

## **CLYDE VALLEY HOUSING ASSOCIATION PRIVACY POLICY**

## Contents

1. Introduction	p1
2. Legislation	p1
3. Data	p1
4. Data Protection Principles	p2
5. Processing of Personal Data	p2
6. Data Sharing	p4
7. Data Storage and Security	p5
8. Breaches	p5
9. Data Protection Officer	p6
10. Data Subject Rights	p7
11. Privacy Impact Assessments	p8
12. Archiving, Retention and Destruction of Data	p8
Appendix 1 – Related Policies	p10
Appendix 2 – Data Retention Schedule	p15
Appendix 3a – Fair Processing Notice Tenants	p17
Appendix 3b – Fair Processing Notice Owner	p24
Appendix 3c - Fair Processing Summary document	p27
Appendix 3d - Privacy Notice (Employees)	p30
Appendix 3e - Privacy Notice (Board Members)	p35
Appendix 4 – Model Data Sharing Agreement	p38
Appendix 5 – Model Data Protection Addendum	p49

## 1. Introduction

Clyde Valley Housing Association (the “**Association**”) is a social housing provider engaged in the provisions of social housing in Lanarkshire.

The Association manages a significant amount of data, from a variety of sources. The Association needs to gather and use certain information about individuals in order to perform its functions. These can include customers (tenants, factored owners etc.), employees and other individuals that the Association has a relationship with.

The personal information that the Association has about individuals is held and processed by different companies in the Association’s group of companies. Which company processes the information depends on the relationship that an individual has with the Association. The personal data that CVHA holds about individuals is processed by different companies within its group. The company that processes the data of an individual depends on the relationship that individual has with CVHA. The personal data of CVHA’s tenants and employees is processed by Clyde Valley Housing Association Limited. The personal data of factored owners, mid-market property owners, and mid-market property tenants is processed by Clyde Valley Property Services Limited through its three subsidiaries:

1. Avant Letting Services Limited (for mid-market property tenants);
2. Nova Property Management Services Limited (for factored owners); and
3. Innov8 Housing Solutions Limited (for mid-market property owners).

Clyde Valley Property Services Limited is a wholly owned subsidiary of Clyde Valley Housing Association Limited.

The Association is committed to ensuring that the data it has is managed securely and in accordance with the law. This Privacy Policy sets out the Association’s duties in processing that data, and the procedures for managing that data.

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.

Appendix 1 provides details of the Association’s related policies.

## 2. Legislation

It is a legal requirement that the Association process data in compliance with the “**Data Protection Law**” which includes:

- the General Data Protection Regulation (EU) 2016/679 (the “**GDPR**”);
- the Data Protection Act 2018;
- the Privacy and Electronic Communications (EC Directive) Regulations 2003;
- all other applicable EU and UK data protection laws, including those that are made as a consequence of the UK leaving the EU; and
- any legislation or laws that amend the above.
-

### 3. Data

3.1 The Association holds a variety of data relating to individuals, including customers, employees and other individuals that the Association has a relationship with (also referred to as “**data subjects**”). The specific data that the Association processes is detailed within the Fair Processing Notice at Appendix 3, as well as in the Data Protection Addendum to the Terms of and Conditions of Employment which has been provided to all employees.

3.2 The data held by the Association about data subjects includes both Personal Data and Special Category Personal Data. The difference between these types of data is explained below:

3.1.1 “**Personal Data**” is any data held by the Association from which a living individual can be identified (either by that data alone, or in conjunction with other data held by the Association). This can include, for example, an individual’s name, address or telephone number.

3.1.2 The Association also holds Personal Data that is sensitive in nature, known as “**Special Category Personal Data**”. This includes Personal Data that reveals:

- racial or ethnic origin;
- religious and philosophical beliefs;
- political opinions;
- trade union membership;
- genetic or biometric data;
- data concerning health;
- data concerning sex life or sexual orientation; or
- data concerning criminal convictions or offences.

### 4. Data Protection Principles

The Association complies with the Data Protection Principles set out below. When processing Personal Data (including Special Category Personal Data) it ensures that:

- it is processed lawfully, fairly and in a transparent manner in relation to the data subject (“**lawfulness, fairness and transparency**”);
- it is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (“**purpose limitation**”);
- it is all adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“**data minimisation**”);
- it is all accurate and, where necessary, kept up to date and that reasonable steps will be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“**accuracy**”);
- it is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data are processed (“**storage limitation**”);
- it is processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“**integrity and confidentiality**”).

The Association will facilitate any request from a data subject who wishes to exercise their rights under Data Protection Law as appropriate, always communicating in a concise, transparent, intelligible and easily accessible form and without undue delay. Further information on data subject rights is provided in clause 10.

## **5. Processing of Personal Data**

### **Legal Basis for Processing**

5.1 The Association is permitted to process Personal Data on behalf of data subjects provided it has a legal basis for doing so. The Association would have a legal basis where:

- processing is carried on with the consent of the data subject (see clause 5.4 below);
- 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
- The Association has a legitimate interest to process the Personal Data.

### **Fair Processing Notice**

5.2 The Association has produced a Fair Processing Notice which it is required to provide to all data subjects whose Personal Data (including Special Category Personal Data) it processes. That Fair Processing Notice must be provided to the data subject from the outset of processing their Personal Data and they should be advised of the terms of the Fair Processing Notice when it is provided to them.

5.3 The Fair Processing Notice is provided at Appendix 3. It sets out the Personal Data processed by the Association and the legal basis for that Processing.

### **Association Employees**

5.4 Employee Personal data and, where applicable, Special Category Personal Data, is held and processed by the Association. Details of the data held, and processing of that data, are contained within the Employee Privacy Notice which is provided to employees at the same time as their contract of employment.

5.5 An employee may obtain a copy of their Personal Data held by the Association by submitting a request to the Customer Services Director/Chief Executive.

### **Processing Based on Consent**

5.6 In certain circumstances the Association will be required to obtain the consent of the data subject when processing their Personal Data. Consent should only be used by the Association where no other alternative legal basis for processing is available. The legal bases for processing are set out in clause 5.1 above. 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). If the consent will be relied on by any third parties then the data subject should be made aware of who those third parties are. The data subject must also be informed that they can withdraw their consent at any time, and who they should contact to withdraw their consent. The Association will ensure that it does not use consent as its legal basis for processing when processing employee Personal Data.

### **Processing of Special Category Personal Data**

5.7 In the event that the Association processes Special Category Personal Data, the Association must identify one of the following grounds in addition to a legal basis as set out in clause 5.1 above:

- the data subject has given explicit consent to the processing of this data for a specified purpose;
- processing is necessary under employment, social security or social protection law, so long as the processing is necessary to comply with a legal obligation;
- 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;
- the processing relates to Personal Data which have already manifestly been made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest; or
- Processing is necessary for the purposes of medical treatment or diagnosis or assessing working capacity of an employee.

## **6. Data Sharing**

### **Sharing Data with Third Parties**

6.1 The Association shares its data with third parties for a variety of reasons in order that its day to day activities are carried out in accordance with the Association's 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.

### **Sharing Data with Other Controllers**

6.2 A data "**controller**" is an organisation that decides why data is being processed, how it is being processed and what is happening to personal data. The Association is a data controller in relation to all Personal Data that it decides to collect and process.

- 6.3 From time to time, the Association will require to share Personal Data with third parties who require to process the same Personal Data that the Association processes. These third parties will decide what data they require, and how they will process it. Both the Association and the third party will therefore be processing that data in their individual capacities as data controllers.
- 6.4 Where the Association participates in the processing of personal data with a third party controller (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 Appendix 4 to this Policy.

### **Data Processing**

- 6.5 A data “**processor**” is a third party entity that processes personal data on behalf of, and on the instructions of, the Association. Some of the Association's work is outsourced to data processors (e.g. payroll providers, maintenance and repair contractors).
- 6.6 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 their processing activities and notify the Association if a data breach has occurred.
- 6.7 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.
- 6.8 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 Appendix 5 to this Policy.
- 6.9 There will be instances where Clyde Valley Housing Association Limited will process Personal Data for and on behalf of its subsidiary, Clyde Valley Property Services Limited. This is necessary to allow Clyde Valley Property Services Limited to fulfil its obligations to those individuals that it deals with (e.g. factored owners and mid-market property owners).

## **7. Data Storage and Security**

- 7.1 The Personal Data held in electronic form by the Association is held on its central IT system. This system can be accessed by all of the companies in the Associations' group of companies. However, a particular company within the Association's group can only access the Personal Data relevant to its operations. All Personal Data held by the Association must be stored securely, whether held electronically or in paper format.

### **Paper Storage**

- 7.2 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 procedures.

### **Electronic Storage**

- 7.3 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 drives and servers.

## **8. Breaches**

- 8.1 A “**personal data breach**” is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data (that has been transmitted, stored or processed).
- 8.2 A personal data breach can occur at any point when handling Personal Data and the Association has reporting duties in the event of a personal data breach or potential breach. Breaches which pose a risk to the rights and freedoms of data subjects (who are affected by the breach) must be reported to the ICO, and potentially to data subjects in accordance with clauses 8.3-8.4.

### **Internal Reporting**

- 8.3 The Association takes the security of data very seriously and in the unlikely event of a personal data breach, it 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 DPO 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 DPO must consider whether the breach is one which requires to be reported to the ICO and affected data subjects in accordance with this clause 8.4; and
  - notify third parties in accordance with the terms of any applicable Data Sharing Agreements.

### **Reporting to the ICO and Data Subjects**

- 8.4 The DPO will require to report any personal data breaches which pose a risk to the rights and freedoms of the data subjects who are affected by the breach to the Information Commissioner's Office (“**ICO**”) within 72 hours of the breach occurring. The notification to the ICO should include:



- a description of the personal data breach, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned;
  - the name and contact details of the DPO or other contact point where more information can be obtained; and
  - the measures taken or proposed to be taken by the Association to address the personal data breach.
- 8.5 If the personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the DPO must inform the data subject without undue delay (in addition to informing the ICO as set out above). The data subject should be advised (in plain language) of the personal data breach, its likely consequences for the data subject, steps taken to remedy the breach, and any steps that the data subject can take to mitigate potential adverse effects.
- 8.6 The Association will document all personal data breaches whether they have been reported or not. The record will detail the facts surrounding the breach, its effects, and remedial action taken.

## 9. Data Protection Officer (“DPO”)

- 9.1 A Data Protection Officer (“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 at Appendix 3.
- 9.2 The DPO will be responsible for:
- monitoring the Association’s compliance with Data Protection Laws and this Privacy Policy;
  - co-operating with and serving as the Association’s contact point for communication with the ICO;
  - reporting breaches or suspected breaches to the ICO and data subjects in accordance with clause 8 of this Privacy Policy.

## 10. Data Subject Rights

- 10.1 Under Data Protection Laws, data subjects have certain rights in relation to their Personal Data held by the Association. These rights include:
- **Access:** a right to be told what Personal Data is being processed and to be provided with a copy of that data;
  - **Rectification:** a right to have inaccurate Personal Data rectified;
  - **Erasure:** a right to have Personal Data erased under certain circumstances;
  - **Restriction of processing:** a right to ask for processing of Personal Data to be restricted in certain circumstances; and
  - **Data portability:** a right to receive a copy of Personal Data processed by automated means in a format that can be transferred from one data controller to another.
- 10.2 These rights are notified to the Association’s tenants and other customers in more detail in the Association’s Fair Processing Notice at Appendix 3.

## **Subject Access Requests**

10.3 Data subjects are permitted to view their data held by the Association upon 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. A request by a data subject may be made in writing or orally. The Association:

- must provide the data subject with an electronic or hard copy of the Personal Data requested, unless any exemptions to the provision of that information apply under Data Protection Law.
- 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, and even without consent consider whether it is reasonable to disclose the personal data of another data subject or
- where the Association does not hold the Personal Data sought by the data subject, must confirm that it does not hold any Personal Data sought 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.

## **The Right to be Forgotten**

10.4 A data subject can exercise their right to be forgotten by submitting a request in writing to the Association seeking that the Association erase the data subject's Personal Data in its entirety. This is only required in certain circumstances where the Association no longer has a legal basis to hold onto the Personal Data and even if this is not the case, the Association may require to hold onto the data for other reasons.

10.5 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, and will respond in writing to the request.

## **The Right to Restrict or Object to Processing**

10.6 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.

10.7 In the event that any direct marketing is undertaken 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.

10.8 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, and will respond in writing to the request.

## **11. Data Protection Impact Assessments (“DPIAs”)**

11.1 These are a means of assisting the Association in identifying and reducing the risks that our operations have on personal privacy of data subjects.

11.2 The Association shall:

- carry out a DPIA 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
- in carrying out a DPIA, 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.

11.3 The Association will require to consult the ICO in the event that a DPIA 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.

## **12. 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 length of time that the Association needs to process it for its identified purpose or purposes. The Association shall ensure that all Personal Data is archived and destroyed in accordance with the periods specified within the table at Appendix

### List of Appendices

Appendix 1 – Related Policies	p10
Appendix 2 – Data Retention Schedule	p15
Appendix 3a – Fair Processing Notice Tenants	p17
Appendix 3b – Fair Processing Notice Owner	p24
Appendix 3c - Fair Processing Summary document	p27
Appendix 3d - Privacy Notice (Employees)	p30
Appendix 3e - Privacy Notice (Board Members)	p35
Appendix 4 – Model Data Sharing Agreement	p38
Appendix 5 – Model Data Protection Addendum	p49

## Related Policies

## Appendix 1

### CVG Policies with GDPR Implication

Title	Policy Number	Review Date
Payments and Benefits Policy	G01	September 2019
Board Expenses Policy	G02	September 2019
Board Code of Conduct	G03	September 2019
Complaints Policy	G04	September 2019
Access to Information Policy	G05	September 2019
Equality and Diversity Policy	G06	September 2019
<a href="#">Customer Care and Service Standards Policy</a>	G07	March 2017
Policy Development Framework	G08	September 2019
Board Training and Performance Development Policy	G09	September 2019
<a href="#">Membership Policy</a>	G10	September 2019
Board <a href="#">Composition, Skills and Recruitment</a> Policy	G11	September 2019
Board Succession Plan	G12	September 2019
<a href="#">Standing Orders</a> and Delegated Authority Policy	G13	September 2019
<a href="#">Performance Management Framework</a>	G14	September 2019
Retention Policy	G15	September 2019
Risk Strategy	G16	September 2019
Fraud, Bribery and Money Laundering Policy	G17	September 2019
Insurance Policy	G18	September 2019
Data Protection Policy	G19	September 2019
Crisis Response and Management Plan*	-	December 2016
Procurement Strategy*	-	March 2018
Customer Engagement Strategy*	-	November 2018
Value for Money Strategy*	-	November 2020

### IT Policy Register

All documents detailed below can be located in the IT Policy Manual, unless otherwise specified.

Title	Policy Number	Review Date
<a href="#">ICT Security Policy</a>	IT1	September 2019
<a href="#">ICT Acceptable Usage Policy</a>	IT2	September 2019
IT Strategy*	-	August 2017

## HR Policy Register

All documents detailed below can be located in the HR Policy Manual, unless otherwise specified.

<b>Title</b>	<b>Policy Number</b>	<b>Review Date</b>
Code of Conduct - Staff	HR01	February 2019
Health and Safety Policy	HR02	February 2019
Corporate Clothing and Equipment Policy	HR03	February 2019
Staff Training Policy	HR04	February 2019
Stress Policy	HR05	February 2019
Transport Policy	HR06	February 2019
Whistleblowing Policy	HR07	February 2019
Dignity at Work Policy	HR08	February 2019
Recruitment Policy	HR09	February 2019
Working from Home Policy	HR10	February 2019
Alcohol and Drug Policy	HR11	February 2019
Smoking Policy	HR12	February 2019
Personal Relationships at Work Policy	HR13	February 2019
Childcare Voucher Policy	HR14	February 2019
Absence Management Procedures	HR15	February 2019
Flexible Working Policy	HR16	February 2019
Shared Parental Leave Policy	HR17	February 2019
HR Strategy*	-	February 2019

## Housing Policy Register

<b>Title</b>	<b>Policy Number</b>	<b>Review Date</b>
Housing Allocation Policy (North Lanarkshire)	HM01NL	August 2019
Housing Allocation Policy (South Lanarkshire)	HM01SL	August 2019
Arrears Policy	HM02	August 2019
Void Management Policy	HM03	August 2019
Anti-Social Behaviour Policy	HM04	August 2019
Customer Allowances Policy	HM05	August 2019
Policy on Leases, Management Agreements and SSSTs	HM06	August 2019
Rent Setting and Service Charges Policy	HM07	August 2019
Shared Ownership Arrears	HM08	August 2019
Tenancy Sustainment Policy	HM09	August 2019
Income Maximisation Policy	HM10	August 2019
Decant Policy	HM11	August 2019
Scottish Secure Tenancy Agreement	-	-
Short Scottish Secure Tenancy Agreement	-	-
Short Assured Tenancy Agreement	-	-
Occupancy Agreement (Shared Housing)	-	-

## CVPS Policy Register

All documents detailed below can be located in the CVPS Policy Manual, unless otherwise specified.

<b>Title</b>	<b>Policy Number</b>	<b>Review Date</b>
Property Factoring Policy	CVPS1	September 2019
Factoring Arrears Policy	CVPS2	September 2019
Complaints Policy	CVPS3	September 2019
Mid-Market and Market Rent Letting Policy	CVPS4	September 2019
Rent Setting Policy	CVPS5	September 2019
Mid-Market and Market Rent Arrears Policy	CVPS6	September 2019
Maintenance Policy	CVPS7	September 2019
Anti-Social Behaviour Policy	CVPS8	September 2019
Bad Debts Policy	CVPS9	September 2019
Written Statement of Services*	-	September 2019
Factoring Agreement – Flat*	-	September 2019
Factoring Agreement – House*	-	September 2019

## Finance Policy Register

<b>Title</b>	<b>Policy Number</b>	<b>Review Date</b>
Depreciation Policy	F03	May 2019
Financial Regulations	F06	November 2019
Treasury Management Policy	F08	November 2017
Bad Debts Policy	G33	May 2019

## Investment Policy Register

All documents detailed below can be located in the Investment Manual.

<b>Title</b>	<b>Review Date</b>
Joint New Supply and Asset Management Procedures	November 2019
Consultation	
Design	
Design Brief	
Compliance with CDM Regulations	
Health & Safety Responsibilities on an Acquired New Supply Site	
Financial Procedures	
Post Project Appraisal	
Defects Process and Monitoring	
New Supply	
New Supply Objectives	
Development Planning and Monitoring	
Submission to Scottish Government or Other for Funding and Compliance with Offers of Grant	
Handovers for New Supply Projects	
Asset Management	
Asset Management Plan	
Asset Management Programme Delivery – Planning	
Asset Management Works Programmes/Projects	

<b>Title</b>	<b>Review Date</b>
Asset Management Programme Delivery – Post Project Update	
Defective Property Strategy and Remedial Process	

Repairs Policy Register

<b>Title</b>	<b>Policy Number</b>	<b>Review Date</b>
Housing Maintenance Policy	M01	November 2018
Alterations & Improvements Policy	M02	February 2016
Fire Safety Policy	M03	June 2016
Gas Servicing Policy	M04	June 2016
Electrical Inspections Policy	M05	June 2017
Rechargeable Repairs Policy	M08	June 2016
Energy Performance Certificate Policy	M09	June 2016
Asbestos Management Policy	M10	June 2016
Medical Adaptations Policy	M11	June 2016
Legionella Policy	M12	May 2018

\* *Standalone Strategy/Agreement documents*

## Appendix 2

### Data Retention Schedule

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.

Type of record	Retention time
Membership records.	5 years after last contact.
Personnel 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.
Application forms, interview notes.	Minimum 6 months to a year from date of interviews. Successful applicant 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.	3 years after the end of the tax year they relate to
Income tax, NI returns, correspondence with tax office.	At least 7 years after the end of the tax year they relate to.
Retirement benefits schemes – notifiable events, e.g. relating to incapacity.	6 years from end of the scheme year in which the event took place.
Pension records.	12 years after the benefit ceases.
Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence.	3 years after the end of the tax year to which they relate.
Parental leave.	18 years.
Statutory Sick Pay records, calculations, certificates, self-certificates.	3 years.
Wages/salary records, expenses, bonuses.	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.
Board members documents.	5 years after cessation of membership.



Documents relation to successful tenders.	5 years after end of contract.
Documents relating to unsuccessful form of tender.	5 years after notification.
Applications for accommodation.	For the duration that the applicant is on the housing list. Where the application is unsuccessful, then for 5 years after the date of application.
Housing Benefit notifications.	Duration of tenancy.
Tenancy files.	Duration of tenancy.
Former tenants' files (key information).	5 years after the termination/expiry of the tenancy.
Third party documents relating to care plans.	Duration of tenancy.
Records relating to offenders and ex-offenders (e.g. sex offender register).	Duration of tenancy.
Lease documents.	5 years after lease termination.
ASB case files.	5 years/end of legal action.
Board meetings/residents' meetings.	1 year.
Minutes of factoring meetings.	Duration of appointment.

## Fair Processing Notice

### (How we use your personal information)

This notice explains what information we collect, when we collect it and how we use it. During the course of our activities we will process personal data (which may be held on paper, electronically, or otherwise) about you and we recognise the need to treat it in an appropriate and lawful manner. The purpose of this notice is to make you aware of how we will handle your information.

#### 1. Who are we?

Clyde Valley Housing Association (“**CVHA**”) is a Registered Social Landlord owning, investing in and managing 7000 homes and customers across Lanarkshire and East Dunbartonshire. CVHA operates through a group of companies that provide different services to its customers. CVHA’s head office is located at 50 Scott Street, Motherwell, ML1 1PN.

The personal data that CVHA holds about individuals is processed by different companies within its group. The company that processes the data of an individual depends on the relationship that individual has with CVHA. The personal data of CVHA’s tenants and employees is processed by Clyde Valley Housing Association Limited. The personal data of factored owners, mid-market property owners, and mid-market property tenants is processed by Clyde Valley Property Services Limited through its three subsidiaries:

1. Avant Letting Services Limited (for mid-market property tenants);
2. Nova Property Management Services Limited (for factored owners); and
3. Innov8 Housing Solutions Limited (for mid-market property owners).

The data controller for the purposes of any personal data that you provide to CVHA will be the company that is processing that data, as detailed above. CVHA is registered as data controllers with the Information Commissioner’s Office.

We take the issue of information security and data protection very seriously. We are committed to ensuring that any processing of your personal data by us is in accordance with Data Protection Law. “**Data Protection Law**” includes the Data Protection Act 2018, the General Data Protection Regulation (EU) 2016/679 and all other relevant EU and UK data protections laws.

Our Data Protection Officer is our HR & Corporate Services Manager, Sandra Haig Any questions relating to this notice and our privacy practices should be sent to Sandra Haig [sandra.haig@cvha.org.uk](mailto:sandra.haig@cvha.org.uk).

## **2. How we collect information from you and what information we collect**

We collect information about you:

- when you apply for housing with us, become a tenant, request services/ repairs, enter in to a factoring agreement with us, or where you provide us with your personal details;
- when you provide information to our income maximisation officers to assist with your financial situation;
- when you apply to become a member;
- when you are a member of our customer panel or take part in its activities;
- from your use of our online services, whether to report any tenancy / factor related issues, make a complaint or otherwise; and
- from your arrangements to make payment to us (such as bank details, payment card numbers, employment details, benefit entitlement and any other income and expenditure related information).

We collect the following information about you:

- name;
- address;
- telephone number;
- e-mail address;
- date of birth
- National Insurance Number;
- next of kin;
- care and support needs;
- vulnerabilities;
- ethnic origin;
- race;
- nationality;
- disabilities;
- GP/health records;
- bank details;
- benefit entitlements;
- employment details;
- access to digital services;

In addition to collecting information from you we also receive the following information from third parties:

- benefits information, including awards of Housing Benefit / Universal Credit;
- payments made by you to us;
- complaints or other communications regarding behaviour or other alleged breaches of the terms of your contract with us, including information obtained from Police Scotland;
- reports as to the conduct or condition of your tenancy, including references from previous tenancies, and complaints of anti-social behaviour.

## **3. Why we need this information about you and how it will be used**

We need your information and will use your information:

- to undertake and perform our obligations and duties to you in accordance with the terms of our contract with you;

- to enable us to supply you with the services and information which you have requested;
- to enable us to respond to your repair request, housing application and complaints;
- to provide you with access to advice, information and support to maximise your income, reduce rent arrears and help you to manage and sustain your tenancy;
- to analyse the information we collect so that we can administer, support and improve and develop our business and the services we offer;
- to contact you in order to send you details of any changes to our supplies which may affect you;
- for all other purposes consistent with the proper performance of our operations and business; and
- to contact you for your views on our products and services.

#### **4. Processing your information**

We will:

- ensure that the legal basis for processing your personal data is identified in advance and that all processing complies with the law;
- not do anything with your data that you would not expect given the content of our privacy policy and this fair processing notice;
- ensure that appropriate privacy policies are in place advising staff and others how and why their data is being processed, and in particular advising data subjects of their rights;
- only collect and process the personal data that we need for purposes we have identified above;
- ensure that as far as possible the personal data we hold is accurate, or a system is in place for ensuring that it is kept up to date as far as possible;
- only hold onto your personal data for as long as it is needed after which time we will securely erase or delete the personal data. Our Privacy Policy sets out the period of time for which we will retain your personal data; and
- ensure that appropriate security measures are in place to ensure that personal data can only be accessed by those who need to access it and that it is held and transferred securely.

We will ensure that all staff who handle personal data on our behalf are aware of their responsibilities under our Privacy Policy and other relevant data protection and information security policies. We will also ensure that our staff are adequately trained and supervised in the performance of their responsibilities.

#### **5. Sharing of Your Information**

The information you provide to us will be treated by us as confidential and will be processed only by our employees within the UK. We may disclose your information to other third parties who act for us for the purposes set out in this notice or for purposes approved by you, including the following:

- if we enter into a joint venture with or merged with another business entity, your information may be disclosed to our new business partners or owners;
- if we instruct repair or maintenance works, major works, electrical and/or gas safety testing your information may be disclosed to any contractor involved in such repairs or works;
- if we are investigating a complaint, information may be disclosed to Police Scotland, Local Authority departments, the Scottish Fire & Rescue Service and others involved in a complaint, whether they are investigating the complaint or otherwise;
- if we are updating tenancy details, your information may be disclosed to third parties (such as utility companies and Local Authority);

- if we are investigating payments, your information may be disclosed to payment processors, Local Authority and the Department of Work & Pensions;
- if we are seeking court action against you for rent arrears or anti-social behaviour, we will share your information with our solicitors, and the in-court advice service at the Court;
- if we are conducting a survey of our products and/or services, your information may be disclosed to third parties assisting in the compilation and analysis of the survey results;
- when you make a payment through our third party payment provider (IMPACT), your information will be shared with it;
- if we are providing support with your income and benefit entitlement, we may share you information with the relevant organisations and agencies (such as the Citizens Advice Bureau, Money Matters, and other debt and advice agencies);
- if we are providing support or referring you for support to manage your tenancy, we may share your information with the relevant third parties (such as Local Authority Social Work Departments, alcohol and drug support agencies and your GP);
- the Scottish Ministers (in respect of shared equity properties).

Your information will also be shared with third parties with whom the Association has a contractual arrangement for services provision, such as payment processing or letter distribution. The Association will ensure that there is an agreement in place between the Association and the third party which provides adequate safeguards for your information.

Unless required to do so by law, we will not otherwise share, sell or distribute any of the information you provide to us without your consent.

Your information will only be stored within the UK.

## 6. Security

When you give us information we take steps to make sure that your personal information is kept secure and safe. Our Privacy Policy sets out these measures.

## 7. Your rights

There are a number of rights that you can exercise in relation to your personal data held by us. We have processes in place to ensure that we can facilitate any request made by you to exercise your rights. All staff have received training and are aware of your rights. Staff can identify such a request and know who to send it to. The relevant rights that you may exercise are listed below.

All requests to exercise any of the below rights will be considered without undue delay and within one month of receipt as far as possible.

**Subject access:** the right to request information about how personal data is being processed, including whether personal data is being processed, and the right to be allowed access to that data and to be provided with a copy of that data. This includes the right to obtain the following information:

- the purpose of the processing;
- the categories of personal data;
- the recipients to whom data has been disclosed or which will be disclosed;
- the retention period;
- the right to lodge a complaint with the ICO;
- the source of the information if not collected direct from the subject; and

- the existence of any automated decision making.

**Rectification:** the right to allow a data subject to rectify inaccurate personal data concerning them.

**Erasure:** the right to have data erased and to have confirmation of erasure, but only where:

- the data is no longer necessary in relation to the purpose for which it was collected;
- where consent is withdrawn;
- where there is no legal basis for the processing; or
- there is a legal obligation to delete data.

Even if one of the above conditions applies we can hold onto your data in the following circumstances: where processing is necessary for: exercising the rights of freedom of expression; to comply with a legal obligation in the public interest or in the exercise of an official authority; for public health reasons; for archiving purposes; and for the establishment, exercise or defence of legal claims.

**Restriction of processing:** the right to ask for certain processing to be restricted in the following circumstances:

- if the accuracy of the personal data is being contested; or
- if our processing is unlawful but the data subject does not want it erased; or
- if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims; or
- if the data subject has objected to the processing, pending verification of that objection.

**Data portability:** the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if we were processing the data using your consent or on the basis of a contract.

**Object to processing:** the right to object to the processing of personal data relying on the legitimate interests processing condition unless we can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claims.

If you would like to exercise any of your rights as set out above, please contact us at [cvha@cvha.org.uk](mailto:cvha@cvha.org.uk).

## 8. Special category personal data

We may hold and process special category personal data relating to you where this is necessary. This may be, for example, to allow us to comply with employment and social security law, or where you have consented to the processing of your special category personal data. Special category personal data is data of a sensitive nature which is given stronger protection under Data Protection Law. This includes information that reveals:

- racial or ethnic origin;
- religious or philosophical beliefs;
- political opinions;
- trade union membership;
- processing of genetic or biometric data;

- data concerning health;
- data concerning sex life or sexual orientation; or
- data concerning criminal convictions or offences.

We have appropriate safeguards in place to ensure that any processing of your special category data is carried out in accordance with Data Protection Law.

## **9. How long we will keep your information**

We review our data retention periods regularly and will only hold your personal data for as long as is necessary for the relevant activity, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you.

We will generally keep your information for the duration of your tenancy or factored owner contract with us. However, we may have to retain certain amounts of data for longer than this. The specific retention periods for which your information will be kept by us are set out in our Privacy Policy. Once your personal data is no longer required by us it will be securely destroyed.

## **10. The Information Commissioner's Office**

You also have the right to complain to the Information Commissioner's Office in relation to our use of your information. The Information Commissioner's Office can be contacted at:

The Information Commissioner's Office – Scotland  
45 Melville Street, Edinburgh, EH3 7HL  
Telephone: 0131 244 9001  
Email: [Scotland@ico.org.uk](mailto:Scotland@ico.org.uk)

## **11. Help us keep your information up to date**

The accuracy of your information is important to us. Please help us keep our records updated by informing us of any changes to your email address and other contact details.

## **Fair Processing Notice**

### **(How we use your personal information)**

This notice explains what information we collect, when we collect it and how we use it. During the course of our activities we will process personal data (which may be held on paper, electronically, or otherwise) about you and we recognise the need to treat it in an appropriate and lawful manner. The purpose of this notice is to make you aware of how we will handle your information.

#### **1. Who are we?**

Clyde Valley Housing Association (“**CVHA**”) is a Registered Social Landlord owning, investing in and managing 7000 homes and customers across Lanarkshire and East Dunbartonshire. CVHA operates through a group of companies that provide different services to its customers. CVHA’s head office is located at 50 Scott Street, Motherwell, ML1 1PN.

The personal data that CVHA holds about individuals is processed by different companies within its group. The company that processes the data of an individual depends on the relationship that individual has with CVHA. The personal data of CVHA’s tenants and employees is processed by Clyde Valley Housing Association Limited. The personal data of factored owners, mid-market property owners, and mid-market property tenants is processed by Clyde Valley Property Services Limited through its three subsidiaries:

1. Avant Letting Services Limited (for mid-market property tenants);
2. Nova Property Management Services Limited (for factored owners); and
3. Innov8 Housing Solutions Limited (for mid-market property owners).

The data controller for the purposes of any personal data that you provide to CVHA will be the company that is processing that data, as detailed above. CVHA is registered as data controllers with the Information Commissioner’s Office.

We take the issue of information security and data protection very seriously. We are committed to ensuring that any processing of your personal data by us is in accordance with Data Protection Law. “**Data Protection Law**” includes the Data Protection Act 2018, the General Data Protection Regulation (EU) 2016/679 and all other relevant EU and UK data protections laws.

Our Data Protection Officer is our HR & Corporate Services Manager, Sandra Haig. Any questions relating to this notice and our privacy practices should be sent to Sandra Haig [sandra.haig@cvha.org.uk](mailto:sandra.haig@cvha.org.uk).

#### **2. How we collect information from you and what information we collect**

We collect information about you:

- when you apply for housing with us, become a tenant, request services/ repairs, enter in to a factoring agreement with us, or where you provide us with your personal details;
- from your arrangements to make payment to us (such as bank details, payment card numbers, employment details, benefit entitlement and any other income and expenditure related information).



We collect the following information about you:

- name;
- address;
- telephone number;
- e-mail address;
- bank details (if using direct debit)
- sequestration details (factored owners);
- trust deed information (factored owners);
- title deeds (factored owners); and
- land disposal records (factored owners).

In addition to collecting information from you we also receive the following information from third parties:

- complaints or other communications regarding behaviour or other alleged breaches of the terms of your contract with us, including information obtained from Police Scotland;
- change of ownership details for factored properties from both sellers' and purchasers' solicitors.

### **3. Why we need this information about you and how it will be used**

We need your information and will use your information:

- to undertake and perform our obligations and duties to you in accordance with the terms of our contract with you;
- to enable us to supply you with the services and information which you have requested;
- to enable us to respond to your repair request, landscape enquiries and complaints;
- to analyse the information we collect so that we can administer, support and improve and develop our business and the services we offer;
- for all other purposes consistent with the proper performance of our operations and business; and
- to contact you for your views on our products and services.

### **4. Processing your information**

We will:

- ensure that the legal basis for processing your personal data is identified in advance and that all processing complies with the law;
- not do anything with your data that you would not expect given the content of our privacy policy and this fair processing notice;
- ensure that appropriate privacy policies are in place advising staff and others how and why their data is being processed, and in particular advising data subjects of their rights;
- only collect and process the personal data that we need for purposes we have identified above;
- ensure that as far as possible the personal data we hold is accurate, or a system is in place for ensuring that it is kept up to date as far as possible;
- only hold onto your personal data for as long as it is needed after which time we will securely erase or delete the personal data. Our Privacy Policy sets out the period of time for which we will retain your personal data; and

- ensure that appropriate security measures are in place to ensure that personal data can only be accessed by those who need to access it and that it is held and transferred securely.

We will ensure that all staff who handle personal data on our behalf are aware of their responsibilities under our Privacy Policy and other relevant data protection and information security policies. We will also ensure that our staff are adequately trained and supervised in the performance of their responsibilities.

## 5. Sharing of Your Information

The information you provide to us will be treated by us as confidential and will be processed only by our employees within the UK. We may disclose your information to other third parties who act for us for the purposes set out in this notice or for purposes approved by you, including the following:

- if we instruct repair or maintenance works, major works, electrical and/or gas safety testing your information may be disclosed to any contractor involved in such repairs or works;
- if we are investigating a complaint, information may be disclosed to Police Scotland, Local Authority departments, the Scottish Fire & Rescue Service and others involved in a complaint, whether they are investigating the complaint or otherwise;
- if we are investigating payments, your information may be disclosed to payment processors, Local Authority and the Department of Work & Pensions;
- if we are seeking court action against you for factoring arrears, we will share your information with our solicitors, and the in-court advice service at the Court;
- if we are conducting a survey of our products and/or services, your information may be disclosed to third parties assisting in the compilation and analysis of the survey results;
- when you make a payment through our third party payment provider (IMPACT), your information will be shared with it;
- if we are providing support with your income and benefit entitlement, we may share you information with the relevant organisations and agencies (such as the Citizens Advice Bureau, Money Matters, and other debt and advice agencies);
- We will disclose your final account to third parties (sellers' and purchasers' solicitors); and
- the Scottish Ministers and their solicitors (in respect of shared equity properties).

Your information will also be shared with third parties with whom the Association has a contractual arrangement for services provision, such as payment processing or letter distribution. The Association will ensure that there is an agreement in place between the Association and the third party which provides adequate safeguards for your information.

Unless required to do so by law, we will not otherwise share, sell or distribute any of the information you provide to us without your consent.

Your information will only be stored within the UK.

## 6. Security

When you give us information we take steps to make sure that your personal information is kept secure and safe. Our Privacy Policy sets out these measures.

## 7. Your rights

There are a number of rights that you can exercise in relation to your personal data held by us. We have processes in place to ensure that we can facilitate any request made by you to exercise your rights. All staff have received training and are aware of your rights. Staff can identify such a request and know who to send it to. The relevant rights that you may exercise are listed below.

All requests to exercise any of the below rights will be considered without undue delay and within one month of receipt as far as possible.

**Subject access:** the right to request information about how personal data is being processed, including whether personal data is being processed, and the right to be allowed access to that data and to be provided with a copy of that data. This includes the right to obtain the following information:

- the purpose of the processing;
- the categories of personal data;
- the recipients to whom data has been disclosed or which will be disclosed;
- the retention period;
- the right to lodge a complaint with the ICO;
- the source of the information if not collected direct from the subject; and
- the existence of any automated decision making.

**Rectification:** the right to allow a data subject to rectify inaccurate personal data concerning them.

**Erasure:** the right to have data erased and to have confirmation of erasure, but only where:

- the data is no longer necessary in relation to the purpose for which it was collected;
- where consent is withdrawn;
- where there is no legal basis for the processing; or
- there is a legal obligation to delete data.

Even if one of the above conditions applies we can hold onto your data in the following circumstances: where processing is necessary for: exercising the rights of freedom of expression; to comply with a legal obligation in the public interest or in the exercise of an official authority; for public health reasons; for archiving purposes; and for the establishment, exercise or defence of legal claims.

**Restriction of processing:** the right to ask for certain processing to be restricted in the following circumstances:

- if the accuracy of the personal data is being contested; or
- if our processing is unlawful but the data subject does not want it erased; or
- if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims; or
- if the data subject has objected to the processing, pending verification of that objection.

**Data portability:** the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if we were processing the data using your consent or on the basis of a contract.

**Object to processing:** the right to object to the processing of personal data relying on the legitimate interests processing condition unless we can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claims.

If you would like to exercise any of your rights as set out above, please contact us at [cvha@cvha.org.uk](mailto:cvha@cvha.org.uk).

## **8. How long we will keep your information**

We review our data retention periods regularly and will only hold your personal data for as long as is necessary for the relevant activity, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you.

We will generally keep your information for the duration of your tenancy or factored owner contract with us. However, we may have to retain certain amounts of data for longer than this. The specific retention periods for which your information will be kept by us are set out in our Privacy Policy. Once your personal data is no longer required by us it will be securely destroyed.

## **9. The Information Commissioner's Office**

You also have the right to complain to the Information Commissioner's Office in relation to our use of your information. The Information Commissioner's Office can be contacted at:

The Information Commissioner's Office – Scotland  
45 Melville Street, Edinburgh, EH3 7HL  
Telephone: 0131 244 9001  
Email: [Scotland@ico.org.uk](mailto:Scotland@ico.org.uk)

## **10. Help us keep your information up to date**

The accuracy of your information is important to us. Please help us keep our records updated by informing us of any changes to your email address and other contact details.

# CLYDE VALLEY GROUP

PROVIDING HOMES | SHAPING COMMUNITIES

## **Clyde Valley Housing Association Limited**

### **How we use your personal information**

You may already know that EU data protection law changed on 25 May 2018. This is the date on which the General Data Protection Regulation (GDPR) came into effect across the EU. The GDPR strengthens the rights you have in relation to your personal information, and it obliges organisations that hold your information to tell you why they are holding it and what they are doing with it. This notice tells you why Clyde Valley Housing Association (CVHA) holds your personal information, and how this information is used by us. You can find out more about how we use your personal information in our Fair Processing Notice which is available at [[www.cvha.org.uk/rightsandresponsibilities/usefuldocumentsandinformation](http://www.cvha.org.uk/rightsandresponsibilities/usefuldocumentsandinformation)].

CVHA collects your personal information if you are a customer (e.g. a tenant or a factored owner) or where we have some other relationship with you (e.g. when you apply to become a member or where you are a member of our customer panel). Your personal information is held and processed by different companies in the CVHA group depending on whether you are a tenant or factored owner. If you are a tenant, your information is held and processed by Clyde Valley Housing Association Limited. If you are a factored owner, your information is held and processed by Clyde Valley Property Services Limited. This information may include basic personal information about you (such as your name, address, telephone number and date of birth) as well as more sensitive information (such as your ethnic origin and medical information). A full list of the information we hold about you can be found in our Fair Processing Notice.

The reason we hold and process your information will depend on the relationship that we have with you. For example, if you are a tenant, we need to hold and process your personal information so that we can provide housing and other services to you. If on the other hand you are a factored owner, we will need to process your information so that we can fulfil our obligations under our contract with you.

We collect your personal information from you when you apply for housing with us or become a factored owner with us. We may collect further information from you over the course of our relationship with you. Information about you may also be collected from third parties such as Government departments (e.g. the Department of Work and Pensions or Local Authorities) and law enforcement agencies (e.g. Police Scotland).

We make sure that we only collect the information about you that we need in order to perform our functions. We store this information securely in both paper and digital formats, and we make sure that it is only disclosed to other third parties where the law allows for this. We only retain your information for as long as it is needed after which it is securely deleted or destroyed.

The GDPR also gives you a number of rights that you can exercise in relation to the information that we hold about you. You have the right to:

1. request that we provide you with a copy of the information we hold about you;
2. have any inaccurate information that we hold about you rectified;
3. request that we erase the information that we hold about you (in certain circumstances);
4. ask that we restrict the processing of your information (in certain circumstances);
5. to be given a copy of your information in a commonly used machine readable format; and
6. object to the processing of your information.

If you would like to exercise any of these rights, please contact us at [cvha@cvha.org.uk](mailto:cvha@cvha.org.uk). More information on all of these rights can be found in our Fair Processing Notice.

If you have any questions about this notice or our privacy practices you can contact our Data Protection Officer, Sandra Haig, on [sandra.haig@cvha.org.uk](mailto:sandra.haig@cvha.org.uk). You can also contact our Data Protection Officer if you are unhappy about the way in which we have dealt with your personal information. If you are not satisfied with the response you receive from us, then you have the right to raise the matter with the Information Commissioner's Office (ICO). More information on how to contact the ICO can be found on [www.ico.org.uk](http://www.ico.org.uk) and in our Fair Processing Notice.

The accuracy of your information is important to us. Please help us keep our records updated by informing us of any changes to your contact details and other information.

Sandra Haig  
Data Protection Officer  
Clyde Valley Housing  
Association  
25<sup>th</sup> May 2018

# CLYDE VALLEY GROUP

PROVIDING HOMES | SHAPING COMMUNITIES

## Clyde Valley Group

### Staff Privacy Notice

(How we use employee information)

This notice explains what information we collect from employees, when we collect it and how we use it. During the course of our activities we will process personal data (which may be held on paper, electronically, or otherwise) about you and we recognise the need to treat it in an appropriate and lawful manner. The purpose of this notice is to make you aware of how we will handle your information.

1. Clyde Valley Housing Association (“**CVHA**”) is a Registered Social Landlord owning, investing in and managing 7000 homes and customers across Lanarkshire and East Dunbartonshire. CVHA operates through a group of companies that provide different services to its customers. CVHA’s head office is located at 50 Scott Street, Motherwell, ML1 1PN.

The personal data that CVHA holds about individuals is processed by different companies within its group. The company that processes the data of an individual depends on the relationship that individual has with CVHA. The personal data of CVHA’s tenants and employees is processed by Clyde Valley Housing Association Limited. The personal data of factored owners, mid-market property owners, and mid-market property tenants is processed by Clyde Valley Property Services Limited through its three subsidiaries:

1. Avant Letting Services Limited (for mid-market property tenants);
2. Nova Property Management Services Limited (for factored owners); and
3. Innov8 Housing Solutions Limited (for mid-market property owners).

The data controller for the purposes of any personal data that you provide to CVHA will be the company that is processing that data, as detailed above. CVHA is registered as data controllers with the Information Commissioner’s Office.

We take the issue of information security and data protection very seriously. We are committed to ensuring that any processing of your personal data by us is in accordance with Data Protection Law. “**Data Protection Law**” includes the Data Protection Act 2018, the General Data Protection Regulation (EU) 2016/679 and all other relevant EU and UK data protections laws.

Our Data Protection Officer is our HR & Corporate Services Manager, Sandra Haig Any questions relating to this notice and our privacy practices should be sent to Sandra Haig [sandra.haig@cvha.org.uk](mailto:sandra.haig@cvha.org.uk).

2. We collect a variety of information about you in order to allow us to effectively manage our employees. This information is obtained both directly from you and from third parties such as employment agencies and pension services providers. This information includes:

- (a) Name;
- (b) Date of Birth;
- (c) Address;
- (d) Telephone Number;
- (e) E-mail address;
- (f) NI number;
- (g) Personal characteristics such as marital status, gender and ethnic group;
- (h) Medical or health information relevant to your employment;
- (i) Details of your qualifications, skills, experience and work history including start and end dates with previous employers and workplaces;
- (j) Details of your work pattern (days and hours) and attendance at work;
- (k) Next of Kin / dependents / emergency contact details;
- (l) GP's details;
- (m) Information about your remuneration, including entitlement to benefits such as pay, pension and holidays;
- (n) Bank Account details;
- (o) GP medical requests/ letters of health related appointments;
- (p) Information about your nationality and entitlement to work in the UK;
- (q) Employment References;
- (r) Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- (s) Assessments of your performance, including performance reviews and related correspondence;
- (t) General correspondence relating to your employment;
- (u) Vehicle details including business insurance;
- (v) Information about any criminal convictions if this is relevant to your job; and
- (w) Details of periods of leave taken by you, including annual leave, sickness absence, family leave and sabbaticals.

3. We need to process the data we hold about you so that we can comply with our obligations as contained in the contract of employment between us and you. This includes:

- (a) Administration of contracts of employment in line with our Terms and Conditions of Employment;
- (b) Payment of salaries;
- (c) Recruitment and selection;
- (d) Pensions and associated benefits, appraisal, training and development;
- (e) Membership of professional bodies;
- (f) SHR annual return; and
- (g) Disclosure checks.

4. We also need to process your personal data in order to allow us to comply with the obligations to which we are subject. For example, we are required;

- (a) to obtain checks regarding your right to work in the UK;
- (b) to deduct tax, National Insurance, and administrate your pension;
- (c) to comply with health and safety laws; and
- (d) to enable you to take periods of leave to which you are entitled.
- (e) to carry out regulatory and/or statutory checks in relation to your engagement with us.

We are also required to process special categories of personal data, such as information about health or medical conditions which we are required to process in line with our obligations under employment law (e.g. information pertaining to any disability you may have or which may arise). Special category personal data is any data that reveals:



- (a) Racial or ethnic origin;
- (b) Religious or philosophical beliefs;
- (c) Political opinion;
- (d) Trade union membership;
- (e) Genetic or biometric data;
- (f) Data concerning health;
- (g) Data concerning sex life or sexual orientation; or
- (h) Data concerning criminal convictions or offences.

We are also entitled to process your data when we have a legitimate interest to do so during and after our employer/employee relationship. This allows us to:

- (a) Run recruitment processes;
- (b) Maintain accurate and up to date employment records, contact details, emergency contact details, and records of employee contractual statutory rights;
- (c) Operate and keep a record of disciplinary and grievance processes;
- (d) Plan for career development, succession planning and workforce planning;
- (e) Operate and keep a record of absence management procedures, to allow workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- (f) Obtain occupational health advice, ensuring that it complies with duties in relation to individuals with disabilities and meets requirements under health and safety law;
- (g) Operate and keep a record of other leave you may take including maternity, paternity, adoption, parental and shared parental leave;
- (h) Ensure effective general HR and business administration;
- (i) Provide references on request for current or past employees;
- (j) Respond to and defend against legal claims; and
- (k) In the event of a business sale/transfer.

5. We may disclose to and share information about you with third parties for the purposes set out in this notice, or for purposes approved by you, including the following:

- (a) To assist in the recruitment process of staff members;
- (b) To allow your pension provider to process pensions information and handle your pension;
- (c) To allow your electronic payslips to be produced and issued to you;
- (d) To obtain employment law advice;
- (e) To HMRC, DWP and other third party agencies; and
- (f) If we enter into a joint venture with or are sold to or merged with another business entity, your information may be disclosed to our new business partners or owners.

6. Your information will only be stored within the UK and EEA.

7. When you give us information we take steps to make sure that your personal information is kept secure and safe. We hold a copy of your personnel file electronically. Access is restricted to the organisation's HR function and line managers. Please see our Privacy Policy for further details on our security arrangements. The Privacy Policy can be found in the HR Policy manual.

8. We review our data retention periods regularly and will only hold your personal data for as long as is necessary for the relevant activity, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you. Data retention guidelines on the information we hold are provided in our Privacy Policy.

9. You have the right at any time to:

- (a) Ask for information about the processing and request a copy of the data we hold about you;
- (b) Object to, or request that we restrict, the processing of your personal data;
- (c) Request that we erase the personal data that we hold about you in certain circumstances; and
- (d) Require us to correct any inaccuracies in your information

10. If you would like to exercise any of the rights outlined above, please contact Customer Services. You have the right to complain to the Information Commissioner's Office in relation to our use of your information: <https://ico.org.uk/make-a-complaint/> .

The accuracy of your information is important to us – please help us keep our records updated by informing the Customer Services Officer (HR) of any changes to your personal and contact details.

# CLYDE VALLEY GROUP

PROVIDING HOMES | SHAPING COMMUNITIES

## Clyde Valley Group

### Privacy Notice

(How we use Board Members' information)

This notice explains what information we collect from Board Members, when we collect it and how we use it. During the course of our activities we will process personal data (which may be held on paper, electronically, or otherwise) about you and we recognise the need to treat it in an appropriate and lawful manner. The purpose of this notice is to make you aware of how we will handle your information.

1. Clyde Valley Housing Association (“**CVHA**”) is a Registered Social Landlord and Registered Charity owning, investing in and managing 7000 homes and customers across Lanarkshire and East Dunbartonshire. CVHA operates through a group of companies that provide different services to its customers. CVHA's head office is located at 50 Scott Street, Motherwell, ML1 1PN.

The personal data that CVHA holds about individuals is processed by different companies within its group. The company that processes the data of an individual depends on the relationship that individual has with CVHA. The personal data of CVHA and Clyde Valley Property Services' (“**CVPS**”) Board Members is processed by Clyde Valley Housing Association Limited.

The data controller for the purposes of any personal data that you provide to CVHA will be the company that is processing that data, as detailed above, and is registered as The Data Controller with the Information Commissioner's Office.

We take the issue of information security and data protection very seriously. We are committed to ensuring that any processing of your personal data by us is in accordance with Data Protection Law. “**Data Protection Law**” includes the Data Protection Act 2018, the General Data Protection Regulation (EU) 2016/679 and all other relevant EU and UK data protections laws.

Our Data Protection Officer is our HR & Corporate Services Manager, Sandra Haig Any questions relating to this notice and our privacy practices should be sent to Sandra Haig [sandra.haiq@cvha.org.uk](mailto:sandra.haiq@cvha.org.uk).

2. We collect a variety of information about you in order to allow us to effectively manage membership of our Board. This information is obtained both directly from you and from third parties such as recruitment agencies and includes:

- (a) Name;
- (b) Address;
- (c) Telephone Number;
- (d) E-mail address;

- (e) Personal characteristics such as gender, racial and ethnic origin, data concerning health;
- (f) Details from your CV and Board Member Application form;
- (g) Information about your nationality;
- (h) Assessments of your performance, including performance reviews and related correspondence;
- (i) Your signed declarations as a Board member (as required by Regulation and to comply with CVHA policies) e.g. Code of Conduct, Payments and Benefits.

3. We need to process the data we hold about you so that we can comply with our Rules and obligations as contained in your appointment as a Board Member. This includes:

- (a) Administration of our governance requirements;
- (b) Board Member recruitment and selection;
- (d) Appraisal, training and development;
- (e) Membership of professional bodies;
- (f) Regulatory compliance to meet the requirements of the Scottish Housing Regulator, the Office of the Scottish Charity Regulator including annual returns;
- (g) Annual returns and information required by Companies House (applies to CVPS members only).

4. We also need to process your personal data in order to allow us to comply with the obligations to which we are subject. For example, we are required;

- (a) to comply with health and safety laws; and
- (b) to carry out regulatory and/or statutory checks in relation to your position with us

We are also required to process special categories of personal data, such as information about health or medical conditions which we are required to process in line with our obligations under equalities legislation (e.g. information pertaining to any disability you may have or which may arise). Special category personal data is any data that reveals:

- (a) Racial or ethnic origin;
- (b) Data concerning health;

We are also entitled to process your data when we have a legitimate interest to do so during and after our governance relationship. This allows us to:

- (a) To assist in the recruitment process of Board Members;
- (b) Maintain accurate and up to date governance records and contact details;
- (c) Operate and keep a record of governance processes;
- (d) Plan for development, succession planning and board planning;
- (e) Operate and keep a record of absence management procedures, to allow governance management and ensure that Board Member are receiving expenses to which they are entitled;
- (f) Ensure effective general and business administration;
- (g) Provide references on request for current or past Board Member;
- (h) Respond to and defend against legal claims;
- (i) Complete a business sale/transfer; and
- (j) To ensure ongoing regulatory and statutory compliance.

5. We may disclose to and share information about you with third parties for the purposes set out in this notice, or for purposes approved by you, including the following:

- (a) To assist in the recruitment process of board members;
- (b) If we enter into a joint venture with or are sold to or merged with another business entity, your information may be disclosed to our new business partners or owners;
- (c) In order to comply with regulatory requirements.

6. Your information will only be stored within the UK and EEA.

7. When you give us information we take steps to make sure that your personal information is kept secure and safe. We hold a copy of your personnel file electronically. Access is restricted to the organisation's corporate function and Chief Executive. Please see our Privacy Policy for further details on our security arrangements. The Privacy Policy can be found in the Board Packs.

8. We review our data retention periods regularly and will only hold your personal data for as long as is necessary for the relevant activity, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you. Data retention guidelines on the information we hold are provided in our Privacy Policy.

9. You have the right at any time to:

- (a) Ask for information about the processing and request a copy of the data we hold about you;
- (b) Object to, or request that we restrict, the processing of your personal data;
- (c) Request that we erase the personal data that we hold about you in certain circumstances; and
- (d) Require us to correct any inaccuracies in your information

10. If you would like to exercise any of the rights outlined above, please contact the Customer Services Officer. You have the right to complain to the Information Commissioner's Office in relation to our use of your information: <https://ico.org.uk/make-a-complaint/> .

The accuracy of your information is important to us – please help us keep our records updated by informing the Customer Services Officer of any changes to your personal and contact details.

## Model Data Sharing Agreement

### DATA SHARING AGREEMENT

between

#[insert name of RSL], a Scottish Charity (Scottish Charity Number #), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number # and having their Registered Office at # (the "Association");

and

#[Insert organisation name, a # [e.g. Company] registered in terms of the Companies Acts with registered number [registered number] and having its registered office/main office at #[ address]] ("#[Party 2]") [Drafting note: amend from Party 2 to suitable defined term];

(each a "Party" and together the "Parties").

### WHEREAS

*Drafting Note: Further detail will require to be inserted here to confirm relationship between Parties to the Agreement. This will depend on the precise nature of relationship so will require to be adapted for every individual use of this model Agreement.*

- (a) The Association and [Insert name of party] ("Party 2") intend that this data sharing agreement will form the basis of the data sharing arrangements between the parties (the "Agreement"); and
- (b) The intention of the Parties is that they shall each be independent Data Controllers in respect of the Data that they process under this Agreement.
- (c) Nothing in this Agreement shall alter, supersede, or in any other way affect the terms of #[insert details of relationship/ contract with Party 2]

### NOW THEREFORE IT IS AGREED AS FOLLOWS:

#### 1 DEFINITIONS

1.1 In construing this Agreement, capitalised words and expressions shall have the meaning set out opposite:

"**Agreement**" means this Data Sharing Agreement, as amended from time to time in accordance with its terms, including the Schedule;

"**Business Day**" means any day which is not a Saturday, a Sunday or a bank or public holiday throughout Scotland;

"**Data**" means the information which contains Personal Data and Sensitive Personal Data (both of which have the definition ascribed to them in Data Protection Law) described in Part 1;

"**Data Controller**" has the meaning set out in Data Protection Law;

**"Disclosing Party"** means the Party (being either the Association or #[Party 2], as appropriate) disclosing Data (or on behalf of whom Data is disclosed to the Data Recipient);

**"Data Protection Law"** means Law relating to data protection, the processing of personal data and privacy from time to time, including:

- (a) the Data Protection Act 1998;
- (b) (with effect from 25 May 2018) the General Data Protection Regulation (EU) 2016/679;
- (c) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
- (d) 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;

**"Data Recipient"** means the party (being either the Association or #[Party 2], as appropriate) to whom Data is disclosed;

**"Data Subject"** means any identifiable individual to whom any Data relates: and the categories of data subjects within the scope of this Agreement are listed in Part 1;

**"Data Subject Request"** means a written request of either party as Data Controller by or on behalf of a Data Subject to exercise any rights conferred by Data Protection Law in relation to the data or the activities of the parties contemplated by this Agreement;

**"Disclosing Party"** means the party (being either the Association or #[Party 2], as appropriate) disclosing Data to the Data Recipient;

**"Information Commissioner"** means the UK Information Commissioner and any successor;

**"Law"** means any statute, directive, other legislation, law or regulation in whatever form, delegated act (under any of the foregoing), rule, order of any court having valid jurisdiction or other binding restriction, decision or guidance in force from time to time;

**"Legal Basis"** means in relation to either Party, the legal basis for sharing the Data as described in Clause **Error! Reference source not found.** and as set out in Part 2;

**"Purpose"** means the purpose referred to in Part 2;

**"Representatives"** means, as the context requires, the representative of the Association and/or the representative of #[Party 2] as detailed in Part 4 of the Schedule. The same may be changed from time to time on notice in writing by the relevant Party to the other Party;

**"Schedule"** means the Schedule in 6 Parts annexed to this Agreement and a reference to a "Part" is to a Part of the Schedule; and

**"Security Measures"** has the meaning given to that term in Clause **Error! Reference source not found.**

1.2 In this Agreement unless the context otherwise requires:

1.2.1 words and expressions defined in Data Protection Law shall have the same meanings in this Agreement so that, in the case of Data Protection Law, words and expressions shall be interpreted in accordance with:

- (a) the Data Protection Act 1998, in respect of processing undertaken on or before 24 May 2018;
- (b) the General Data Protection Regulation (EU) 2016/679, in respect of processing undertaken on or after 25 May 2018; and
- (c) in respect of processing undertaken on or after the date on which legislation comes into force that replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, that legislation;

1.2.2 more generally, references to statutory provisions include those statutory provisions as amended, replaced, re-enacted for the time being in force and shall include any bye-laws, statutory instruments, rules, regulations, orders, notices, codes of practice, directions, consents or permissions and guidelines (together with any conditions attached to the foregoing) made thereunder;

## **2 DATA SHARING**

### **Purpose and Legal Basis**

2.1 The Parties agree to share the Data for the Purpose in accordance with the provisions of Part 2 of the Schedule.

2.2 Save as provided for in this Agreement, the Parties agree not to use any Data disclosed in terms of this Agreement in a way that is incompatible with the Purpose.

2.3 Each Party shall ensure that it processes the Data fairly and lawfully in accordance with Data Protection Law and each Party as Disclosing Party warrants to the other



Party in relation to any Data disclosed, that such disclosure is justified by a Legal Basis.

### **Parties Relationship**

2.4 The Parties agree that the relationship between them is such that any processing of the Data shall be on a Data Controller to Data Controller basis. The Data Recipient agrees that:

2.4.1 it is a separate and independent Data Controller in respect of the Data that it processes under this Agreement, and that the Parties are not joint Data Controllers or Data Controllers in common;

2.4.2 it is responsible for complying with the obligations incumbent on it as a Data Controller under Data Protection Law (including responding to any Data Subject Request);

2.4.3 it shall comply with its obligations under Part 6 of the Schedule;

2.4.4 it shall not transfer any of the Data outside the United Kingdom except to the extent agreed by the Disclosing Party;

2.4.5 Provided that where the Data has been transferred outside the United Kingdom, the Disclosing Party may require that the Data is transferred back to within the United Kingdom:

(a) on giving not less than 3 months' notice in writing to that effect; or

(b) at any time in the event of a change in Law which makes it unlawful for the Data to be processed in the jurisdiction outside the United Kingdom where it is being processed; and

2.4.6 it shall implement appropriate technical and organisational measures including the security measures set out in Part 5 of the Schedule (the "**Security Measures**"), so as to ensure an appropriate level of security is adopted to mitigate the risks associated with its processing of the Data, including against unauthorised or unlawful processing, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or damage or access to such Data.

2.5 The Disclosing Party undertakes to notify in writing the other as soon as practicable if an error is discovered in Data which has been provided to the Data Recipient, to ensure that the Data Recipient is then able to correct its records. This will happen whether the error is discovered through existing Data quality initiatives or is flagged up through some other route (such as the existence of errors being directly notified to the Disclosing Party by the Data Subjects themselves).

### **Transferring Data**

- 2.6 Subject to the Data Recipient's compliance with the terms of this Agreement, the Disclosing Party undertakes to endeavour to provide the Data to the Data Recipient on a non-exclusive basis in accordance with the transfer arrangements detailed in Part 3 of the Schedule.

### **3 BREACH NOTIFICATION**

- 3.1 Each Party shall, promptly (and, in any event, no later than 12 hours after becoming aware of the breach or suspected breach) notify the other party in writing of any breach or suspected breach of any of that Party's obligations in terms of Clauses 1 and/or 2 and of any other unauthorised or unlawful processing of any of the Data and any other loss or destruction of or damage to any of the Data. Such notification shall specify (at a minimum):
- 3.1.1 the nature of the personal data breach or suspected breach;
  - 3.1.2 the date and time of occurrence;
  - 3.1.3 the extent of the Data and Data Subjects affected or potentially affected, the likely consequences of any breach (in the case of a suspected breach, should it have occurred) for Data Subjects affected by it and any measures taken or proposed to be taken by the that party to contain the breach or suspected breach; and
  - 3.1.4 any other information that the other Party shall require in order to discharge its responsibilities under Data Protection Law in relation to such breach or suspected breach.
- 3.2 The Party who has suffered the breach or suspected breach shall thereafter promptly, at the other Party's expense (i) provide the other Party with all such information as the other Party reasonably requests in connection with such breach or suspected breach; (ii) take such steps as the other Party reasonably requires it to take to mitigate the detrimental effects of any such breach or suspected breach on any of the Data Subjects and/or on the other Party; and (iii) otherwise cooperate with the other Party in investigating and dealing with such breach or suspected breach and its consequences.
- 3.3 The rights conferred under this Clause 3 are without prejudice to any other rights and remedies for breach of this Agreement whether in contract or otherwise in law.

#### 4 DURATION, REVIEW AND AMENDMENT

- 4.1 This Agreement shall come into force immediately on being executed by all the Parties and continue for #[*insert termination: this will be when Parties cease sharing data in terms of contractual relationship with each other*], unless terminated earlier by the Disclosing Party in accordance with Clause 4.5.
- 4.2 This Agreement will be reviewed one year after it comes into force and every two years thereafter until termination or expiry in accordance with its terms.
- 4.3 In addition to these scheduled reviews and without prejudice to Clause 4.5, the Parties will also review this Agreement and the operational arrangements which give effect to it, if any of the following events takes place:
- 4.3.1 the terms of this Agreement have been breached in any material aspect, including any security breach or data loss in respect of Data which is subject to this Agreement; or
- 4.3.2 the Information Commissioner or any of his or her authorised staff recommends that the Agreement be reviewed.
- 4.4 Any amendments to this Agreement will only be effective when contained within a formal amendment document which is formally executed in writing by both Parties.
- 4.5 In the event that the Disclosing Party has any reason to believe that the Data Recipient is in breach of any of its obligations under this Agreement, the Disclosing Party may at its sole discretion:
- 4.5.1 suspend the sharing of Data until such time as the Disclosing Party is reasonably satisfied that the breach will not re-occur; and/or
- 4.5.2 terminate this Agreement immediately by written notice to the Data Recipient if the Data Recipient commits a material breach of this Agreement which (in the case of a breach capable of a remedy) it does not remedy within five (5) Business Days of receiving written notice of the breach.
- 4.6 Where the Disclosing Party exercises its rights under Clause **Error! Reference source not found.**, it may request the return of the Data (in which case the Data Recipient shall, no later than fourteen (14) days after receipt of such a written request from the Disclosing Party, at the Disclosing Party's option, return or permanently erase/destroy all materials held by or under the control of the Data Recipient which contain or reflect the Data and shall not retain any copies, extracts or other reproductions of the Data either in whole or in part and shall confirm having done so to the other Party in writing), save that the Data Recipient will be permitted to retain

one copy for the purpose of complying with, and for so long as required by, any law or judicial or administrative process or for its legitimate internal compliance and/or record keeping requirements.

## **5 LIABILITY**

- 5.1 Nothing in this Agreement limits or excludes the liability of either Party for:
- 5.1.1 death or personal injury resulting from its negligence; or
  - 5.1.2 any damage or liability incurred as a result of fraud by its personnel; or
  - 5.1.3 any other matter to the extent that the exclusion or limitation of liability for that matter is not permitted by law.
- 5.2 The Data Recipient indemnifies the Disclosing Party against any losses, costs, damages, awards of compensation, any monetary penalty notices or administrative fines for breach of Data Protection Law and/or expenses (including legal fees and expenses) suffered, incurred by the Disclosing Party, or awarded, levied or imposed against the other party, as a result of any breach by the Data Recipient of its obligations under this Agreement. Any such liability arising from the terms of this Clause 5.2 is limited to £# (# STERLING) in the aggregate for the duration of this Agreement.
- 5.3 Subject to Clauses **Error! Reference source not found.** and **Error! Reference source not found.** above:
- 5.3.1 each Party excludes all liability for breach of any conditions implied by law (including any conditions of accuracy, security, completeness, satisfactory quality, fitness for purpose, freedom from viruses, worms, trojans or other hostile computer programs, non-infringement of proprietary rights and the use of reasonable care and skill) which but for this Agreement might have effect in relation to the Data;
  - 5.3.2 neither Party shall in any circumstances be liable to the other party for any actions, claims, demands, liabilities, damages, losses, costs, charges and expenses that the other party may suffer or incur in connection with, or arising (directly or indirectly) from, any use of or reliance on the Data provided to them by the other Party; and
  - 5.3.3 use of the Data by both Parties is entirely at their own risk and each party shall make its own decisions based on the Data, notwithstanding that this Clause shall not prevent one party from offering clarification and guidance to the other party as to appropriate interpretation of the Data.

## **6 DISPUTE RESOLUTION**

- 6.1 The Parties hereby agree to act in good faith at all times to attempt to resolve any dispute or difference relating to the subject matter of, and arising under, this Agreement.
- 6.2 If the Representatives dealing with a dispute or difference are unable to resolve this themselves within twenty (20) Business Days of the issue arising, the matter shall be escalated to the following individuals in Part 4 of the Schedule identified as escalation points who will endeavour in good faith to resolve the issue.
- 6.3 In the event that the Parties are unable to resolve the dispute amicably within a period of twenty (20) Business Days from date on which the dispute or difference was escalated in terms of Clause **Error! Reference source not found.**, the matter may be referred to a mutually agreed mediator. If the identity of the mediator cannot be agreed, a mediator shall be chosen by the Dean of the Royal Faculty of Procurators in Glasgow.
- 6.4 If mediation fails to resolve the dispute or if the chosen mediator indicates that the dispute is not suitable for mediation, and the Parties remain unable to resolve any dispute or difference in accordance with Clauses 6.1 to 6.3, then either Party may, by notice in writing to the other Party, refer the dispute for determination by the courts in accordance with Clause **Error! Reference source not found.**
- 6.5 The provisions of Clauses 6.1 to 6.4 do not prevent either Party from applying for an interim court order whilst the Parties attempt to resolve a dispute.

## **7 NOTICES**

- 7.1 Any Notices to be provided in terms of this Agreement must be provided in writing and addressed to the relevant Party in accordance with the contact details noted in Part 4 of the Schedule, and will be deemed to have been received (i) if delivered personally, on the day of delivery; (ii) if sent by first class post or other next working day delivery, the second day after posting; (iii) if by courier, the date and time the courier's delivery receipt is signed; or (iv) if by fax, the date and time of the fax receipt.

**8 GOVERNING LAW**

8.1 This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) (a "**Dispute**") shall, in all respects, be governed by and construed in accordance with the law of Scotland. Subject to Clause 6, the Parties agree that the Scottish Courts shall have exclusive jurisdiction in relation to any Dispute.

**IN WITNESS WHEREOF** these presents consisting of this and the preceding 6 pages together with the Schedule in 6 parts hereto are executed by the Parties hereto as follows:

On behalf of the Association

at

on

by

\_\_\_\_\_

Print Full Name

\_\_\_\_\_

Director/Secretary/Authorised  
Signatory

before this witness

\_\_\_\_\_

Print Full Name

\_\_\_\_\_

Witness

Address

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

On behalf of #[Party 2]

at

on

by

\_\_\_\_\_  
Print Full Name

\_\_\_\_\_  
Director/Secretary/Authorised  
Signatory

before this witness

\_\_\_\_\_  
Print Full Name

\_\_\_\_\_  
Witness

Address

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_  
**THIS IS THE SCHEDULE REFERRED TO IN THE FOREGOING DATA SHARING AGREEMENT BETWEEN  
THE ASSOCIATION AND #[PARTY 2]**

## **SCHEDULE PART 1 – DATA**

***Drafting Note: This Part should contain details of the Personal Data to be shared between Parties and will need to be populated on a case by case basis when utilising this Agreement.***

### **DATA SUBJECTS**

For the purposes of this Agreement, Data Subjects are all living persons about whom information is transferred between the Parties.



## Model Data Processor Addendum

*[Drafting Note: It is anticipated that specific standard clauses will require to be included within finalised DP Addendums depending on the third party processor and nature of the member's relationship with them, in which case this draft will require to be updated to reflect that]*

### DATA PROTECTION ADDENDUM

between

**#[insert name of RSL]**, a Scottish Charity (Scottish Charity Number #), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number # and having their Registered Office at # (the "Association");

and

**#[Insert organisation name, a # [e.g. Company]** registered in terms of the Companies Acts with registered number *[registered number]* and having its registered office/main office at **#[address]** (the "Processor")

(each a "Party" and together the "Parties")

### WHEREAS

*[Drafting Note: Further detail will require to be inserted here to confirm relationship between Parties to the Agreement. This will depend on the precise nature of relationship so will require to be adapted for every individual use of this model Agreement.]*

- (d) The Association and the Processor have entered in to an agreement/ contract to **#[insert detail]** (hereinafter the "Principal Agreement"/"Principal Contract");
- (e) This Data Protection Addendum forms part of the Principal Agreement/Principal Contract (\*delete as appropriate); and
- (f) In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

### 1. Definitions

- 1.1 The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalised terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement/Contract shall remain in full force and effect. In this Addendum,

the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

- 1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Association Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws;
- 1.1.2 "**Association Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of the Association pursuant to or in connection with the Principal Agreement/Contract;
- 1.1.3 "**Contracted Processor**" means Processor or a Subprocessor;
- 1.1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;
- 1.1.5 "**EEA**" means the European Economic Area;
- 1.1.6 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;
- 1.1.7 "**GDPR**" means EU General Data Protection Regulation 2016/679;
- 1.1.8 "**Restricted Transfer**" means:
  - 1.1.8.1 *a transfer of Association Personal Data from the Association to a Contracted Processor; or*
  - 1.1.8.2 *an onward transfer of Association Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,*in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);
- 1.1.9 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of the Processor for the Association pursuant to the Principal Agreement/ Contract;
- 1.1.10 "**Subprocessor**" means any person (including any third party and any , but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of Processor which is engaged in the Processing of Personal Data on behalf of the Association in connection with the Principal Agreement/Contract; and

- 1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their related terms shall be construed accordingly.
- 1.3 The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

## **2. Processing of Association Personal Data**

- 2.1 The Processor shall:
- 2.1.1 comply with all applicable Data Protection Laws in the Processing of Association Personal Data; and
  - 2.1.2 not Process Association Personal Data other than on the Association's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform the Association of that legal requirement before the relevant Processing of that Personal Data.
- 2.2 The Association
- 2.2.1 Instructs the Processor (and authorises Processor to instruct each Subprocessor) to:
    - 2.2.1.1 *Process Association Personal Data; and*
    - 2.2.1.2 *in particular, transfer Association Personal Data to any country or territory,*as reasonably necessary for the provision of the Services and consistent with the Principal Agreement/Contract; and
  - 2.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 2.2.1.
- 2.3 The Schedule to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Association Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). The Association may make reasonable amendments to the Schedule by written notice to Processor from time to time as the Association reasonably considers necessary to meet those requirements. Nothing in the Schedule (including as amended pursuant to this section 2.3) confers any right or imposes any obligation on any party to this Addendum.

### 3. **Processor and Personnel**

The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Association Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Association Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

### 4. **Security**

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall in relation to the Association Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

### 5. **Subprocessing** [*Drafting Note: This clause should be adjusted depending on the arrangements between Parties*]

5.1 The Association authorises the Processor to appoint (and permit each Subprocessor appointed in accordance with this section 5 to appoint) Subprocessors in accordance with this section 5 and any restrictions in the Principal Agreement.

5.2 The Processor may continue to use those Subprocessors already engaged by the Processor as at the date of this Addendum, subject to the Processor in each case as soon as practicable meeting the obligations set out in section 5.4.

5.3 The Processor shall give the Association prior written notice of its intention to appoint a Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. The Processor shall not appoint (nor disclose any Association Personal Data to) the proposed Subprocessor except with the prior written consent of the Association.

5.4 With respect to each Subprocessor, the Processor or the relevant shall:

5.4.1 before the Subprocessor first Processes Association Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level

of protection for Association Personal Data required by the Principal Agreement;

5.4.2 ensure that the arrangement between on the one hand (a) the Processor, or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Association Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

5.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) the Processor or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Association Personal Data; and

***[Drafting Note: Each member organisation will require to check arrangements with its Data Processors to ascertain where the Processing is taking place – i.e. within UK/EEA or outwith. If outwith, where. The Standard Contractual Clauses are not appended to this initial draft for discussion as it is not anticipated that member organisations will be contracting with Data Processors who are Processing Personal Data outwith the UK/EEA]***

5.4.4 provide to the Association for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as the Association may request from time to time.

5.5 The Processor shall ensure that each Subprocessor performs the obligations under sections 2.1, 3, 4, 6.1, 7.2, 8 and 10.1, as they apply to Processing of Association Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of the Processor.

## **6. Data Subject Rights**

6.1 Taking into account the nature of the Processing, the Processor shall assist the Association by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Association's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 The Processor shall:

- 6.2.1 promptly notify the Association if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Association Personal Data; and
- 6.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of the Association or as required by Applicable Laws to which the Contracted Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform the Association of that legal requirement before the Contracted Processor responds to the request.

## **7. Personal Data Breach**

- 7.1 The Processor shall notify the Association without undue delay upon the Processor or any Subprocessor becoming aware of a Personal Data Breach affecting the Association Personal Data, providing the Association with sufficient information to allow it to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
- 7.2 The Processor shall co-operate with the Association and at its own expense take such reasonable commercial steps as are directed by the Association to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

## **8. Data Protection Impact Assessment and Prior Consultation**

The Processor shall provide reasonable assistance to the Association with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Association reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Association Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

## **9. Deletion or return of Association Personal Data**

- 9.1 Subject to sections 9.2 and 9.3, the Processor shall promptly and in any event within seven (7) days of the date of cessation of any Services involving the Processing of Association Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.
- 9.2 Subject to section 9.3, the Association may in its absolute discretion by written notice to the Processor within seven (7) days of the Cessation Date require the Processor to (a) return a complete copy of all Association Personal Data to the Association by

secure file transfer in such format as is reasonably notified by the Association to the Processor; and (b) delete and procure the deletion of all other copies of Association Personal Data Processed by any Contracted Processor. The Processor shall comply with any such written request within seven (7) days of the Cessation Date.

- 9.3 Each Contracted Processor may retain Association Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that the Processor shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.
- 9.4 Processor shall provide written certification to the Association that it has fully complied with this section 9 within fourteen (14) days of the Cessation Date.

## **10. Audit rights**

- 10.1 Subject to sections 10.2 and 10.3, the Processor shall make available the Association on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by the Association or an auditor mandated by the Association in relation to the Processing of the Association Personal Data by the Contracted Processors.
- 10.2 Information and audit rights of the Association only arise under section 10.1 to the extent that the Principal Agreement/Contract does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).
- 10.3 Where carrying out an audit of Personal Data, the Association shall give the Processor reasonable notice of any audit or inspection to be conducted under section 10.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:
- 10.3.1 to any individual unless they produce reasonable evidence of identity and authority; or
- 10.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the Association undertaking an audit has given notice to the Processor that this is the case before attendance outside those hours begins

## **11. General Terms**

### ***Governing law and jurisdiction***

- 11.1 The Parties hereby submit to the choice of jurisdiction stipulated in the Principal Agreement/Contract with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and
- 11.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement/Contract.

### ***Order of precedence***

- 11.3 Nothing in this Addendum reduces the Processor's obligations under the Principal Agreement/Contract in relation to the protection of Personal Data or permits the Processor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement/Contract.
- 11.4 Subject to section 11.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement/Contract and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

***[Drafting Note: see comments above re Restricted Transfers etc and the applicability of standard contractual clauses]***

### ***Changes in Data Protection Laws, etc.***

- 11.5 The Association may:
- 11.5.1 by giving at least twenty eight (28) days' written notice to the Processor, from time to time make any variations to the terms of the Addendum which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and
- 11.5.2 propose any other variations to this Addendum which the Association reasonably considers to be necessary to address the requirements of any Data Protection Law.

### ***Severance***

- 11.6 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its



validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

On behalf of the Association

at

on

by

\_\_\_\_\_  
Print Full Name

\_\_\_\_\_  
Director/Secretary/Authorised  
Signatory

before this witness

\_\_\_\_\_  
Print Full Name

\_\_\_\_\_  
Witness

Address

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_  
On behalf of the Processor

at

on

by

\_\_\_\_\_

\_\_\_\_\_

Print Full Name

Director/Secretary/Authorised  
Signatory

before this witness

\_\_\_\_\_  
Print Full Name

\_\_\_\_\_  
Witness

Address

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

## **SCHEDULE**

**This is the Schedule referred to in the foregoing Data Protection Addendum between  
the Association and the Processor**