DATA PROTECTION POLICY

Date Approved	Proposed Review Date
Oct 2019	
Chair Person/Office Bearers Signature:	

CASSILTOUN HOUSING ASSOCIATION LTD

Castlemilk Stables, 59 MACHRIE ROAD, GLASGOW G45 OAZ

Cassiltoun Housing Association is a recognised Scottish Charity SC035544

This Data Protection Policy sets out how the Cassiltoun Group handles the personal data of our customers, suppliers, employees, workers and other third parties.

This Data Protection Policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other data subject.

This Data Protection Policy applies to all Company personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when processing personal data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. You must also comply with our related policies, including our Data Retention & Disposal Policy and Data Security Policy. Any breach of this Data Protection Policy or related policies could result in disciplinary action.

This Data Protection Policy (together with related policies) is an internal document and should not be shared with third parties, clients or regulators without prior authorisation from the Data Protection Officer, David Mills (RGDP).

SCOPE OF THIS POLICY

We recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the General Data Protection Regulations ("GDPR").

All managers are responsible for ensuring their direct reports comply with this Data Protection Policy.

The Data Protection Officer is responsible for overseeing this Data Protection Policy and, as applicable, developing related policies and guidelines. That post is held by: David Mills, david@rgdp.co.uk

PERSONAL DATA PROTECTION PRINCIPLES

We adhere to the principles relating to processing of personal data set out in the GDPR which require personal data to be:

- Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**).
- Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (**Data Minimisation**).
- Accurate and where necessary kept up to date (**Accuracy**).
- Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (**Storage Limitation**).
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).
- Not transferred to another country without appropriate safeguards being in place

(**Transfer Limitation**).
- Made available to data subjects and data subjects allowed to exercise certain rights in relation to their Personal Data (**Data Subject's Rights and Requests**).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (**Accountability**).

LAWFULNESS AND FAIRNESS

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

We may only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the data subject.

The GDPR allows processing for specific purposes, some of which are set out below:

(a) the data subject has given his or her consent;
(b) the processing is necessary for the performance of a contract with the data subject;
(c) to meet our legal compliance obligations;
(d) to protect the data subject's vital interests;
(e) for the performance of a task carried out in the public interest or in the exercise of official authority;
(f) to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process personal data for legitimate interests need to be set out in applicable privacy notices.

If you are relying upon (f) "legitimate interests" as the legal basis for processing, please complete a Legitimate Interest Assessment using the **Legitimate Interest Assessment** (appendix 1)

The legal bases set out above **do not** apply to the following categories of personal data which are referred to as "special categories of personal data":

- Racial or ethnic origin
- Political opinions
- Religious/philosophical beliefs
- Health data
- Trade Union membership
- Sex life/sexual orientation
- Genetic/biometric data for identification
- Criminal convictions and alleged offences

If we are processing a special category of personal data we must have one of the following justifications:

(a) explicit consent from the data subject;
(b) for the purposes of carrying out obligations or rights in the field of employment and social security and social protection law providing for appropriate safeguards for the fundamental rights and interests of the data subject;
(c) to protect the data subject's vital interests;

(d) to pursue legitimate activities by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on the condition that the processing relates solely to the members of the body or persons with regular contact and the data is not disclosed outside that body;
(e) the personal data is manifestly made public by the data subject;
(f) it is necessary for legal claims;
(g) it is necessary for substantial public interest and measures to safeguard the rights of the data subject are provided;
(h) it is necessary for preventative or occupational medicine, for the assessment of working capacity of the employee, medical diagnosis, provision of health or social care or treatment or the managment of health or social care systems and services;
(i) necessary for public interest in public health such as protecting against serious cross-border threats to health;
(j) it is necessary for archiving in the public interest, scientific or historical research purposes or statistical purposes.

For our business, the most likely justifications for processing a special category of personal data will be (a), (b) or (c) if this scenario occurs at all.

We must identify the legal ground being relied on for each processing activity and document it in the Company's Data Processing Register / Data Map / Data Audit.

If you are unsure whether the criteria for a legal basis has been achieved, please contact the Data Protection Officer.

TRANSPARENCY (NOTIFYING DATA SUBJECTS)

The GDPR requires us to provide detailed, specific information to data subjects depending on whether the information was collected directly from them or from elsewhere. Such information must be provided through appropriate Privacy Notices that must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand them.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we must provide the data subject with all the information required by the GDPR including:
our company details as the data controller, the identity of the Data Protection Officer how and why we will use, process, disclose, protect and retain that personal data when the data subject first provides the personal data.

When personal data is collected indirectly (for example, from a third party), we must provide the data subject with all the information required by the GDPR as soon as possible after collecting/receiving the data but at the latest within one month. We must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis that contemplates our proposed processing of that personal data.
If you need support preparing a privacy notice, please contact the Data Protection Officer.

PURPOSE LIMITATION

Personal data must be collected only for specified, explicit and legitimate purposes.
We cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purposes and they have consented where necessary.

DATA MINIMISATION

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only process personal data when performing your job duties requires it. You cannot process personal data for any reason unrelated to your job duties.
You may only collect personal data that you require for your job duties: do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes.

You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's Data Retention Policy.

ACCURACY

Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We will ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

STORAGE LIMITATION

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

We must not keep personal data in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain a Data Retention & Disposal Policy to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with the Company's Data Retention & Destruction Policy.

You will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with all the Company's applicable Data Retention & Disposal policies. This includes requiring third parties to delete such data where applicable.
We will ensure data subjects are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

SECURITY INTEGRITY AND CONFIDENTIALITY

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data. You are responsible for protecting the personal

data we hold.

You must at all times comply with any relevant Data Protection Policies and follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. You may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

REPORTING A PERSONAL DATA BREACH

The GDPR requires us to notify any personal data breach to the applicable Information Commissioners Office and, in certain instances, the data subject.
If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself.

Immediately contact the Data Protection Officer. You should preserve all evidence relating to the potential personal data breach.

TRANSFER LIMITATION

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer personal data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer personal data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the data subjects' rights and freedoms;
(b) appropriate safeguards are in place such as standard approved contractual clauses, an approved code of conduct or a certification mechanism;
(c) the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or
(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject and, in some limited cases, for our legitimate interest.

DATA SUBJECT'S RIGHTS AND REQUESTS

Data subjects have rights when it comes to how we handle their personal data. These include rights to:

(a) withdraw consent to processing at any time;
(**b)** receive certain information about our processing activities;
(c) request access to their personal data that we hold;
(d) prevent our use of their personal data for direct marketing purposes;
(e) ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
(f) restrict our processing in specific circumstances;
(g) challenge our processing where we have sought to justify it on the basis of our legitimate interests or in the public interest;
(h) request a copy of an agreement under which we transfer the personal data outside of the

EEA;
(i) object to decisions based solely on automated processing, including profiling;
(j) prevent processing that is likely to cause damage or distress to the data subject or anyone else;
(k) be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
(l) make a complaint to the supervisory authority; and
(m) in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing personal data without proper authorisation).
You must immediately forward any data subject request you receive to the Data Protection Officer.

ACCOUNTABILITY

We must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

In order to demonstrate that we have adequate resources and controls in place to ensure and to document GDPR compliance we have done the following:

- appointed a Data Protection Officer to be responsible for data protection compliance;
- implemented privacy by design when processing personal data and completing Data Protection Impact Assessments where processing presents a high risk to rights and freedoms of data subjects;
- integrated data protection into internal documents including this Data Protection Policy, Data Retention & Destruction Policy, Data Security Policy and Privacy Notices;
- provided training to Company personnel on the GDPR and how to maintain a record of our data processing activities and retained a record of such training; and
- committed to regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

RECORD KEEPING

The GDPR requires us to keep full and accurate records of all our data processing activities.

You must ensure that any data processing activities that you are involved in are recorded on the Company's Data Processing Register that must be updated regularly to reflect any changes. Copies of any related data protection processing documentation including copies of consents, legitimate interest assessments and data protection impact assessments must also be included in the register.

TRAINING AND AUDIT

We are required to ensure all Company personnel have undergone adequate training to enable them to comply with data privacy laws. You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

We are required to implement Privacy by Design measures when processing personal data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that process personal data by taking into account the following:

(a) the state of the art;
(b) the cost of implementation;
(c) the nature, scope, context and purposes of processing; and
(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

We must also conduct Data Protection Impact Assessments ("DPIAs") in respect to high risk processing. You should conduct a DPIA (and discuss your findings with the Data Protection Officer when considering implementing major system or business change programs involving the processing of personal data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- automated processing including profiling and automated decision making;
- large scale processing of special categories of personal data; and
- large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- a description of the processing, its purposes and the Company's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

As a business we are not involved in any data processing activities that involve profiling or automated decision-making. If a situation arises where you believe this processing activity is necessary please contact the Data Protection Officer before implementing such activity.

DIRECT MARKETING

As a business we are not involved in any direct marketing activities. If a situation arises where you believe this processing activity is necessary please contact the Data Protection before implementing such activity.

SHARING PERSONAL DATA

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the personal data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer

complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;
(b) sharing the personal data complies with the privacy notice provided to the data subject and, if required, the data subject's consent has been obtained;
(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
(d) the transfer complies with any applicable cross border transfer restrictions; and
(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

Such data transfer must be recorded in the Company's Data Processing Register

CHANGES TO THIS DATA PROTECTION POLICY

We reserve the right to change this Data Protection Policy at any time without giving notice to you. When we do update the policy, we will endeavour to publish the updated policy as soon as practically possible.

Appendix 1

Sample LIA template

This legitimate interests assessment (LIA) template is designed to help you to decide whether or not the legitimate interests basis is likely to apply to your processing. It should be used alongside our legitimate interests guidance.

Part 1: Purpose test

You need to assess whether there is a legitimate interest behind the processing.

• Why do you want to process the data? • What benefit do you expect to get from the processing? • Do any third parties benefit from the processing? • Are there any wider public benefits to the processing? • How important are the benefits that you have identified? • What would the impact be if you couldn't go ahead with the processing? • Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)? • Are you complying with other relevant laws? • Are you complying with industry guidelines or codes of practice? • Are there any other ethical issues with the processing?

Part 2: Necessity test

You need to assess whether the processing is necessary for the purpose you have identified.

• Will this processing actually help you achieve your purpose? • Is the processing proportionate to that purpose? • Can you achieve the same purpose without the processing? • Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

Part 3: Balancing test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

First, use the DPIA screening checklist. If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail.

Nature of the personal data
• Is it special category data or criminal offence data? • Is it data which people are likely to consider particularly 'private'? • Are you processing children's data or data relating to other vulnerable people? • Is the data about people in their personal or professional capacity?
Reasonable expectations
• Do you have an existing relationship with the individual? • What's the nature of the relationship and how have you used data in the past? • Did you collect the data directly from the individual? What did you tell them at the time? • If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you? • How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations? • Is your intended purpose and method widely understood? • Are you intending to do anything new or innovative? • Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation? • Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

Likely impact
• What are the possible impacts of the processing on people? • Will individuals lose any control over the use of their personal data? • What is the likelihood and severity of any potential impact? • Are some people likely to object to the processing or find it intrusive? • Would you be happy to explain the processing to individuals? • Can you adopt any safeguards to minimise the impact?

Can you offer individuals an opt-out?	Yes / No

Making the decision

This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interests basis.

Can you rely on legitimate interests for this processing?	Yes / No
Do you have any comments to justify your answer? (optional)	

LIA completed by	
Date	

What's next?

Keep a record of this LIA, and keep it under review.

Do a DPIA if necessary.

Include details of your purposes and lawful basis for processing in your privacy information, including an outline of your legitimate interests.