DATA PROTECTION POLICY

Date Approved	Proposed Review Date
November 2021	November 2024
Chair Person/Office Bearers Signature:	

CASSILTOUN HOUSING ASSOCIATION LTD

Castlemilk Stables, 59 MACHRIE ROAD, GLASGOW G45 OAZ

This Data Protection Policy sets out how the Cassiltoun Group processes the personal data, including, but not limited to, that of our customers, suppliers, employees, workers, website users 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 processed.

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 compliancewith this Data Protection Policy is mandatory. You must also comply with our related data protection policies and procedures. 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, Claire Beckley (RGDP LLP).

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, reputational damage and / or civil claims, for failure to comply with the provisions of the data protection laws. Individuals should also be mindful of the fact that they may also individually be committing a criminal offence.

All Cassiltoun Housing Association personnel, accessing or otherwise processing personal data controlled by Cassiltoun Housing Association have a responsibility for ensuring personal data is collected, stored and handled appropriately and must ensure that it is handled and processed in compliance with data protection law, this policy and the data protection principles.

All managers are additionally responsible for ensuring their direct reports comply with this Data Protection Policy. The Board are ultimately responsible for ensuring that Cassiltoun Housing Association meets its legal obligations.

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: Claire Beckley, claire@rgdp.co.uk

PERSONAL DATA PROTECTION PRINCIPLES

We adhere to the principles relating to processing of personal data set out in the UK General Data Protection Regulation (‘UK GDPR’) whichrequire personal data to be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals (**Lawfulness, Fairness and Transparency**).
- Collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those 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; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay (**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**).

In addition, Cassiltoun Housing Association will comply with the 'Accountability Principle' that states that organisations are to be responsible for, and be able to demonstrate, compliance with the above principles.

LAWFUL BASES FOR PROCESSING PERSONAL DATA

The UK GDPR only allows processing for 6 lawful bases, namely:

(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 also have one of the following legal bases for the processing

(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 ortreatment or the management 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 in our Record of Processing Activities.

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

DATA SHARING

In certain circumstances we may share personal data with third parties. This may be part of a regular exchange of data, one-off disclosures or in unexpected or emergency situations. In all cases, appropriate security measures will be used when sharing any personal data.

Where data is shared regularly, a contract or data sharing agreement will be put in place to establish what data will be shared and the agreed purpose and this will be recorded on our Third-Party Contractors / Suppliers Register.

Prior to sharing personal data, we will consider any legal implications of doing so.

Data Subjects will be advised of data sharing via the relevant the Privacy Notice.

DATA PROCESSORS

Where we engage Data Processors to process personal data on our behalf we will ensure that there is an agreement in place between ourselves and the data processor which meets the requirements of Article 28 of the UK GDPR. Such an agreement will be recorded on our Third=Party Contractors / Supplier Register.

REPORTING A PERSONAL DATA BREACH

The UK GDPR requires us in certain circumstances 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 Chief Executive Officer, or in their absence, the Data Protection Officer. You should preserve any evidence relating to the actual or suspected personal data breach.

INTERNATIONAL TRANSFERS

UK data protection legislation restricts data transfers to countries outside of the UK and the EEA in order to ensure that the level of data protection afforded to individuals by the UK 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 UK and / or the EEA in certain circumstances, including:

(a) the UK Government have issued a decision confirming that the country to which wetransfer the Personal Data ensures an adequate level of protection for the data subjects' rightsand freedoms; and appropriate safeguards are in place.
You must liaise with the Data Protection Officer if you are proposing to transfer personal data outside of the UK and / or the EEA.

DATA SUBJECT'S RIGHTS AND REQUESTS

If a data subjects wishes to exercise ant of their data subject's rights, these should be handled in accordance with Cassiltoun Housing Association's Data Subjects' Rights Procedure.

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 certain processing activities, including high-risk processing. You should conduct a DPIA pre-screening checklist, and where appropriate a full DPIA, in accordance with Cassiltoun Housing Association's Data Protection Impact Assessment Procedure (and liaise with our Data Protection Officer in relation to the same.

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.

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

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 – e.g. from market research, focus groups or other formsof 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.