Policy Name: Data Protection Policy

Policy Number: G05

Policy Owner	Senior Governance and Compliance Officer		
Responsible Executive	Director of Finance and Corporate Services		
Effective Date	November 2025		
Review Date	November 2028		
Approved By	Executive Management Team		
Date Approved	**November 2025**		
EIA Status	**Initial Screening Conducted**	**Yes**	**No**
		X	
	Full EIA Conducted	**Yes**	**No**
Posted on Website	Yes		

If you need this publication in larger print, audio form, Braille, or in another language, please contact our office.

Contents

1. Introduction

1.1. Clyde Valley Housing Association (hereinafter the "Association") aims to provide homes and services of the highest standard. In doing so the Association is committed to ensuring the secure and safe management of data held by the Association in relation to customers, staff and other individuals. The Association's staff members have a responsibility to ensure compliance with the terms of this policy, and to manage the data of individuals in accordance with the procedures outlined in this policy and documentation referred to herein.

1.2. The Association needs to gather and use certain information about individuals. These can include customers (tenants, factored owners, etc.), employees and other individuals that the Association has a relationship with. The Association manages a significant amount of data, from a variety of sources. This data includes personal data and sensitive personal data (known as special categories of personal data and criminal offence data under the UK GDPR).

1.3. 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.

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

2. Scope of the Policy

2.1. This Data Protection Policy applies to all personal data processed by the Association, including data collected through our website, mobile applications, and any other services we offer. It covers the collection, use, disclosure, transfer and storage of personal data. This policy is designed to ensure compliance with data protection laws and regulations, including the UK General Data Protection Regulation (UK GDPR) and other relevant privacy laws.

2.2 The Policy applies to all employees, contractors, and third party service providers who handle personal data on behalf of the Association. It also extends to all individuals whose personal data we process, including customers, partners and website visitors.

3. Policy Aims and Objectives

3.1 This Policy sets out the Association's duties in processing that data, and the procedures for the management of such data, including subject access to records and creation and management of records including retention and disposal of records.

3.2 The aim of this Data Protection Policy is to ensure the protection of personal data and to uphold the privacy rights of individuals. Our objectives are to:

- Comply with all applicable data protection laws and regulations.
- Safeguard the confidentiality, integrity, and availability of personal data.
- Promote transparency in our data processing activities.
- Ensure that personal data is collected, used and stored responsibly, legally and ethically.
- Provide individuals with clear information about their data protection rights and how to exercise them.

4. Definitions

4.1 This section defines any key terms that have been used within the policy to ensure consistent understanding.

Key Term	Definitions
Personal Data	Any information relating to an identified or identifiable living individual.
Processing	Any operation or set of operations performed on personal data, whether by automated means or not, such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure or destruction.
Data Subject	The individual to whom personal data relates.
Data Controller	The entity that determines the purposes and means of processing personal data.
Data Processor	The entity that processes personal data on behalf of the controller.
Consent	Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.
Subject Access Request (SAR)	A request made by or on behalf of an individual for the information which they are entitled to ask for under data protection law.
Criminal Offence Data	Personal data relating to criminal convictions and offences or related security measures including suspicion or allegations of criminal activity
Special Category Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation

5. Procurement Requirements

5.1. This section outlines the principles and procedures for the procurement of goods and services to ensure compliance with data protection laws and regulations. A GDPR Addendum is included as part of tender documentation and must be submitted by contractors when tender is submitted. (appendix 5) .

5.2 Before engaging any contractor, the Association will conduct a thorough assessment to ensure that the contractor complies with applicable data protection laws. This assessment will include a review of the contractor's data protection policies, security measures, and any relevant certifications.

5.3 All contractors that process personal data on behalf of the Association must enter into a Data Processing Agreement (DPA). The DPA will outline the contractor's obligations regarding the processing of personal data, including data security, confidentiality, and compliance with data protection laws.

5.4 The Association will conduct regular due diligence on all contractors to ensure ongoing compliance with data protection laws. This may include periodic audits, reviews of contractor's data protection practices, and assessments of any changes in the contractor's operations that may impact data protection.

5.5 The Association will ensure that contractors only process personal data that is necessary for the provision of goods and services. Any unnecessary collection or processing of personal data by contractors is strictly prohibited.

5.6 Contractors must implement appropriate, technical and organisational measures to protect personal data against unauthorised access, loss or destruction. These measures must be in line with the law, industry standards and best practices.

5.7 Contractors are required to notify the Association immediately in the event of a breach that affects personal data. The notification must include details of the breach, the impact on personal data, and the measures taken to mitigate the breach.

5.8 The Association reserves the right to terminate any contractor relationship if the contractor fails to comply with data protection laws or the terms of the Data Processing Agreement.

6. Notification

6.1 Clyde Valley Housing Association is registered as a Data Controller (Reference Z7559249) and will notify the Information Commissioner's Office of:

- The personal data being or to be processed;
- The category or categories of data subject to which they relate;
- The purposes for which the data are being or are to be processed;
- The people to whom the Association may wish to disclose the information; and
- The names or a description of any countries or territories outside the United Kingdom to which the Association may wish to transfer the personal data.

6.2 Further information on data protection is available from the Information Commissioner's Office via telephone on 0303 123 1113 and from the website at www.ico.org.uk.

7. Data

7.1. The Association holds a variety of Personal Data relating to individuals, including customers, employees, member and Board members and other individuals that the Association has a relationship with . The specific data that the Association holds and processes is detailed within the various Privacy Notices made available to different categories of data subjects as well as in the Data Protection Addendum to the Terms of and Conditions of Employment which has been provided to all employees.

7.2. The data held by the Association about data subjects includes Personal Data Special Category Personal Data and Criminal Offence Data.

7.3. Data Protection Principles

7.3.1. The Association complies with the Data Protection Principles set out below. When processing Personal Data (including Special Category Personal Data and Criminal Offence 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**").

7.3.2. 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 section 10.

7.4. Data Processing

7.4.1. Some of the Association's work is outsourced to data processors (e.g., payroll providers, maintenance and repair contractors).

7.4.2. A data processor must comply with data protection law. 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.

7.4.3. If a data processor wishes to sub-contact their processing, prior written consent of the Association must be obtained.

7.4.4. Where the Association contracts with a third party to process personal data held by the Association, it shall require the third party to enter into a 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.

7.4.5. 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 its deals with (e.g., factored owners and mid-market property owners).

7.5. Processing of Personal Data

7.5.1. 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
- 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.

7.6. Fair Processing Notice

7.6.1. The Association has produced a variety of Privacy Notices (FPN) and it is required to provide the appropriate one to each data subject whose Personal Data is processed by the Association. That FPN must be provided to the data subject when the data is provided to the Association.

7.6.2. The Privacy Notices are provided at **Appendices 2a-c**. They set out the Personal Data processed by the Association and the basis for that Processing. The appropriate document must be provided to each data subject at the outset of processing their data.

7.7. Association Employees

7.7.1. Employee Personal Data and, where applicable, Special Category Personal Data or Criminal Offence 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.

7.7.2. An employee may obtain a copy of their Personal Data held by the Association by submitting a written request to the People Director/Chief Executive or via a Subject Access Request which will be responded to by the Data Protection Officer.

7.8. Processing Based on Consent

7.8.1 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. 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 where possible the data subject should sign a relevant consent form if willing to consent. Where a data subject is unable to sign either for reasons of ability or practicality present maybe provide oral and this will be recorded and a record kept. Any consent to be obtained by the Association must be for a specific and defined purpose (i.e. general consent cannot be sought) Records of consent must be kept.

7.8.2 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, unless explicitly given and recorded as its legal basis for processing when processing employee Personal Data.

7.9. Processing of Special Category Personal Data or Sensitive Personal Data

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

- the data subject has given explicit consent to the processing of this data for a specified purpose.
- processing is necessary 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

8. Data Sharing

8.1. The Association shares some of its data with various 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 law, the Association may require the third-party organisations to enter into an agreement with the Association governing the processing of data, security measures to be implemented and responsibility for breaches. These agreements are known as Data Sharing Agreements.

8.2. The Association is a data controller in relation to all Personal Data that it decides to collect and process.

8.3. From time to time, the Association will require to share Personal Data with third parties who require to process data in accordance with Data Protection Principles. 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.

8.4. 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 into 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.

Paper Storage

8.5. 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, for example external consultants or visitors 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, via confidential waste bins which are available in the office. 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 Data Retention Schedule.

Electronic Storage

8.6. Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should be protected using access permissions where possible with a fallback of password protecting if needed when being sent internally or externally to the Association's data processors or those with whom the Association has entered into a Data Sharing Agreement. This may be sent via a password protected email. Personal data must not be stored on any removable devices such as USB, … due to significant cyber and data security risks.. Personal Data should not be saved directly to mobile devices and should be stored on designated One Drives, email systems and servers.

Archiving, Retention and Destruction of Data

8.7. 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 document retention guidelines.

8.8. It is essential that we do not keep data and information that we are not required to keep. As this is the case, we have a retention schedule in place which should be followed by all staff and data and information should not be kept beyond these timescales – Appendix 1.

8.9. When archiving data and information, both paper based and electronic, details should be clearly outlined on the box or file when the information should be destroyed in line with the retention timelines. Please note that these retention timescales also apply to information that is held on our IT systems and databases.

8.10. Unless a record of signatures is required, general office information should be held electronically rather than by hard copy. This will avoid any unnecessary storage. The Association ensure that adequate backup systems in place for the retention of electronic files.

8.11. The data retention schedule will also ensure that data and information is manageable and can be stored and access effectively.

8.12. All departments should review the data and information they hold on a regular basis. When archiving information staff should include the following:

- Any information that is over a year old should be electronically archived as per the retention schedule.
- Any information that is not required should be destroyed as per the retention schedule.
- Any information that is archived and due to be destroyed should be destroyed as per the retention schedule.

8.13. When archiving data and information, electronically or hard copies, the following should be applied:

- The data and information should be stored in a tidy and logical system – our preferred option is our electronic document management system.
- The archive box or electronic file should be labelled with the following information:
  - What is the data and information e.g. invoices.
  - The date that relates to the information e.g. 2024/25 or September to November 2024.
  - When the data and information should be destroyed.
  - File/box number.

8.14. It is essential that the disposal of records is undertaken in accordance with these policies and procedures. All paper based records containing personal information should be shredded or disposed of through confidential waste systems. All electronic records containing personal information should be deleted completely from the system.

9. Breaches

9.1. 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).

9.2. 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 occurring. 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 sections 9.3 – 9.4.

9.3. Internal Reporting

9.3.1. 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 (using

the data breach report form) (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on the data subject(s).

- the Association must seek to contain the breach by whatever means available.
- the Line Manager of the person responsible for the breach must complete the Data Breach Investigation Form and ensure that all mitigations have been completed to contain the breach.
- 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 section 9.3.
- notify third parties in accordance with the terms of any applicable Data Sharing Agreements.

9.4. Reporting to the ICO and Data Subjects

9.4.1. The DPO will require to report any 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 DPO must also consider whether it is appropriate to notify those data subjects affected by the breach. 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.

9.4.2. 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.

9.4.3. 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.

10. Data Subject Rights

10.1. Under data protection law, 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, whether in written or electronic form.
- **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 the Association's Privacy Notice.

11. Subject Access Requests

11.1. Data subjects are permitted to view or obtain copies of 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 includes data relating to other data subjects, must (where appropriate to do so) 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.

11.2. A complaints process is in place to respond to complaints about responses to subject access requests as per ICO guidelines.

12. The Right to be Forgotten

12.1. A data subject can submit a request in writing to the Association seeking that the Association erase the data subject's Personal Data in its entirety.

12.2. Each request received by the Association will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests. The DPO will have responsibility for accepting or refusing the data subject's request and will respond in writing to the request.

13. The Right to Restrict or Object to Processing

13.1. A data subject may request that the Association restrict its processing of the data subject's Personal Data, or object to the processing of that data.

13.2. In the event that any direct marketing is undertaken from time to time by the Association, a data subject has an absolute right to object to processing of this nature by the Association, and if the Association receives a written request to cease processing for this purpose, then it must do so immediately.

13.3. Each request (other than in relation to direct marketing) 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. The DPO will have responsibility for accepting or refusing the data subject's request and will respond in writing to the request.

14. CCTV

14.1. CCTV is installed in Scott Street at the main entrance points, there is also CCTV installed in some estate car parks and bin areas. The CCTV installed covers only the Association's property areas and does not cover any personal homes. We comply in full with all GDPR and data protection law requirements, including clear signage, justifiable purpose (like security), responsible data handling and storage, and ensuring cameras don't capture private areas. A copy of CCTV Privacy Notice is available at Appendix 6.

14.2. The following key compliance steps are in place:

- Clearly state why we have installed CCTV, such as deterring crime or improving safety.
- Visible signage in place to inform everyone that they are entering a CCTV-monitored area.
- Ensure that cameras only capture the necessary area.
- Positioned cameras to focus solely on the car park and avoid capturing private areas like residents' windows or homes.
- Secure and managed footage where recordings are stored securely and access is only granted to authorised individuals. We delete footage when it's no longer needed or after a maximum of one month, unless required for a dispute.
- A regular maintenance regime must be set up to ensure that the system continues to produce high quality images and regular checks must be carried out to ensure that the date and time stamp record on the images is accurate.
- Complete a DPIA before installing CCTV.

14.3. Data protection law does not prescribe any specific maximum or minimum retention periods for CCTV systems or footage, but images should not be kept for longer than is necessary. The timeframe for keeping images will be set on the equipment.

14.4. On occasion it may be necessary to keep images for a longer period, for example where they are being used by a law enforcement body investigating a crime.

- Ring doors bells are permitted in our homes, with the following conditions:
  The tenant is data controller.
- Should comply with legislation/ICO guidance.
- Tenant is responsible for system and data protection obligations that arise as a result.
- Approval must be given by the Housing Officer and recorded in writing before installation.
- Any breaches of installation and subsequent use may result in a tenancy breach.

14.5. A CCTV code of practice is available from the Information Commissioner's Office website: www.ico.gov.uk.

15. Data Protection Impact Assessments ("DPIAs")

15.1. These are a means of assisting the Association in identifying and reducing the risks that our operations have on personal privacy of data subjects. Completion of the DPIA will be supported by the Data Protection Officer (DPO) and the staff member who is leading on the procurement process.

15.2. 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.

15.3. In the event that a processor intended to process personal data on behalf of CVHA outside the UK, CVHA would need to follow these steps before making a decision:

- Complete a DPIA to establish whether CVHA needs to make the transfer of personal data in order to meet their purposes
- If it does, consider whether there are UK "adequacy regulations" about the country or territory where the processor is located. If not, then a Transfer Risk Assessment must be completed the purpose is to ensure that CVHA satisfied that for the data subjects of the transferred data the relevant protections under the UK data protection regime will not be undermined.

15.4. 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 DPIA, they require to notify the DPO within five (5) working days.

16. Roles and Responsibilities

16.1. This section defines who is responsible for implementation and oversight to ensure accountability. The core roles and responsibilities pertaining to this Policy are outlined in the table below:

Role	Responsibility
Board	Responsible for approving this Data Protection Policy and ensuring it aligns with the organisation's strategic objectives.
Audit Committee	Will receive and scrutinise quarterly reports.
Executive Management Team	Ensure that adequate resources are allocated for the implementation and maintenance of data protection measures. Responsible for identifying and managing data protection risks across the Group.
Finance and Corporate Services Director	Will manage and support the Data Protection Officer to ensure accountability of all aspects of the Data Protection Policy.
Data Protection Officer (DPO)	Will manage all aspects of data protection law in line with the Data Protection Policy and will ensure that all staff are trained and supported as outlined in 7.1. Our Data Protection Officer has over-arching responsibility and oversight over compliance by the Association with data protection law. The role is filled by the Association's Senior Governance and Compliance Officer, whose details are noted on the Association's website and contained within the Privacy Notice at Appendix 2a The DPO will be responsible for: • Monitoring the Association's compliance with data protection law and this Data Protection Policy. • Overseeing the implementation of this Data Protection Policy and ensuring compliance with applicable data protection laws,

Role	Responsibility
	• Providing guidance and advice to the organisation and its employees on data protection matters. • Developing and delivering data protection training and awareness programs to employees. • Co-operating with and serving as the Association's contact point for communication with the ICO and managing any data protection-related inquiries or investigations. • Managing and responding to data breaches, including notifying relevant authorities and affected individuals as required by law. • Reporting breaches or suspected breaches to the ICO and data subjects in accordance with clause 10.4 of this Data Protection Policy.
IT Team	Responsible for implementing and maintaining technical security measures to protect personal data against unauthorised access, loss, or destruction. Monitoring systems for potential security breaches and ensure that appropriate measures are in place to detect and respond to incidents. Ensure that data back up and recovery procedures are in place and regularly tested to prevent data loss.
People Team	Managing employee personal data in compliance with this Data Protection Policy and applicable data protection laws. Collaborating with the DPO to ensure that all employees receive regular data protection training and are aware of their responsibilities. Ensure that employees are informed of their privacy rights and how to exercise them.
Staff	Have responsibility to that they adhere to this Data Protection Policy and any related procedures. They must follow data protection best practices, including secure handling and storage of personal data and responding to requests in timescales provided and defined by law. Are required to report any data protection incidents or breaches to the DPO immediately.
Third Party Service Providers	Third party service providers that process personal data on behalf of the Association must comply with this Data Protection Policy and applicable data protection laws. Third party service providers must enter into Data Processing Agreements (DPAs) with the Association, outlining their data protection obligations. Third party service providers must implement appropriate technical and organisational measures to protect personal data.

17. Legal and Regulatory Framework

17.1. It is a legal requirement that the Association processes data correctly; the Association must collect, handle and store information in accordance with the relevant legislation.

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

- the General Data Protection Regulation (EU) 2016/679 as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time) (the "UK GDPR");
- Data Protection Act 2018;
- Data (Use and Access) Act 2025
- Privacy and Electronic Communications (EC Directive) Regulations 2003

17.3. The UK GDPR principles state that personal data must be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must 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;

e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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.

17.4. These rights are notified to the Association's tenants and other customers in more detail in the Association's Privacy Notice at Appendix 2a-c.

18. Communication and Awareness

18.1. This policy is posted on the Association's website and is accessible to all. At each review of the policy there will be no formal awareness training unless significant amendments have been made to policy which will be communicated to staff and stakeholders within 30 days of approval.

19. Risk Management

19.1. Effective risk management is essential to ensure the protection of personal data and compliance with data protection laws. The Association will manage any identified risks through its Risk Management Policy ensuring that risks are identified, assessed, managed and mitigated.

19.2. Failure to adhere to this policy can result in significant risks and consequences, including:

- Legal and Regulatory Penalties – non-compliance with data protection laws, can result in substantial fines and penalties. These penalties can have a severe financial impact on the Association.
- Reputational Damage – data breaches and non-compliance with data protection laws can damage the Association's reputation. Loss of trust from customers, lenders, the Scottish Housing Regulator and contractors can lead to a decline in business performance and our ability to deliver vital services to our customers.
- Operational Disruption – data breaches and security incidents can disrupt business operations, leading to downtime, loss of productivity, and increased costs associated with incident response and recovery.
- Legal liability – non-compliance with data protection laws can result in legal liability from affected individuals. This can lead to significant legal costs and potential compensation payments.

20. Improvement, Monitoring and Review

Policy Review

20.1. This policy will be reviewed every three years or as and when changes to legislation or best practice guidance necessitate it. The purpose of the review is to access the policy's effectiveness and adherence to current legislation and good practice and identify any changes which may be required. Any amendments to the policy will be communicated to staff and stakeholders within 30 days of approval.

Internal Assurance

20.2. A formal system of monitoring all aspects of this policy has been established and is maintained with properly defined reporting, escalation, and action procedures. Regular reports will be generated and reviewed by the leadership team to track compliance and identify any potential risks or issues.

20.3. The monitoring system will include quarterly reports that are presented to our Audit Committee for oversight and monitoring.

20.4. The Head of Assurance conduct regular internal reviews to assess compliance with this policy and applicable data protection laws. These reviews will evaluate the effectiveness of data protection measures, identify areas for improvement, and ensure that any non-compliance issues are promptly addressed.

20.5. A robust incident management process is in place to handle data breaches and other security incidents. This process will include procedures for identifying, reporting, and responding to incidents, as well as measures to mitigate the impact and prevent future occurrences.

Audit and Performance Reporting

20.6. The following audit and performance reporting measures are in place:

- Quarterly reports will be prepared and issued to Audit Committee.
- Annual reports will be prepared and issued to CVHA Board as part of the Annual Audit Committee Report.

- Breaches that have been submitted to the ICO will be reported to the CVHA Chair and Board, with regular updates.
- Breaches that have been submitted to the ICO will be reported to the Scottish Housing Regulator (SHR) via a Notifiable Event. The Notifiable Event Log is managed by the Corporate Services Team.

External Quality Assurance

20.7. To ensure the highest standards of data protection and compliance with applicable laws, the Association engages in external quality assurance activities. These activities provide an independent evaluation of our data protection practices and help identify areas for improvement. The key components of our external quality assurance include:

- Third Party Audits – the Association will engage an independent third-party internal auditor to complete an internal audit of our data protection practices every three years. These audits will assess compliance with data protection laws, , and evaluate the effectiveness of our data protection measures. The findings and recommendations from these audits will be used to enhance our data protection mitigations.
- Penetration Testing – to ensure the security of our systems and data, the Association will engage external security experts to conduct regular penetration testing. These tests will identify vulnerabilities in our systems and help us implement measures to mitigate potential security risks.
- Benchmarking – we will participate in benchmarking exercises to compare our data protection practices with those of other organisations in our sector. This will help us identify best practices and areas for improvement, ensuring that we remain at the forefront of data protection.

21.8 By engaging in these external quality assurance activities, the Association ensures that our data protection practices are independently evaluated and continuously improved. This commitment to external quality assurance helps to protect personal data, maintain regulatory compliance, and build trust with our stakeholders.

21. Training and Competency

21.1. To ensure that all employees understand their responsibilities under this policy and are equipped to handle personal data appropriately, the Association has established a robust programme of training. This includes the following:

- Induction training – all new employees will receive mandatory data protection training as part of their induction programme. This training will cover the principles of data protection, the requirements of data protection law and the specific responsibilities of employees under this policy.
- Ongoing training – regular data protection training sessions will be provided to all employees to ensure they remain informed about the latest data protection practices and regulatory requirements. These sessions will include updates on any changes to data protection laws, as well as refresher courses to reinforce key concepts.
- Role specific training – employees with specific roles that involve handling personal data such as those in the IT, People and Corporate Service Teams will receive additional training tailored to their responsibilities. This training will cover advanced topics such as data security measures, incident response, and data subject rights.
- Competency Assessments – to ensure that employees have a thorough understanding of data protection principles and practices, regular competency assessments will be conducted. These assessments may include practical exercises, and scenario-based evaluations to test employee's knowledge and skills.
- Awareness Campaigns – in addition to formal training, the Association will conduct regular awareness campaigns to promote a culture of data protection across the Group. These campaigns may include SharePoint posts, blogs, posters, and other communications to remind employees of their data protection responsibilities and to highlight best practice.

21.2. A high level summary of the training and delivery method are outlined in the table below:

Staff Group	Training/Awareness Required	Method
New Staff	Introduction to GDPR	eLearning
All Staff	Monthly Mimecast session	eLearning
All Staff	Annual GDPR session	In person

Training Records

21.3. The Association's People Team will maintain records of all data protection training sessions both existing and new members of staff. These records will include details of the training provided, the employees who attended, and the results of any assessments. This documentation will be used to track compliance with training requirements and to identify any areas where additional training may be needed.

22. Key References and Supporting Documents

22.1. This policy is supported by a range of internal and external documents that provide further clarification, procedures and guidance.

22.2. This policy should be read in conjunction with the following Policies:

- IT Policies and Procedures.
- Code of Conduct.
- Board Code of Conduct.
- Staff Code of Conduct.

Supporting Documents

22.3. Supporting documents include related policies, procedures, operational standards and guidelines that inform compliance and implementation. This policy should be read in conjunction with the Association's:

- Table of Duration of Retention of certain Data – Appendix 1.
- Privacy Notice – Tenants – Appendix 2A.
- Privacy Notice – Owners – Appendix 2B
- Staff Privacy Notice – Appendix 3A.
- Board Privacy Notice – Appendix 3B.
- Privacy Notice – CCTV – Appendix 4
- Contractor GDPR Addendum – Appendix 5
- Model Sharing Agreement – Appendix 6.
- Model Data Processor Addendum – Appendix 7.
- Data Protection Impact Assessment (DPIA) Template: this document provides a structured approach for assessment of the potential impact of data processing activities on the privacy of individuals. It includes guidelines for identifying and mitigating risks associated with data processing. A copy of this assessment will be provided by Corporate Service Department.
- Business Continuity Plan: this document details the procedures for responding to data breaches and other security/business interruption incidents. It includes steps for identifying, reporting, and mitigating incidents, as well as notifying affected individuals and relevant authorities. A copy of this plan is available on request from Corporate Services Team.
- Privacy Notice: this notice provides clear and transparent information to individuals about how their personal data is collected, used and protected by the Association. It includes details on data subject rights and how to exercise them.

Key References

22.4. Key references include applicable legislation, regulatory requirements and standards:

- the General Data Protection Regulation (EU) 2016/679 ("the UK GDPR");
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- the Privacy and Electronic Communications (EC Directive) Regulations 2003

23. General Data Protection Regulations

23.1. The Association treat personal data in line with our obligations under the current data protection regulations and our own Data Protection Policy. Information regarding how data will be used and the basis for processing data is provided in the Association's Privacy Notices outlined at Appendices 2a-c.

24. Equality, Diversity and Inclusion

24.1. At the Association we value people and their diversity and strive to be inclusive. We respect others, regardless of personal differences and we listen to people to understand their needs and tailor our service accordingly. We will strive to promote equal access to our service for all members of the community and provide fair and equal treatment, promoting human rights in line with our Equality, Diversity and Inclusion Policy.

25. Approval and Review History

Version	Author of Change	Changes	Approved by	Date Approved
1	**L Hughes**	**New Policy**	**Board**	

26. List of Appendices

Appendix 1 Data Retention Schedule
Appendix 2a Fair Privacy Notice (Tenants)
Appendix 2b Privacy Notice (Owner)
Appendix 3a Staff Privacy Notice
Appendix 3b Board Privacy Notice
Appendix 4 CCTV Privacy Notice
Appendix 5 Contractor GDPR Addendum
Appendix 6 Model Data Sharing Agreement
Appendix 7 Model Data Protection Addendum

Appendix 1 - Data Retention Schedule

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
Governance	
Register of Members and Share Certificates	Permanent
AGM Minutes	Permanent
Register of Board Members	5 years after cessation of membership
Certificate of incorporation	Permanent
Memorandum and Articles of Association	Permanent
Confirmation letter of charitable registration	Permanent
HMRC confirmation of chartable status	Permanent
Certificate of registration with the housing regulator	Permanent
Notices of meetings (incl. AGMs)	6 years in case of challenge to validity of meeting.
Complaints records	5 years (from final reply)
Registrations and Statutory Returns	
Annual returns to the regulator	5 years
Audited company returns and financial statements	Permanent
Declarations of interest	6 years (limitation for legal proceedings)
Strategic Management	
Business plans and supporting documentation (e.g. structures, aims, objectives, etc.)	5 years after business
Insurances	
Current and former policies	Permanent
Annual insurance schedule	6 years
Indemnities and guarantees	6 years after expiry
Claims and related correspondence	2 years after settlement
HR Records	
Personnel files including training records and notes of disciplinary and grievance hearings.	7 years after employment ends
Redundancy details, calculations of payments, refunds, notification to the Secretary of State.	7 years after employment ends
Application forms, interview notes.	6 months after interview date. Successful applicant documents should be transferred to personal file.
Documents proving the right to work in the UK.	7 years after employment ends.
Facts relating to redundancies.	7 years after employment ends if less than 20 redundancies. 12 years after employment ends if 20 or more redundancies.
Individual training records	7 years after employment ends.
Retirement benefits schemes – notifiable events, e.g., relating to incapacity.	7 years from end of the scheme year in which the event took place.

Type of record	Retention time
Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence.	7 years after employment ends.
Parental leave.	18 years.
Finance , Accounting and Tax Records	
Financial records – including purchase and sales ledgers, cash, VAT, journals	7 years after year end.
Cheque books, pay-in books	7 years after year end.
Bank statements and reconciliations	7 years after year end.
Payroll.	7 years after year end.
VAT records and VAT related correspondence	7 years after year end.
Copy invoices	7 years after year end.
Instructions to bank	7 years after year end.
Income tax, NI returns, correspondence with tax office.	7 years after year end.
Pension records.	7 years after year end.
Statutory Sick Pay records, calculations, certificates, self-certificates.	7 years after year end.
Wages/salary records, expenses, bonuses.	7 years after year end.
Records relating to working time.	7 years after year end.
Social Housing Grant documentation	Permanent
Budgets and internal financial reports	2 years
Fixed Asset Register	Permanent
Employees: Tax and Social Security	
Record of taxable payments	6 years
Record of tax deducted or refunded	6 years
Records of earnings on which standard National Insurance Contributions payable	6 years
Copies of notices to employee (e.g. P45, P60)	6 years plus current year.
Expense claims	6 years
Income tax PAYE and NI returns	6 years
Contracts and Agreements	
Contracts under Seal and/or executed as deeds	12 years after project completion and incl. defects liability period.
Contracts for the supply of goods and services	6 years after contract end (including any defects liability period).
Loan agreements	12 years after last payment.
Licensing, rental and hire purchase agreements	6 years after expiry.
Indemnities and guarantees	6 years after expiry.
Documents relating to successful tenders.	6 years after contract end.
Documents relating to unsuccessful tenders.	2 years after notification.
Forms of tender	6 years.
Health and Safety	
Accident books and records and reports of accidents.	6 years after date of occurrence (limitation for legal proceedings).
Health and safety assessments and records of consultations with safety representatives and committee.	Permanently.
Health and Safety policy statements	Permanently.
Health records.	During employment and 3 years thereafter if reason for termination of employment is connected to health.
Sickness records	6 years from end of sickness.

Type of record	Retention time
Customers	
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.
Current tenant files including application form, tenancy agreement, housing benefit notifications, tenancy management details.	Duration of tenancy.
Housing Benefit notifications	2 years.
Rent statements	2 years
Former tenants' files (key information).	3 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.
Rent payment records	7 years after year end.
ASB case files.	5 years/end of legal action.
Property Records	
Lease of property from/to another agency/organisation	3 years after end of lease.
Property maintenance records – general repairs, planned/cyclical maintenance, major repairs, improvements.	Permanent (or until no longer used/owned).
Property maintenance records – annual/statutory safety or maintenance checks	3 years
Planning and building control permissions	12 years after interest ceases.
Reports and professional opinions	6 years

Appendix 2a - Privacy Notice (Tenant)

Privacy 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 Limited ("CVHA") are a Scottish Charity (Scottish Charity Number SC037244), a Registered Social Landlord and having their registered office at 50 Scott Street, Motherwell, ML1 1PN. We own or manage around 5,000 homes and support over 8,000 customers across Lanarkshire and East Dunbartonshire.

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, private owners, and mid-market and market rent property tenants is processed by Clyde Valley Property Services Limited through its three subsidiaries:

1. Clyde Valley Lets Limited (for mid-market and market rent property tenants and owners).
2. Clyde Valley Factoring (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. All of the above CVHA group companies are 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 UK General Data Protection Regulation and all other relevant data protection laws.

Our Data Protection Officer is our Senior Governance and Compliance Officer, Lisa Hughes. Any questions relating to this notice and our privacy practices should be sent to Lisa Hughes at lisa.hughes@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 into a factoring agreement with us, or where you provide us with your personal details.
- 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 and former address.
- Telephone number.
- E-mail address.
- Date of birth
- National Insurance Number.
- Personal characteristics such as gender, ethnic group, disabilities.
- Next of kin.
- Marital status.
- Power of attorney/guardian and their contact details.
- Communication and language preferences.
- Care and support needs, including GP/health records.
- Vulnerabilities.
- Nationality.
- Financial information including bank account details.
- Tenancy reference number.
- Tenancy management information.
- Arrears and payment arrangements.
- Relationship with Board members and employees.
- Information required to assess applications.
- 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.
- Information from the NHS or Social Work.
- Information from the Department for Work and Pensions.
- Payments made by you to us.
- Utilities providers.
- 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 made.
- 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 your relationship with us.
- ensure that appropriate privacy policies are in place advising staff and others how and why their data is being processed.
- 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,.
- 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 Data Protection 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 Data Protection 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 authorities).
- if we are investigating payments made or otherwise, your information may be disclosed to payment processors, local authorities and the Department of Work and Pensions.
- if we raise 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 this information will be collected anonymously.
- when you make a payment through our third-party payment provider, your information will be shared with it.

- if we are providing support with your income and benefit entitlement, we may share your information with the relevant organisations and agencies (such as the Citizens Advice Bureau, Money Matters, and other debt and advice agencies) with your consent.
- We will share your information at your request through power of attorney/guardianship or a signed written agreement.
- We will share your information where required with our regulators, including the Scottish Housing Regulator.
- 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) with your consent
- 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.

We may also share personal information with our professional and legal advisors for the purposes of taking advice, as well as our auditors where required.

Unless required to do so by law, 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.

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:

- to be informed of the personal data we hold on you;
- you have a right to request access to the personal information that we hold about you by making a "subject access request";
- if you believe that any of your personal information is inaccurate or incomplete, you have a right to request that we correct or complete your personal information;
- object to the processing of your personal information for specific purposes;
- you have a right to request that we restrict the processing of your personal information for specific purposes;
- ask us for the personal information that we hold about you to reuse it for your own purpose; and
- if you wish us to delete your personal information, you may request that we do so

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

8. Why we need your personal information – special categories of personal data and criminal offence data

Certain personal information we collect is treated as special categories of personal data to which additional protections apply under data protection law. Where we process special categories of personal data or criminal offence data, we will do so under the following conditions:

- for reasons of substantial public interest, including to exercise a function conferred on us by an enactment or rule of law, to prevent or detect unlawful acts, to protect the public against dishonesty, to provide support for individuals with a particularly disability or medical condition and respond to requests from elected representatives;
- in relation to information relating to criminal offences or convictions, to protect individuals' vital interests and for the purposes of legal claims.

We use your personal information relating to your age, marital status, gender, sexuality, ethnicity, religion, disability for equality monitoring purposes and to make reasonable adjustments as required by the Equality Act 2010.
We will process such personal information to identify and keep under review the existence or absence of equality of opportunity or treatment between groups of people within the same categories to promote or maintain equality within the Association.

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 Data Protection 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: https://ico.org.uk/make-a-complaint/.

6th floor
Quartermile One
15 Lauriston Place
Edinburgh
EH3 9EP.
Telephone Number: 0303 123 1115
Email: 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.

Appendix 2b - Privacy Notice (Owner)

Privacy 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 Limited ("CVHA") are a Scottish Charity (Scottish Charity Number SC037244), a Registered Social Landlord and having their registered office at 50 Scott Street, Motherwell, ML1 1PN. We own or manage around 5,000 homes and support over 8,000 customers across Lanarkshire and East Dunbartonshire.

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 factored owners and, private owners, is processed by Clyde Valley Property Services Limited through its three subsidiaries:

1. Clyde Valley Lets Limited (for mid-market and market rent property tenants and owners).
2. Clyde Valley Factoring (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. All of the above CVHA group companies are 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 UK General Data Protection Regulation and all other relevant data protection laws.

Our Data Protection Officer is our Senior Governance and Compliance Officer, Lisa Hughes. Any questions relating to this notice and our privacy practices should be sent to Lisa Hughes at lisa.hughes@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 into a factoring agreement with us, or where you provide us with your personal details.
- 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.
- 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:

- Payments made by you to us.
- Utilities providers.
- 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 our relationship with you.
- 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,.
- 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 Data Protection 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 Data Protection 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, this may also apply to landlords of properties that we rent for them
- 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, your information will be shared with it.
- if we are providing support with your income and benefit entitlement, we may share your information with the relevant organisations and agencies (such as the Citizens Advice Bureau, Money Matters, and other debt and advice agencies).
- We will share your information at your request through power of attorney/guardianship or a signed written agreement.
- We will share your information where required with our regulators, including the Scottish Housing Regulator.
- We will disclose your final account to third parties (sellers' and purchasers' solicitors).
- 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. Details of security measures that are in place can be found in our Data Protection Policy. This can be viewed on our website at www.cvha.org.uk.

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 have been disclosed or which will be disclosed.
- the retention periods.
- 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.

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:

6th floor
Quartermile One
15 Lauriston Place
Edinburgh
EH3 9EP.
Telephone Number: 0303 123 1115
Email: 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

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. Who are we?

Clyde Valley Housing Association Limited ("CVHA") are a Scottish Charity (Scottish Charity Number SC037244), a Registered Social Landlord and having their registered office at 50 Scott Street, Motherwell, ML1 1PN. We own or manage around 5,000 homes and support over 8,000 customers across Lanarkshire and East Dunbartonshire.

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 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. All of the above CVHA group companies are 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 UK General Data Protection Regulation, the Data (Use and Access) Act 2025 and all other relevant data protection laws.

Our Data Protection Officer is our Senior Governance and Compliance Officer, Lisa Hughes. Any questions relating to this notice and our privacy practices should be sent to Lisa Hughes at lisa.hughes@cvha.org.uk.

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

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:

- Name.
- Date of Birth.
- Address.
- Telephone Number.
- E-mail address.
- National Insurance number.
- Personal characteristics such as marital status, gender and ethnic group.

- Medical or health information relevant to your employment.
- Details of your qualifications, skills, experience and work history including start and end dates with previous employers and workplaces.
- Details of your work pattern (days and hours) and attendance at work.
- Next of Kin / dependents / emergency contact details.
- GP's details.
- Information about your remuneration, including entitlement to benefits such as pay, pension and holidays.
- Bank Account details.
- Passport, driving licence or other identification documents.
- PVG or disclosure details.
- GP medical requests/letters of health-related appointments.
- Information about your nationality and entitlement to work in the UK.
- Employment References.
- Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence.
- Assessments of your performance, including performance reviews and related correspondence.
- General correspondence relating to your employment.
- Vehicle details including business insurance.
- Information about any criminal convictions if this is relevant to your job; and
- Details of periods of leave taken by you, including annual leave, sickness absence, family leave and sabbaticals.

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

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

- Administration of contracts of employment in line with our Terms and Conditions of Employment.
- Payment of salaries.
- Recruitment and selection.
- Pensions and associated benefits, appraisal, training and development.
- Membership of professional bodies.
- Provision of ID cards.
- Scottish Housing Regulator annual return.
- PVG and Disclosure checks.

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.

- to obtain checks regarding your right to work in the UK.
- to deduct tax, National Insurance, and administrate your pension.
- to comply with health and safety laws.
- to enable you to take periods of leave to which you are entitled.
- 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:

- Racial or ethnic origin.
- Religious or philosophical beliefs.

- Political opinion.
- Trade union membership.
- Genetic or biometric data.
- Data concerning health. or
- Data concerning sex life or sexual orientation

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:

- Run recruitment processes.
- Maintain accurate and up to date employment records, contact details, emergency contact details, and records of employee contractual statutory rights.
- Operate and keep a record of disciplinary and grievance processes.
- Plan for career development, succession planning and workforce planning.
- 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.
- Obtain occupational health advice, ensuring that it complies with duties in relation to individuals with disabilities and meets requirements under health and safety law.
- Operate and keep a record of other leave you may take including maternity, paternity, adoption, parental and shared parental leave.
- Ensure effective general HR and business administration.
- Provide references on request for current or past employees.
- Respond to and defend against legal claims.
- In the event of a business sale/transfer.
- Criminal Offence has been committed.

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 our relationship with you
- 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.
- 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 Data Protection 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 Data Protection 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

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:

- To assist in the recruitment process of staff members.
- To allow your pension provider to process pensions information and handle your pension.
- To allow your electronic payslips to be produced and issued to you.
- To obtain employment law advice.
- To HMRC, DWP and other third-party agencies; and
- 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.

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. We hold a copy of your personnel file electronically. Access is restricted to the organisation's HR function and line managers. Please see our Data Protection Policy for further details on our security arrangements. The Data Protection Policy can be found in the HR Policy manual.

7. 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.

Data retention guidelines on the information we hold are provided in our Data Protection Policy.

8. 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:

- to be informed of the personal data we hold on you;
- you have a right to request access to the personal information that we hold about you by making a "subject access request";
- if you believe that any of your personal information is inaccurate or incomplete, you have a right to request that we correct or complete your personal information;
- object to the processing of your personal information for specific purposes;
- you have a right to request that we restrict the processing of your personal information for specific purposes;
- ask us for the personal information that we hold about you to reuse it for your own purpose;
- and if you wish us to delete your personal information, you may request that we do so

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.

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:

Information Commissioner's Office (ICO) who regulates data protection across the UK:

6th floor
Quartermile One
15 Lauriston Place
Edinburgh
EH3 9EP.
Telephone Number: 0303 123 1115
Email: 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 personal and contact details.

Appendix 3b - Privacy Notice (Board)

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. Who are we?

Clyde Valley Housing Association Limited ("CVHA") are a Scottish Charity (Scottish Charity Number SC037244), a Registered Social Landlord and having their registered office at 50 Scott Street, Motherwell, ML1 1PN. We own or manage around 5,000 homes and support over 8,000 customers across Lanarkshire and East Dunbartonshire

The personal data of CVHA and Clyde Valley Property Services' ("CVPS") Board Members is processed by Clyde Valley Housing Association Limited.

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. We are registered with the Information Commissioner's Office as a data controller.

Our Data Protection Officer is our Senior Governance and Compliance Officer, Lisa Hughes. Any questions relating to this notice and our privacy practices should be sent to Lisa Hughes at lisa.hughes@cvha.org.uk.

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

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:

- Name.
- Address.
- Date of Birth.
- Telephone Number.
- E-mail address.
- Personal characteristics such as gender, racial and ethnic origin, data concerning health.
- Details from your CV and Board Member Application form.
- Qualifications and professional experience.
- Passport, driving licence or other identification documents.
- Bank details.

- Photographs.
- Information about your nationality.
- Assessments of your performance, including performance reviews and related correspondence.
- 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. Why we need this information about you and how it will be used

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:

- Administration of our governance and regulatory requirements.
- Board Member recruitment and selection.
- Administration of Board related processes, meetings and events.
- Appraisal, training and development.
- Membership of professional bodies.
- Regulatory compliance to meet the requirements of the Scottish Housing Regulator, the Office of the Scottish Charity Regulator including annual returns.
- Annual returns and information required by Companies House (applies to CVPS members only).
- Payment of Board Member expenses and remuneration.

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.

- to comply with health and safety laws; and
- 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 includes any data that reveals:

- Racial or ethnic origin.
- Data concerning health.

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

- To assist in the recruitment process of Board Members.
- Maintain accurate and up to date governance records and contact details.
- Operate and keep a record of governance processes.
- Plan for development, succession planning and board planning.
- 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.
- Ensure effective general and business administration.
- Provide references on request for current or past Board Member.
- Respond to and defend against legal claims.
- Complete a business sale/transfer; and
- To ensure ongoing regulatory and statutory compliance.

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 our relationship with you.
- All processing complies with law.

We will ensure that all staff who handle personal data on our behalf are aware of their responsibilities under our Data Protection 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

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:

- To assist in the recruitment process of board members.
- To publicise the work of the Board on CVHA's website and other publications.
- To comply with audit and procurement procedures.
- 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.
- In order to comply with regulatory requirements.

We will share your information with third parties where we are legally obliged to do so. We may also share your information without professional advisers when required.

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. We hold a copy of your personnel file electronically. Access is restricted to the organisation's corporate function and Chief Executive. Please see our Data Protection Policy for further details on our security arrangements. The Data Protection Policy can be found in the Board Packs.

7. 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 or as set out in any relevant contract we have with you. Data retention guidelines on the information we hold are provided in our Data Protection Policy.

8. 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 have been disclosed or which will be disclosed.
- the retention periods.
- 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.

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:

6th floor
Quartermile One
15 Lauriston Place
Edinburgh
EH3 9EP.
Telephone Number: 0303 123 1115
Email: 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 personal and contact details.

Appendix 4 - Privacy Notice (CCTV)

GUIDANCE FOR STAFF

Residential car park CCTV Scotland -

In Scotland, the use of CCTV in residential car parks is governed by UK data protection law, which includes the UK General Data Protection Regulation (UK GDPR) ,the Data Protection Act 2018 and the Data (Use and Access) Act 2025. These laws apply when a CCTV system captures images of people outside the user's private property, such as in a communal area like a shared car park.

Rules for using CCTV in communal car parks
For CCTV covering a shared residential car park, the person or organisation responsible for the system is considered a "data controller" and must follow these rules:

- Have a valid reason: There must be a clear and legitimate reason for the surveillance, such as protecting the property or preventing crime.
- Be transparent: Visible signs must be displayed to inform people that CCTV is in operation. The signs should state the purpose of the recording and include contact details for the data controller.
- Limit coverage: Cameras should be positioned to minimise intrusion into private spaces, such as pointing away from neighbours' windows. Privacy masks or blockers can be used to blur out unnecessary areas.
- Minimise audio recording: As audio recording is more intrusive, it is generally discouraged unless strictly necessary.
- Store data securely: Recorded footage must be stored securely to prevent unauthorised access. Access should be restricted to authorised personnel.
- Retain footage for a limited time: Footage should not be kept for longer than is necessary. A common retention period is between 7 and 31 days, unless an incident requires it to be kept longer for evidence.
- Handle access requests: Individuals captured in the footage have a right to request a copy of the data. The data controller must respond to a Subject Access Request (SAR) within one calendar month.

What to do if you have concerns
If you have a concern about CCTV system that covers a communal car park or residential , the provides guidance on how to address it. ICO CCTV Guidance

- Talk to your neighbour: The ICO recommends speaking to the CCTV owner first to explain your concerns and see if a resolution can be reached, such as repositioning the camera.
- Write a letter: If a discussion is not successful, you can use the ICO's template letter to formally request information and explain your data protection rights.
- Contact other parties: If you are in social housing, you can report the problem to your housing officer. If you rent privately you can contact the landlord.

CCTV privacy notice is required when a camera records beyond the user's private property, such as a communal residential car park. The notice must be clearly visible and accessible to anyone entering the monitored area.

CLYDE VALLEY HOUSING ASSOCIATION

CCTV Privacy Notice

This notice is to inform you that CCTV is in operation in and around the <<Name of car park or property>> residential car park. This is for the purpose of [*insert purpose* e.g. ensuring the security of the property and for the prevention and detection of crime].

Identity of the data controller

Name: _____

Name of organisation: _____

Address: _____

Phone: _____

Email: _____

Purpose of the CCTV system

The CCTV system is in operation for the following specific and legitimate purposes:

Examples may be

- ***[To prevent and deter criminal activity, including theft and vandalism.***
- ***To protect the property and vehicles of residents and their visitors.***
- ***To assist law enforcement with investigations where a crime has occurred.***]

Lawful basis for processing

The lawful basis for processing personal data via this CCTV system is [*insert appropriate legal basis – for example legitimate interest. We have carried out a balancing test and have determined that our interest in protecting property and ensuring safety outweighs the privacy rights of those recorded*].

Who will we share your information with?

We will only share your information with third parties where we are legally entitled to do so or where we are legally obliged to do so. This may include Police Scotland and HSE.

Data security

We will ensure that the images are stored securely and none of the images will be transferred outside the UK.

Data minimisation

The CCTV system is designed to capture only what is necessary for the stated purposes. The cameras are positioned to avoid, as far as is reasonably possible, overlooking neighbouring private properties or other public areas beyond the communal car park.

Audio recording is /is [not] enabled on this system.

Data retention

Images from the CCTV system are automatically and securely stored for a period of X days. They may be kept longer if we have a legitimate reason to do for example

- In response to a request from law enforcement agencies, such as Police Scotland, to investigate an incident.
- In response to a valid legal request or court order.
- When responding to a Subject Access Request from an individual.

Your data protection rights

Under data protection law, individuals have the right to request access to CCTV footage of themselves. To make a Subject Access Request (SAR), you must contact the data controller named above. When making a request, you should provide sufficient information, such as the date and time of the incident, to enable us to locate the relevant footage.

You also have the right to object to the processing of your data, or to request its deletion, where there is no legitimate reason for it to be kept.

Concerns or complaints

If you have any concerns about the use of CCTV, please contact the data controller using the details provided above.

If you remain dissatisfied, you can lodge a complaint with the Information Commissioner's Office (ICO):

Website: https://ico.org.uk/make-a-complaint/

Phone: 0303 123 1113

Appendix 5 - Contractor GDPR Addendum

CLYDE VALLEY HOUSING ASSOCIATION

DATA PROCESSOR – GDPR REQUIREMENTS

1. In this Addendum, the following terms shall have the following meanings:

   a. "Contractor" means [INSERT NAME OF CONTRACTOR);

   b. "controller", "data protection impact assessment", "data subject", "Commissioner", "personal data", "process" (including any derivatives thereof), "processor", "and "special categories of personal data" shall each have the same meaning as defined in the Data Protection Laws; and

   c. "Data Protection Laws" means the General Data Protection Regulation (EU) 2016/679 as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time), the Data Protection Act 2018, the Data (Use and Access) Act 2025 and all applicable laws relating to processing of personal data and privacy.

2. In providing services to Clyde Valley HA, the Contractor shall process such categories of personal data (including special categories of personal data) in relation to such categories of data subjects for and on behalf of Clyde Valley HA as shall be strictly necessary for the provision of the services by the Contractor to Clyde Valley HA and to perform and discharge the Contractor's obligations under this Addendum.

3. Clyde Valley HA shall be the controller and the Contractor shall be the processor of all personal data that the Contractor processes in providing services to Clyde Valley HA. The Contractor shall comply with the Data Protection Laws relating to the processing of personal data in providing services to Clyde Valley HA.

4. The Contractor shall only process, the personal data in accordance with this Addendum and Clyde Valley HA's written instructions from time to time, except where otherwise required by applicable law Data Protection Legislation(and shall inform Clyde Valley HA of that legal requirement in such case before processing, unless applicable law prevents it from doing so on important grounds of public interest).

5. The Contractor shall not transfer the personal data outside the United Kingdom without Clyde Valley HA's prior written consent.

6. The Contractor shall at all times (at its own cost and expense) implement and maintain appropriate technical and organisational measures to protect the personal data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access.

7. The Contractor shall not permit the processing of the personal data by any subcontractor without the prior specific written authorisation of that subcontractor by Clyde Valley HA and only then subject to such conditions as Clyde Valley HA may require. Prior to the subcontractor processing the personal data, the Contractor must ensure that the subcontractor enters into a written agreement (to be approved by Clyde Valley HA in advance) imposing on the subcontractor the same obligations as are imposed on the

Contractor under this Addendum and that the subcontractor complies with all such obligations. The Contractor shall remain fully liable to Clyde Valley HA under this Addendum for all the acts and omissions of the subcontractor as if they were its own.

8. The Contractor shall ensure that all persons authorised by the Contractor or any subcontractor to process the personal data are:

   a. reliable and adequately trained in the Data Protection Laws;

   b. informed of the confidential nature of the personal data and that they must not disclose the personal data to any unauthorised party; and

   c. subject to a binding and enforceable written contractual obligation to keep the personal data confidential.

9. The Contractor shall (at its own cost and expense) promptly:

   a. provide such information and assistance (including by taking all appropriate technical and organisational measures) as Clyde Valley HA may require in relation to the fulfilment of Clyde Valley HA's obligations under the Data Protection Laws to respond to requests exercising data subjects' rights;

   b. provide such information, co-operation and other assistance to Clyde Valley HA as Clyde Valley HA requires to ensure compliance with Clyde Valley HA's obligations under the Data Protection Laws, including in relation to: security of processing of the personal data; data protection impact assessments; prior consultation with the Commissioner (or other supervisory authority) regarding high risk processing; and any remedial action and / or notifications to be made or taken in response to any breach, complaint or request regarding either the Contractor's or Clyde Valley HA's obligations under the Data Protection Laws relevant to this Addendum;

   c. record and refer all requests and communications received from data subjects or the Commissioner (or other supervisory authority) to Clyde Valley HA which relate to the personal data and shall not respond to any such requests and communications without Clyde Valley HA's express written approval and strictly in accordance with Clyde Valley HA's instructions;

   d. and (in any case) within 24 (Twenty Four) hours, notify Clyde Valley HA if it or any subcontractor suspects or becomes aware of any suspected, actual or threatened occurrence of any breach of the Data Protection Laws in respect of any personal data and shall provide all information and assistance to Clyde Valley HA as Clyde Valley HA requires to report the breach to the Commissioner (or other supervisory authority) and to notify affected data subjects under the Data Protection Laws; and

   e. make available (and shall ensure that all subcontractors make available) to Clyde Valley HA such information as is required to demonstrate the Contractor's and the subcontractor's compliance with their respective obligations under this Addendum and the Data Protection Laws, and allow for, permit and contribute to audits, including inspections by Clyde Valley HA (or an auditor appointed by Clyde Valley HA) for this purpose at Clyde Valley HA's request from time to time.

10. The Contractor shall (and shall ensure that each of its subcontractors and employees shall) immediately, at Clyde Valley HA's request, either securely delete or securely return all the personal data to Clyde Valley HA in such form as Clyde Valley HA requests after the earlier of:

    a. the termination of the provision of services by the Contractor to Clyde Valley HA; or

b. once processing of the personal data by the Contractor is no longer required for the performance of the Contractor's relevant obligations under this Addendum,

and securely delete existing copies of the personal data (except to the extent that the Contractor is required to retain the personal data by applicable law, in which case, the Contractor shall inform Clyde Valley HA of any such requirement).

11. The Contractor shall indemnify and keep Clyde Valley HA indemnified against all losses, claims, damages, liabilities, fines, interest, penalties, costs, charges, sanctions, expenses, compensation paid to data subjects, demands and legal and other professional costs (calculated on a full indemnity basis and, in each case, whether or not arising from any investigation by, or imposed by, the Commissioner (or other supervisory authority) arising out of or in connection with any breach by the Contractor of its obligations under this Addendum and all amounts paid or payable by Clyde Valley HA to a third party which would not have been paid or payable if the Contractor's breach of this Addendum had not occurred.

Subscribed for and on behalf of [INSERT NAME OF CONTRACTOR] by:

Name:	
Signature:	
At:	
Date:	**day of 2025**
Witness by:	
Name:	
Signature:	
Address:	

Appendix 6 - Data Sharing Agreement

CLYDE VALLEY HOUSING ASSOCIATION

DATA SHARING AGREEMENT

between

1. **CLYDE VALLEY HOUSING ASSOCIATION LIMITED**, a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 2489RS, a Scottish Charity with Scottish Charity Number SC037244 and having its registered office at 50 Scott Street, Motherwell, ML1 1PN (hereinafter referred to as **"CVHA"**);

and

2. **«Contractor_»**, a company incorporated under the Companies Acts and having its registered office/main office at «Partner_Address» (hereinafter referred to as the "Service Provider").

WHEREAS

(A) CVHA has engaged the services of the Service Provider for the Purpose and in the course of this engagement, CVHA may share the Data of [its tenants and factored owners] with the Service Provider in terms of the tender and/or contractor; **[Drafting Note: Amend if no overarching services agreement.]**

(B) The Parties intend that this Agreement will form the basis of the data sharing arrangements between them;

(C) The intention of the Parties is that they shall each be independent Controllers in respect of the Data that they process under this Agreement; and

(D) Nothing in this Agreement shall alter, supersede, or in any other way affect the terms of the agreement between CVHA and the Service Provider for the provision of the Services in terms of[tender and/or contract UK,] unless this would result in either Party breaching its obligations under Data Protection Law. **[Drafting Note: Delete if no overarching services agreement.]**

NOW THEREFORE IT IS AGREED AS FOLLOWS:

1 DEFINITIONS AND INTERPRETATION

1.1 In construing this Agreement, capitalised words and expressions shall have the meanings set out in this Clause 1.1:

"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 in Scotland;

"Controller", **"Personal Data"**, **"Personal Data Breach"**, "**Commissioner**" **"Process"** (including any derivatives thereof) and **"Special Categories of Personal Data"** have the meanings set out in Data Protection Law;

"Data" means the information which contains Personal Data and Special Categories of Personal Data described in Part 1 of the Schedule;

"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 2018;

(b) the UK GDPR;

(c) the Data (Use and Access) Act 2025;
(d) the Privacy and Electronic Communications (EC Directive) Regulations 2003 and
(e) any other Law relating to the Processing, privacy and/or use of Personal Data;

"Data Recipient" means the Party (being either CVHA or the Service Provider, as appropriate) to whom Data is disclosed;

"Data Subject" means any identified or identifiable living individual to whom any Data relates and the categories of Data Subjects within the scope of this Agreement are listed in Part 1 of the Schedule;

"Data Subject Request" means a written request received by either Party as 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 CVHA or the Service Provider, as appropriate) disclosing Data to the Data Recipient;

"UK GDPR" means the General Data Protection Regulation (EU) 2016/679 as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time);

"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;

"Party" means a party to this Agreement, and **"Parties"** shall be construed accordingly;

"Purpose" means the purpose referred to in Part 2 of the Schedule

"Representatives" means, as the context requires, the representative of CVHA and/or the representative of the Service Provider 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 2.4.6; and

"Services/Contract" has the meaning given in recital (A) of this

1.1.1 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 Data Protection Law

1.1.2 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;

1.1.3 any words following the terms including, include, in particular, for example or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms;

1.1.4 a reference to writing or written includes email; and

1.1.5 any obligation on a Party not to do something includes an obligation not to allow that thing to be done.

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 under the Data Protection Law.

Parties Relationship

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

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

2.4.2 it is responsible for complying with the obligations incumbent on it as a 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 three (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.

Mutual Assistance

2.7 Each Party shall assist the other in complying with all applicable requirements of Data Protection Law and in particular each Party shall:

2.7.1 consult with the other Party about any notices given to Data Subjects in relation to the Data;

2.7.2 promptly (and at the latest within seven (7) days of receipt) inform the other Party about the receipt of any Data Subject Request;

2.7.3 provide the other Party with reasonable assistance in complying with any Data Subject Request;

2.7.4 not disclose or release any Data in response to a Data Subject Request without first consulting the other Party wherever possible; and

2.7.5 assist the other Party, at the cost of the other party, in responding to any Data Subject Request and in ensuring compliance with its obligations under the Data Protection Law with respect to security, breach notifications, impact assessments and consultations with the Commissioner or any other supervisory authority or regulator.

Records

2.8 The Receiving Party shall maintain complete, accurate and up to date written records of all of its Processing of the Data as necessary to demonstrate its compliance with this Agreement.

3 BREACH NOTIFICATION

3.1 Each Party shall, promptly (and, in any event, no later than twelve (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 Personal Data Breach affecting the Data. Such notification shall specify (at a minimum):

3.1.1 the nature of the breach (including a Personal Data Breach) or suspected breach;

3.1.2 the date and time of the breach;

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 reasonable 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 until the expiration (or earlier termination) of the main agreement between CVHA and the Service Provider for the provision of the Services, unless terminated earlier by the Disclosing Party in accordance with Clause 4.5. **[Drafting Note: Amend if no overarching services agreement.]**

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 (including a Personal Data Breach); or

4.3.2 the Commissioner or any of his or her authorised staff recommends that this 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 4.5, 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;

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 shall indemnify and keep indemnified 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 reasonable 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.

5.3 Subject to Clauses 5.1 and 5.2 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 6.2, 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 13.1.

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 email, the date and time of the email receipt.

8 NO PARTNERSHIP OR AGENCY

8.1 Nothing in this agreement is intended to, or shall be deemed to, establish any partnership or joint venture between the Parties, constitute any Party the agent of another Party or authorise any Party to make or enter into any commitments for or on behalf of any other Party.

8.2 Each Party confirms it is acting on its own behalf and not for the benefit of any other person.

9 VARIATION

9.1 No variation of this Agreement shall be effective unless it is in writing and signed by the Parties (or their authorised representatives).

10 ASSIGNATION

10.1 Neither Party shall be entitled to assign, transfer, mortgage, charge, sub-contract, declare a trust over or deal in any other manner with any of its rights and obligations under this Agreement.

11 NO WAIVER OF REMEDIES OR RIGHTS

11.1 No failure or delay by a Party to exercise any right or remedy provided under this Agreement or by Law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy.

12 INVALIDITY, ILLEGALITY AND UNENFORCEABLITY

12.1 If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this Clause shall not affect the validity and enforceability of the rest of this Agreement.

13 GOVERNING LAW

13.1 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 9 pages together with the Schedule in 6 Parts hereto are executed by the Parties hereto as follows:

On behalf of **Clyde Valley Housing Association Limited**
At 50 Scott Street
Motherwell
ML1 1PN

on

by

Print Full Name

before this witness

Print Full Name Witness

Address
At 50 Scott Street
Motherwell
ML1 1PN

On behalf of «**Contractor**_»

at

on

by

Print Full Name

before this witness

Print Full Name Witness

Address

THIS IS THE SCHEDULE REFERRED TO IN THE FOREGOING DATA SHARING AGREEMENT BETWEEN THE CVHA AND THE SERVICE PROVIDER

SCHEDULE PART 1 – DATA

DATA SUBJECTS

For the purposes of this Agreement, Data Subjects include tenants and factored owners of CVHA or its subsidiaries, the Data of whom is transferred between the Parties under this Agreement. The Data may include a Data Subject's:

- name;
- address;
- telephone number;
- e-mail address;

SCHEDULE PART 2: PURPOSE

Purpose

The Parties are exchanging Data to allow the Service Provider to provide <<insert service being provided>> in relation to properties of tenants and factored owners of CVHA and its subsidiaries.

SCHEDULE PART 3 - DATA TRANSFER RULES

Information exchange can only work properly in practice if it is provided in a format which the Data Recipient can utilise. It is also important that the Data is disclosed in a manner which ensures that no unauthorised reading, copying, altering or deleting of the Data occurs during electronic transmission or transportation of the Data. The Parties therefore agree that to the extent that data is physically transported, the following media are used:

- Face to face;
- Secure email;
- Courier; and
- Encrypted removable media.

SCHEDULE PART 4 – REPRESENTATIVES

Contact Details

CVHA

Name:	Lisa Hughes
Job Title:	Data Protection Officer
Address:	50 Scott Street, Motherwell, ML1 1PN
E-mail:	lisa.hughes@cvha.org.uk
Telephone Number:	01698 268855

Service Provider

Name:	
Job Title:	
Address:	
E-mail:	
Telephone Number:	

SCHEDULE PART 5 – SECURITY MEASURES

1 The Parties shall each implement an organisational information security policy.

2 Physical Security

2.1 Any use of data processing systems by unauthorised persons must be prevented by means of appropriate technical (keyword / password protection) and organisational (user master record) access controls regarding user identification and authentication. Any hacking into the systems by unauthorised persons must be prevented. Specifically, the following technical and organisational measures are in place:

The unauthorised use of IT systems is prevented by:

- User ID;
- Password assignment;
- Lock screen with password activation
- Each authorised user has a private password known only to themselves
- Regular prompts for password amendments.

The following additional measures are taken to ensure the security of any Data:

- Network Username;
- Network Password;
- Application Username;
- Application Password.

3 Disposal of Assets

3.1 Where information supplied by a Party no longer requires to be retained, any devices containing Personal Data should be physically destroyed or the information on such devices should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

4 Malicious software and viruses

Each Party must ensure that:

4.1.1 PCs used in supporting the service are supplied with anti-virus software and anti-virus and security updates are promptly applied.

4.1.2 All files received by one Party from the other are scanned to ensure that no viruses are passed.

4.1.3 The Parties must notify each other of any virus infections that could affect their systems on Data transfer.

SCHEDULE PART 6 – DATA GOVERNANCE

Data accuracy

The Disclosing Party shall make reasonable efforts to ensure that Data provided to the Data Recipient is accurate, up-to-date and relevant.

In the event that any information, in excess of information reasonably required in order to allow both organisations to comply with their obligations, is shared, the Data Recipient will notify the other party immediately and arrange the secure return of the information and secure destruction of any copies of that information.

Data retention and deletion rules

The Parties shall independently determine what is appropriate in terms of their own requirements for data retention.

Both Parties acknowledge that Data that is no longer required by either organisation will be securely removed from its systems and any printed copies securely destroyed.

Appendix 7 - Data Processing Agreement

Data Processing Agreement

DATA PROTECTION ADDENDUM

between

Clyde Valley Housing Association, a Scottish Charity (Scottish Charity Number SC037244, a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 2489RS and having its Registered Office at 50 Scott Street Motherwell (the "**Association**")

and

XXXX, registered in terms of the Companies Acts with registered number **XXXX** and having its registered office at **XXXXX** (the "**Processor**")

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

WHEREAS

(a) The Association and the Processor have entered into an agreement/ contract to supply **XXXXXXX** (hereinafter the "Principal Agreement");

(b) This Data Protection Addendum forms part of the Principal Agreement; and

(c) 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 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 any statute, directive, other legislation, law or regulation in whatever form, delegated act (under any of the foregoing), rule or other binding restriction, decision or guidance in force from time to time ;

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;

1.1.3 "**Contracted Processor**" means Processor or a Subprocessor;

1.1.4 "**Data Protection Laws**" means, to the extent applicable, the data protection or privacy laws applicable to either Party in connection with the Principal Agreement:

1.1.4.1 the GDPR;

1.1.4.2 the Data Protection Act 2018;

1.1.4.3 Data (Use and Access) Act 2025

1.1.4.4 the Privacy and Electronic Communications (EC Directive) Regulations 2003; and

1.1.4.5 any other Applicable Laws relating to the Processing, privacy and/or use of Personal Data;

1.1.5 "**GDPR**" means General Data Protection Regulation (EU) 2016/679 as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time);

1.1.6 "**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;

1.1.7 "**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; and

1.2 The terms, "**Commissioner", "Controller", "Data Subject", "Personal Data", "Personal Data Breach"** and **"Processing**" 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 each Subprocessor) not to transfer the Association Personal Data to any country outside the UK without the prior written approval of the Association, such approval may be subject to and given on such terms as the Association may in its absolute discretion prescribe.

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 organisational 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

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;
and

5.4.3 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 the Commissioner, 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 This Addendum 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. The Parties agree that the Scottish Courts shall have exclusive jurisdiction in relation to any Dispute.

Order of precedence

11.2 Nothing in this Addendum reduces the Processor's obligations under the Principal Agreement 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.

11.3 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.

Changes in Data Protection Laws, etc.

11.4 The Association may:

11.4.1 by giving at least twenty eight (28) days' written notice to the Processor, from time to time 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

11.5 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 50 Scott Street, Motherwell, ML1 1PN

on

by

Print Full Name	Director/Secretary/Authorised Signatory

before this witness

Print Full Name	Witness - Corporate Services Officer

Address
50 Scott Street Motherwell, ML1 1PN

On behalf of **XXXX**
at <insert address>

on

by

<INSERT NAME> Print Full Name	Director/Secretary/Authorised Signatory

before this witness

<INSERT NAME> Print Full Name	