association's compliance with Data Protection laws and this Policy;

8.2.2 co-operating with and serving as the Association's contact for discussions with the ICO;

8.2.3 reporting breaches or suspected breaches to the ICO 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 the GDPR. Data Subjects are entitled to view the Personal Data held about them by the Association, whether in written or electronic form.

9.2 Data Subjects have a right to request a restriction of processing their data, a right to be forgotten, and a right to object to the Association's processing of their data. These rights are notified to the Association's tenants and other customers in the Association's Fair Processing Notice.

9.3 **Subject Access Requests**

Data Subjects are permitted to view their data held by the Association through making a request to do so (a Subject Access Request). Upon receipt of a request by a Data Subject, the Association must respond to the Subject Access Request within one month of the date of receipt of the request. The Association:

9.3.1 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.

9.3.2 where the Personal Data comprises data relating to other Data Subjects, must take reasonable steps to obtain consent from those Data Subjects to the disclosure of that Personal Data to the Data Subject who has made the Subject Access Request, or

9.3.3 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 Forgotten**

9.4.1 A Data Subject can exercise their right to be forgotten by submitting a request in writing 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.

9.5 **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.

9.5.1.1 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.

9.5.2 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 9.5 and will respond in writing to the request.

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.

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’s privacy. 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 ICO 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

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.

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
Conflics 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
Whisleblowing	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
	Housing 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