



"Offering our community more than a home"

Data Protection Policy

SMT Review date:	28 April 2026
Last Approved:	29 November 2022
Approved:	(Oct 2026 MC report)
Review date:	April 2029

- CHA Objectives:**
- To manage the houses provided, in a professional and cost effective manner, for the benefit of our local community and the environment.
 - To ensure that our resources are adequate to deliver our objectives by investing in our people, demonstrating value for money and through robust procurement practices.
 - To promote social inclusion by applying principles of equality and diversity to everything we do.

- Regulatory Standards:**
- The governing body leads and directs the RSL to achieve good outcomes for its tenants and other service users.
 - The RSL is open about and accountable for what it does. It understands and takes account of the needs and priorities of its tenants, service users and stakeholders. And its primary focus is the sustainable achievement of these priorities.
 - The RSL manages its resources to ensure its financial well-being, while maintaining rents at a level that tenants can afford to pay.
 - The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation's purpose.

If you have difficulty with reading this policy, including any difficulties with sight or hearing, or if you require this document translated into another language, please contact us and we will be happy to provide this information in a format that suits your needs.

Clydebank Housing Association Limited

Data Protection Policy

Contents

1. Introduction	p4
2. Legislation	p4
3. Freedom of Information	p5
4. Data	p5
5. Lawful Basis for Processing of Data	p5
6. Data Sharing	p7
7. Data Storage and Security	p8
8. Breaches	p9
9. Data Protection Officer	p10
10. Data Subject Rights	p10
11. Data Protection Impact Assessments	p12
12. Archiving, Retention and Destruction of Data	p12
13. Staff Training	p12
Complaints handling	p13
Appendix 1 - Data Protection Impact Assessment Template	p14
Appendix 2 - Standard Data Processing Agreement	p21

Glossary of Key Terms

The following is a glossary of key terms, which Committee members and staff should be familiar with to execute this policy, they include:

1. Information Commissioner's Office (ICO) – Responsible for enforcing legislation. The Association requires submitting an annual notification to the ICO detailing the systems containing data and how the data is used. We are also required to notify the ICO of any changes to the register within 28 days.
2. Data Controller - The organisation that determines the purposes for which and manner in which personal data is used, in our case, the Association.
3. Data Subject – a living individual who is the subject of personal data e.g., tenant, employee, committee member, suppliers, applicant, complainant, etc.
4. Personal data is defined as, data relating to a living individual who can be identified from that data and other information. which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.
5. Relevant Filing System - Any set of information relating to individuals and structured, either by reference to the individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily available.
6. Processing – obtaining, recording or holding data or carrying out any operation on data, including disclosure and destruction.
7. Data breach - A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

1. Introduction

Clydebank Housing Association (hereinafter the “Association”) is committed to ensuring the secure and safe management of data held by the Association in relation to customers, staff and other individuals. The Association’s staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals’ data in accordance with the procedures outlined in this policy and documentation referred to herein.

The Association needs to gather and use certain information about individuals. These can include customers (tenants, factored owners etc.), employees and other individuals that the Association has a relationship with. The Association manages a significant amount of data, from a variety of sources. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the General Data Protection Regulations - GDPR).

This Policy sets out the Association’s duties in processing that data, and the purpose of this Policy is to set out the procedures for the management and protection of personal data.

2. Legislation

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

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

- (a) The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).
- (b) The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications. customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.
- (c) The Freedom of Information (Scotland) Act 2002 (FOISA) is an Act of the Scottish Parliament which gives everyone the right to ask for any information held by Scottish public authorities.
- (d) The Environmental Information Regulations 2004 provide public access to environmental information held by public authorities.
- (e) Any future legislation relating to data protection, the processing of personal data that replaces current legislation, or is enacted into UK law.

3. Freedom of Information (FOI) and Environmental Information

The Freedom of Information Act gives everyone the right to ask to see recorded information from the Association including paper, computer files, and video with exception of personal information that is covered by GDPR. It also excludes commercially sensitive information and information that might prejudice the safety or security of Clydebank Housing Association.

The Association recognises its 3 mandatory duties under FOI as follows: -

- Duty to publish information
- Duty to respond to requests
- Duty to advise and assist

In order to meet its duties, the Association will publish its Guide to Information via its website and will adhere to the provisions as detailed in its Model Publication Framework (SFHA/GWSF Open All Hours Guide).

4. Data

4.1 The Association holds a variety of Data relating to individuals, including customers and employees (also referred to as data subjects) which is known as Personal Data. The Personal Data held and processed by the Association is detailed within the Fair Processing Notices held on the Clydebank Housing website.

4.1.1 “Personal Data” is that from which a living individual can be identified either by that data alone or in conjunction with other data held by the Association.

4.1.2 The Association also holds Personal data that is sensitive in nature (i.e., relates to or reveals a data subject’s racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is “Special Category Personal Data” or “Sensitive Personal Data”.

5. Lawful Basis for Processing of Personal Data

5.1 At least one of these must apply whenever you process personal data:

- Processing 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 in the public interest and is a recognised pre-approved Legitimate interests.

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the Association's official authority; or
- Processing is necessary for the purposes of legitimate interests.

5.2 Fair Processing Notice

5.2.1 The Association has produced a Fair Processing Notice (FPN) which it is required to provide to all customers and employees whose Personal data is held by the Association. That FPN must be provided to the customer from the outset of processing their Personal Data and they should be advised of the terms of the FPN when it is provided to them.

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

5.2.3 All FPNS are available on the CHA Website within the data protection section.

5.3 Employees

5.3.1 Employee Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data is held and processed by the Association. Details of the data held, and processing of that data is contained within the Fair Processing Notice – Job Applicants which is provided to Employees at the same time as their Contract of Employment.

5.3.2 A copy of any employee's Personal Data held by the Association is available upon written request by that employee from the Association's Chief Executive.

5.4 Consent

Consent as a ground of processing will require to be used from time to time by the Association when processing Personal Data. It should be used by the Association where no other alternative ground for processing is available. In the event that the Association requires obtaining consent to process a data subject's Personal Data, it shall obtain that consent in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained by the Association must be for a specific and defined purpose (i.e., general consent cannot be sought).

The Specific Consent Form GDPR is available on our website under the data protection section.

5.5 Processing of Special Category Personal Data or Sensitive Personal Data

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

- Explicit consent.
- Employment, social security and social protection (a lawful basis is required).
- Vital interests.
- Not-for-profit bodies.
- Made public by the data subject.
- Legal claims or judicial acts.
- Reasons of substantial public interest (a lawful basis is required).
- Health or social care (a lawful basis is required).
- Public health (a lawful basis is required).
- Archiving, research and statistics (a lawful basis is required).

A Data Protection Impact Assessment (DPIA) for any type of processing which is likely to be high risk should therefore be completed (Appendix 1).

6. Data Sharing

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

6.1 Data Sharing

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

Where the Association shares in the processing of personal data with a third-party organisation (e.g., for processing of the employees' pension), it shall require the third-party organisation to enter into a Data Sharing Agreement (Appendix 2) with the Association. All signed data sharing agreements are held within CHA electronic file structure.

6.2 Data Processors

A data processor is a third-party entity that processes personal data on behalf of the Association and are frequently engaged if certain of the Association's work is outsourced (e.g. Maintenance and repair works, IT support, etc.).

A Data processor must comply with Data Protection laws. The Association's data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify the Association if a data breach is suffered.

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

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 Processing Agreement (Appendix 2)

7. Data Storage and Security

All Personal Data held by the Association must be stored securely, whether electronically or in paper format in accordance with the Association's ICT Policy.

7.1 Paper Storage

If Personal Data is stored on paper, it should be kept in a secure place where unauthorised personnel cannot access it. Employees should make sure that no Personal Data is left where unauthorised personnel can access it. When the Personal Data is no longer required it must be disposed of by the employee so as to ensure its destruction. If the Personal Data requires to be retained on a physical file then the employee should ensure that it is affixed to the file which is then stored.

7.2 Electronic Storage

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

8. Breaches

The GDPR introduces a duty on the Association to report certain types of personal data breach to the relevant supervisory authority. This must be done within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay.

Failing to notify a breach when required to do so can result in a maximum fine of £8.7 million or 2 per cent of our annual turnover. The fine can be combined with the ICO's other corrective powers. We will therefore ensure we have robust breach detection, investigation and internal reporting procedures in place to facilitate decision-making about whether or not we need to notify the relevant supervisory authority and the affected individuals.

We will also keep a record of any personal data breaches, regardless of whether we are required to notify.

A data breach can occur at any point when handling Personal Data and the Association has reporting duties in the event of a data breach or potential breach occurring. A data security breach can happen for a number of reasons including e.g., theft or loss of computer hardware and paper files, inappropriate access controls allowing unauthorised use, human error, malicious attacks, contractor computer compromised, etc. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported to the ICO.

8.1 Internal Reporting

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

- As soon as the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the Data Processing Officer must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s).
- The Association must seek to contain the breach by whatever means available.
- The DPO must consider whether the breach is one which requires to be reported to the Information Commissioners Office (ICO) and data subjects affected and do so in accordance with this clause 7.
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

- Update the Breach Register with details of any breach/suspected breach

8.2 Reporting to the ICO

The DPO will require to report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the ICO within 72 hours of the breach occurring. The DPO must also consider whether it is appropriate to notify those data subjects affected by the breach.

9. Data Protection Officer (“DPO”)

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

The DPO will be responsible for:

- Monitoring the Association’s compliance with Data Protection laws and this Policy.
- Co-operating with and serving as the Association’s contact for discussions with the ICO
- Reporting breaches or suspected breaches to the ICO and data subjects.

10. Data Subject Rights

Certain rights are provided to data subjects under the GDPR. Data Subjects are entitled to view the personal data held about them by the Association, whether in written or electronic form.

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

10.1 Subject Access Requests

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

- must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law.
- where the personal data comprises, data relating to other data subjects, must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the Subject Access Request, or
- 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.

10.2 The Right to be Forgotten

A data subject can exercise their right to be forgotten by submitting a request in writing to the Association seeking that the Association erase the data subject's Personal Data in its entirety.

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

10.3 The Right to Restrict or Object to Processing

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.

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.

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

11. Data Protection Impact Assessments (DPIA)

These are a means of assisting the Association in identifying and reducing the risks that our operations have on personal privacy of data subjects (see Appendix 1 DPIA Template). The Association shall:

Carry out a DIA 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.

Consult with 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.

12. Archiving, Retention and Destruction of Data

The Association cannot store and retain Personal Data indefinitely. It must ensure that Personal data is only retained for the period necessary. The Association shall ensure that all Personal data is archived and destroyed in accordance with the periods specified within the Data Retention Schedule.

Destruction will take place via deletion from computer network (including archived files), internal shredding and the use of an external shredding company holding appropriate data security guarantees. Shredding and destruction of data will take place under the express guidance, supervision and authority of appropriate departmental managers in accordance with the Data Retention Schedule.

The Data Retention Schedule is available from the Clydebank Housing Website under the data protection section. Deletion of computer data is regularly monitored through CPTRAX software on a weekly basis.

13. Staff Training

All staff undergo ongoing data protection awareness training with support from the ICT and Compliance Officer. Specific role training will be provided regularly to everyone who has access to personal data, to ensure they understand their responsibilities when handling data. This includes awareness training during induction for new staff members.

14. Complaints

The requirements for data protection complaints handling are:

1. Complaints e-mailed to dataprotection@cldyebank-ha.org.uk.
2. Complaints procedure is specified in the Fair Processing notice.
3. Complaints acknowledged within 30 days of receipt.
4. A Notification of the outcome will be sent without undue delay.

Equality and Human Rights

We will not discriminate on the grounds of Age, Disability, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion or Belief, Sex, and Sexual Orientation. An Equality Impact Assessment has been carried out and none of these protected groups will be unduly affected by this Policy. The Policy applies to all.

The Association will provide equality of opportunity and fair treatment for all, ensuring that no individual or group is treated less favourably than anyone else. We work closely with community stakeholders, to provide assurance that we are achieving these aims.

The Association will meet, and where appropriate exceed our obligations under the Equality Act 2010, including the general equality duty in the Act, to ensure we do not discriminate against, harass or victimise a person because they have one or more of the nine protected characteristics described in the Act.

An Equality Impact Assessment has been carried out as part of the review of this policy, in order to assess where the aims of this policy may have a positive, negative or neutral impact upon any of the nine Protected Characteristics set out in the Equality Act 2010.

Review

CHA undertakes to review this policy regularly, at least every three years after the initial first year review, with regard to:

- Applicable legislation, rules, regulations and guidance
- Changes in the organisation
- Continued best practice

For Office Use Only – Required Actions

Customer Consultation Required/Arranged	No
Intranet Update	Yes
F Drive Update	Yes
Website Update	No
Leaflet change required?	No
Newsletter Promotion?	No
Other information updated, e.g. posters, automatic email responses, post cards, answering machine messages, etc.	No
Equality Impact Assessment completed	Yes

APPENDIX 1 Data Protection Impact Assessment Template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the [Criteria for an acceptable DPIA](#) set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summaries why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion

Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix 2 Standard Data Processing Agreement



Clydebank Housing Association – Standard Data Processing Agreement

Clydebank Housing Association (CHA) and the parties to whom this document has been sent (the “Partner”) have one or more written agreements (collectively, “the Agreements”) pursuant to which the Partner provides services to Clydebank Housing Association (collectively, the “Services”) that may entail the Processing of Personal Data (as defined below).

The UK GDPR sits alongside an amended version of the Data Protection Act 2018 and imposes specific obligations on Clydebank Housing Association and other companies (controllers) with regard to their vendor relationships. The UK GDPR requires companies to conduct appropriate due diligence on processors and to have contracts containing specific provisions relating to data protection.

Each of the Agreements contains provisions requiring each party to comply with all applicable laws. This Agreement documents the data protection requirements imposed upon the parties by the UK GDPR. This document is hereby incorporated by reference into each Agreement in order to demonstrate the parties’ compliance with The Data Protection Act 2018 and UK GDPR.

PROCESSING CONDITIONS

1 General compliance obligations

- 1.1 Each party will comply with all applicable requirements of the Data Protection Laws. The obligations in this Data Processing Agreement are in addition to, and do not relieve, remove or replace, a party’s obligations or rights under the Data Protection Laws.
- 1.2 In connection with the processing described in the Processing Details, CHA is the Controller and the Partner is the Processor. The Processing Details set out the subject matter, nature and purpose of processing by the Partner, the duration of the processing and the types of Personal Data and categories of Data Subject.
- 1.3 The Partner shall, in relation to any Personal Data processed in connection with the performance by the Partner of its obligations under the Agreements:
 - (a) Process Personal Data only on and in accordance with written instructions of CHA, including with regard to transfers of Personal Data to a third country or international organisations, unless the Partner is required to process Personal Data by applicable law in which case the Partner shall inform CHA in writing of that legal requirement before undertaking the processing required by applicable law, unless applicable law prohibits the Partner from notifying CHA on important grounds of public interest;
 - (b) promptly comply with any instruction from CHA requiring the Partner to amend, transfer, delete or otherwise process (or cease the processing of) Personal Data, or to stop, mitigate or remedy any unauthorised processing;
 - (c) maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless CHA or this Data Processing Agreement specifically authorises the disclosure, or as required by law. If a law, court, regulator or Supervisory Authority requires the Partner to process or disclose Personal Data, the Partner must first inform CHA of the legal or regulatory requirement and give CHA an opportunity to object or challenge the requirement, unless the law prohibits such notice;
 - (d) ensure that persons who have access to and/or process the Personal Data are obliged to keep the Personal Data confidential;

- (e) take all measures required pursuant to
- (f) not appoint another Processor without the prior written consent of CHA (which consent may be provided in the Processing Details in respect of the Approved Sub-processors);
- (g) taking into account the nature of the processing, assist CHA by appropriate technical and organisational measures for the fulfilment of CHA's obligation to respond to requests for exercising Data Subjects' rights laid down in Chapter III (*Rights of the Data Subject*) of The UK GDPR;
- (h) assist CHA in ensuring CHA's compliance with its obligations under Data Protection Laws, including the obligations set out in the UK Data Protection Act 2018 and the UK GDPR, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with a Supervisory Authority under Data Protection Laws;
- (i) at the choice of CHA, delete or return to CHA all Personal Data when the processing described in the Processing Details comes to an end and delete existing copies unless applicable law requires storage of the Personal Data (in which case the Partner shall notify CHA in writing of that storage requirement) and in which case in accordance with the terms of this Data Processing Agreement;
- (j) provide to CHA all information necessary to demonstrate the Partner's compliance with the obligations of this Data Processing Agreement and allow for and contribute to audits, including inspections, conducted by CHA or another auditor mandated by CHA; and
- (k) immediately inform CHA if, in its opinion, an instruction from CHA infringes Data Protection Laws.

3 Security of processing

- 3.1 The Partner shall ensure that it has in place appropriate technical and organisational measures, to protect against unauthorised or unlawful processing of Personal Data processed in connection with the performance by the Partner of its obligations under the Agreements and against accidental loss or destruction of, or damage to, Personal Data processed in connection with the performance by the Partner of its obligations under the Agreements, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of the art, the cost of implementing any measures and the nature, scope, context and purposes of processing as well as the risk and varying likelihood and severity for the rights and freedoms of natural persons, (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it).
- 3.2 Without prejudice to clause 3.1, the Partner shall have in place the security measures outlined in the Processing Details.

4 General Obligations

- 4.1 The Partner shall:
 - (a) ensure that only those personnel who need to have access to the Personal Data processed in connection with the performance by the Partner of its obligations under the Agreements are granted access to such Personal Data (and only for the purposes set out in the Processing Details) and that such personnel accessing the Personal Data:
 - (i) are reliable and have been trained in how to handle and Process Personal Data;
 - (ii) have been informed of the confidential nature of the Personal Data processed in connection with the performance by the Partner of its obligations under the Agreements;
 - (iii) are aware of both the Partner's duties and their personal duties and obligations under the Data Protection Laws and this Data Processing Agreement; and
 - (b) notify CHA within three (3) days if it receives:

- (i) a request from a Data Subject to access Personal Data or to exercise any other rights under Data Protection Laws;
- (ii) any communication from a Supervisory Authority in relation to the processing of the Personal Data; or
- (iii) a complaint from a Data Subject

and the Partner will give CHA its full co-operation and assistance in responding to any complaint, notice, communication or request.

5 Appointment of Sub-processors

- 5.1 The Partner must not appoint a sub-processor (which is not already an Approved Sub-Processor provided in the Processing Details) in connection with their obligations under the Agreements unless the specific prior written consent of CHA has been obtained.
- 5.2 The sub-Processor shall also comply with the requirements for sub-processing that the data protection obligations set forth herein and as may otherwise be agreed by the Processor in this Agreements.
- 5.3 The Partner must enter into a written contract with the Sub-Processor that contains terms substantially the same as those set out in this Data Processing Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon CHA's written request, provide CHA with copies of the relevant excerpts from such contracts.

6 Personal Data Breaches

- 6.1 The Partner shall notify CHA in writing without undue delay (and, in any event, no later than within 6 hours) on becoming aware of an actual or suspected Personal Data Breach impacting Personal Data being processed by the Partner in connection with the Agreements and provide CHA with such details as CHA reasonably requests in respect of the same.
- 6.2 Without prejudice to the foregoing generality, the Partner shall provide CHA in writing with:
 - (a) a description of the nature of the actual or suspected Personal Data Breach impacting Personal Data being processed by the Partner in connection with the Agreements including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
 - (b) the name and contact details of the data protection officer or other contact point of the Partner where more information can be obtained;
 - (c) a description of the likely consequences of the actual or suspected Personal Data Breach impacting Personal Data being processed by the Partner in connection with the Agreements; and
 - (d) a description of the measures taken or proposed to be taken by the Partner to address the actual or suspected Personal Data Breach impacting Personal Data being processed by the Partner in connection with the Agreements, including, where appropriate, measures to mitigate possible adverse effects.
- 6.3 Immediately following a Personal Data Breach impacting Personal Data being processed by the Partner in connection with the Agreements, the parties will co-ordinate with each other to investigate the matter. The Partner will reasonably co-operate with CHA, including:
 - (a) assist with any investigation;

- (b) make available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Laws or as otherwise reasonably required by CHA; and
 - (c) take reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach.
- 6.4 The Partner will not inform any third party of any actual or suspected Personal Data Breach impacting Personal Data being processed by the Partner in connection with the Agreements without first obtaining CHA's prior written consent, except when required to do so by law.
- 6.5 CHA has the sole right to determine:
 - (a) whether to provide notice of the Personal Data Breach impacting Personal Data being processed by the Partner in connection with the Agreements to any Data Subjects, Supervisory Authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the discretion of CHA, including the contents and delivery method of the notice; and
 - (b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.
- 6.6 The Partner will cover all reasonable expenses associated with the performance of the obligations under clauses 6.1 to 6.3. The Partner shall restore any Personal Data at its own expense.
- 6.7 Notwithstanding Clause 10.1, the Partner will reimburse CHA for reasonable expenses incurred by CHA when responding to a Personal Data Breach impacting Personal Data being processed by the Partner in connection with the Agreements to the extent that the Partner caused such a Personal Data Breach, including all costs of notice and any remedy as set out in clause 6.5.

7 Transfers of Personal Data from the UK

- 7.1 The Partner (or any Sub-processor) must not transfer any Personal Data processed in connection with the performance by the Partner of its obligations under the Agreements outside of the UK unless the specific prior written consent of CHA has been obtained (which consent may be provided in the Processing Details).

8 Term of this Data Processing Agreement

- 8.1 This Data Processing Agreement will be deemed to come into effect on the Processing Start Date mentioned in the Processing Details (regardless of the date(s) of signing of this Data Processing Agreement).
- 8.2 This Data Processing Agreement will remain in full force and effect for so long as the Partner retains any Personal Data processed in connection with the performance by the Partner of its obligations under the Agreements in its possession or control.
- 8.3 Any provision of this Data Processing Agreement that expressly or by implication is intended to come into or continue in force on or after termination shall remain in full force and effect.
- 8.4 The termination of this Data Processing Agreement will be without prejudice to any other rights or remedies of any party under this Data Processing Agreement or at law and shall not affect any claims or rights which a party may have against the other which have accrued prior to such termination.
- 8.5 This Data Processing Agreement shall be governed and construed in accordance with Scottish law and the Scottish Courts shall have jurisdiction (except for the purposes of enforcement of a Scottish court judgment or order in another jurisdiction) with regard to all matters arising from it.

9 Notice

- 9.1 Any notices to be provided in terms of this Data Processing Agreement must be provided in writing and addressed to the relevant CHA Contact or Partner Contact as outlined in the Processing Details. Such notice must be:
 - (a) Delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or

- (b) Sent by e-mail to the CHA Contact or Partner Contact as outlined in the Processing Details (or an address substituted in writing by the party to be served).

9.2 Any notice shall be deemed to have been received:

- (a) If delivered by hand, at the time the notice is left at the proper address; or
- (b) If sent by pre-paid first-class post or other next working day delivery service, at 9:00am on the second Business Day after posting; or
- (c) If sent by e-mail, at the time of transmission, or if this time falls outside business hours in the place of receipt, when business hours resume.

10 Liability and indemnity

10.1 The Partner shall indemnify and keep CHA indemnified in full and on demand in respect of any direct or indirect losses, claims, costs, expenses, proceedings and damages incurred by CHA arising out of or in connection with any failure by the Partner (or its employees, agents or Sub-processors etc.) to comply with any of its obligations under this Data Processing Agreement or Data Protection Laws.

10.2 Nothing in this Data Processing Agreement will:

- (a) limit or exclude any liability for death or personal injury resulting from negligence; or
- (b) limit or exclude any liability for fraud or fraudulent misrepresentation; or
- (c) limit any liabilities in any way that is not permitted under applicable law; or
- (d) exclude any liabilities that may not be excluded under applicable law.

10.3 Any limitation of liability set forth in the Agreements will not apply to Clause 6.7 or this Clause 10.

PROCESSING DETAILS

Background

The partner will process Personal Data on behalf of Clydebank Housing Association for the purposes set out in these Processing Details.

This Data Processing Agreement sets out the terms on which the Partner will process Personal Data on behalf of CHA. This Data Processing Agreement consists of the below Processing Details and the Processing Conditions including the Schedule.

Parties	
CHA	Clydebank Housing Association Ltd , 77-83 Kilbowie Road, Clydebank G81 1BL, incorporated under the Co-operative and Community Benefit Societies Act 2014 and recognised as a Registered Society (Registered Number 2191RS) and a Scottish charity (Charity number SC033962)
Partner Organisation Name and Address	[INSERT PARTNER ORGANISATION], having its registered office at [], a company incorporated under the Companies Acts (Company number [])

Key processing Details	
Subject matter of the processing	<i>[Note: insert a description of the subject matter of the processing]</i>
Duration of the processing	Processing Start Date: <i>[Note: insert the processing start date. The agreement will apply from that date.]</i> Duration of processing: <i>[Note: insert the duration of the processing by the Partner. Or If no specific duration agreed, add "N/A".]</i>
The nature and purpose of the processing of Personal Data	<i>[Note: insert details on the nature and purpose of the processing.]</i>

Types of Personal Data to be processed	<i>[Note: insert the types of personal data to be processed. This may be e.g. name, contact details, medical details.]</i>
Categories of Data Subject to whom Personal Data relates	<i>[Note: insert the categories of individuals (data subjects) whose personal data will be processed. This may be e.g. Tenants, Contractors]</i>

Additional processing details	
CHA Contacts	<u>Name:</u> <i>[Note: insert CHA primary contact name]</i> <u>Position:</u> <i>[Note: insert CHA primary contact role]</i> <u>E-mail:</u> <i>[Note: insert CHA primary contact e-mail]</i> <u>Telephone:</u> <i>[Note: insert CHA primary contact phone number]</i>
Partner Contact	<u>Name:</u> <i>[Note: insert Partner contact name]</i> <u>Position:</u> <i>[Note: insert Partner contact role]</i> <u>Address:</u> <i>[Note: insert work address of contact]</i> <u>E-mail:</u> <i>[Note: insert Partner contact e-mail]</i> <u>Telephone:</u> <i>[Note: insert contact phone number]</i>
Security measures	<i>[Note: insert details of any security measures which the Partner must follow in connection with the CHA's personal data (e.g. specific access restrictions, personnel security requirements, physical or technical security requirements, etc.) If no specific measures agreed, add "N/A".]</i>
Approved Sub-Processors	Name: Address E-mail: Telephone: Company Number:

Signed for and on behalf of

Clydebank Housing Association

Authorised Signatory

by

(Insert name)

on

(Date of signing)

Signed for and on behalf of

Full name of the Partner

(Authorised Signatory

by

(Insert name)

on

(Date of signing)

This is the Schedule referred to in the foregoing Processing Conditions between Clydebank Housing Association and the Partner named in the Processing Details.

**SCHEDULE
DEFINITIONS**

"Business Day"	Means any weekday which is not a bank holiday, or other public national holiday in Scotland;
"Controller"	has the meaning given in the UK GDPR;
"Data Processing Agreement"	this data processing agreement between CHA and the Partner consisting of the Processing Details, the Processing Conditions and this Schedule;
"Data Processing Details"	means the data processing details annexed to and forming part of this Data Processing Agreement;
"Data Protection Laws"	means any law, statute, subordinate legislation regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body which relates to the protection of individuals with regard to the processing of personal data, electronic communications and privacy to which a party is subject including the Data Protection Act 2018, the UK General Data Protection Regulation (the "UK GDPR") (having the meaning given in section 3(10) (as supplemented by section 205(4) of the Data Protection Act 2018), the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) and any statutory modification or re-enactment thereof;
"Data Subject"	has the meaning given in the UK GDPR;
"parties"	CHA and the Partner, and the word "party" shall be construed accordingly;
"Personal Data"	has the meaning given in the UK GDPR;
"Personal Data Breach"	has the meaning given in the UK GDPR;
"processing"	has the meaning given in the UK GDPR;
"Processing Start Date"	means the processing start date set out in the Processing Details;
"Processor"	has the meaning given in the UK GDPR;
"Schedule"	means this Schedule annexed to and forming part of the Data Processing Agreement;
"Sub-processor"	means any person (including any third-party but excluding an employee of the Partner) appointed by or on behalf of the Partner which is engaged in the processing of Personal Data on behalf of CHA in connection with the Agreements;
"Supervisory Authority"	means the UK Information Commissioner's Office and any other supervisory authority within the meaning of the Data Protection Laws; and

Clydebank Housing Association Equality Impact Assessment Tool

The Equality Impact Assessment process aims to prevent discrimination against people who are categorised as being disadvantaged or vulnerable within society (as listed in point 4).



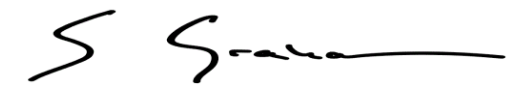
Name of the policy / proposal to be assessed	Data Protection Policy	Is this a new policy / proposal or a revision?	revision
Person(s) responsible for the assessment	Scott Graham, Lynette Lees, Joe Farrell.		
1. Briefly describe the aims, objectives and purpose of the policy / proposal	This Policy sets out the Association's duties in processing that data, and the purpose of this Policy is to set out the procedures for the management and protection of personal data.		
2. Who is intended to benefit from the policy / proposal? <i>(e.g. applicants, tenants, staff, contractors)</i>	Anyone who provides personal data to Clydebank Housing Association		
3. What outcomes are wanted from this policy / proposal ? <i>(e.g. the benefits to customers)</i>	To set out clear concise guidelines for the processing and protection of personal data by Clydebank Housing Association.		

4. Which **protected characteristics** could be **affected** by the proposal? (*tick all that apply*)

☒ Minority Ethnic ☒ Gender ☒ Disability ☒ Sexual Orientation ☒ Age ☒ Religion ☒ Transgender /Transsexual ☒ Marriage /Civil Partnership ☒ Pregnancy /Maternity

5. If the policy / proposal is not relevant to any of the **protected characteristics** listed in part 4, state why and end the process here.

6. Describe the likely positive or negative impact(s) the policy / proposal could have on the groups identified in part 4	Positive impact(s)	Negative impact(s)
	Updated with new legislation changes.	
7. What actions are required to address the impacts arising from this assessment? (<i>This might include; collecting additional data, putting monitoring in place, specific actions to mitigate negative impacts</i>).		

Signed:  (Job title): ICT and Compliance Officer

Date the Equality Impact Assessment was completed: 23/06/26

**Please save the completed document at the following location: -
F:Policies&Procedures/Equal Opportunities/Policies/Impact Assessments**