clydebank housing association

"Offering our community more than a home"

Data Protection Policy

Management Committee submission:	29 November 2022
Last Approved:	27 August 2019
Approved:	29 November 2022
Review date:	November 2025

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 provide a first class maintenance service which offers value for money and ensures the comfort and safety of our residents while achieving high levels of satisfaction
- 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.

This policy can be made available on request in a variety of different formats, such as on CD, in large print and translated into other languages.

Contents

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:

a) 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.

b) Data Controller - The organisation that determines the purposes for which and manner in which personal data is used, in our case, the Association.

c) Data Subject – a living individual who is the subject of personal data e.g., tenant, employee, committee member, suppliers, applicant, complainant, etc.

d) 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.

e) 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.

f) Processing – obtaining, recording or holding data or carrying out any operation on data, including disclosure and destruction.

g) 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 can 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 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

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

6.2 Data Sharing

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

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

6.3 Data Processors

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

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

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

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

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 drivers 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 20 million euros or 4 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.

8.1 A data breach can occur at any point when handling Personal Data and the Association has reporting duties in the event of a data breach or potential breach occurring. 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.

8.2 Internal Reporting

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

- As soon as the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the Data 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

8.3 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")

9.1. 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.

9.2 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

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

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

10.3 **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.

10.4 **The Right to be Forgotten**

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

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

10.5 **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.

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

11.1 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.

11.2 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.

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