ARDENGLEN

PRIVACY POLICY

Policy Title:	**Privacy Policy**
Policy Author:	**Claire Beckley, Data Protection Officer**
Date of Approval:	**29 June 2021**
Date for Next Scheduled Review:	**2024**
Review Body:	**Board**
Equality Impact Assessment Complete:	**N/A**
Policy Published on Web:	
Scottish Social Housing Charter Standard	**N/A**
Scottish Housing Regulator Standard:	**N/A**
Scottish Housing Regulator Guidance:	**N/A**

Contents

1. Introduction

Ardenglen Housing Association is committed to ensuring the secure and safe management of personal data held in relation to customers, staff and other individuals. Ardenglen'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 Category Personal Data under the UK General Data Protection Regulation ('UK 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 of such data.

2. Legislation

It is a legal requirement that The Association process personal data lawfully; the Association must process, including collecting, handling storing and destroying personal data in accordance with the relevant legislation.

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

(a) the UK General Data Protection Regulation ("the UK GDPR");

(b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications);

(c) the Data Protection Act; and

(d) any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy.

3. Personal Data

3.1 The Association holds a variety of personal 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 relevant Fair Processing Notices and the Data Protection Addendum of the Terms of and Conditions of Employment which has been provided to all employees.

3.1.1 "Personal Data"means any information relating to an identified or identifiable people ('data subjects'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such a a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

3.1.2 Special category personal data is defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation. (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".

3.1.3 Personal data relating to criminal convictions, suspicions of criminal activity and the absence of criminal convictions.

4. Processing of Personal Data

4.1 The Association is permitted to process Personal Data on behalf of data subjects provided it is doing so on one of the following legal basis:

- Processing with the consent of the data subject (see 4.4 below);
- Processing is necessary for the performance of a contract between The Association and the data subject or for negotiations taking place seeking to enter into such a contract
- 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 and a legitimate interest assessment has been undertaken.

4.2 Fair Processing Notice

4.2.1 The Association has produced a Fair Processing Notice (FPN) which it is required to provide to all customers whose Personal data is processed 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.

4.2.2 The Fair Processing Notice 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.

4.3 Employees

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

4.4 Consent

4.4.1 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. Where consent is relied on it needs to be a freely given, specific, informed and unambiguous indication of the data subjects wishes by which he or she, in a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to him or her.

4.5 Processing of Special Category Personal Data or Sensitive Personal Data

4.5.1 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:

- The data subject has given explicit consent to the processing of this data for a specified purpose;
- Processing is necessary for carrying out obligations or exercising rights related to employment or social security;
- Processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity;

- Processing is necessary for reasons of substantial public interest, on the basis of UK law;
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care treatment or the management of health or social care systems and services on the basis of UK law or pursuant to contract with a health professional;
- Processing is necessary for reasons of public interest in the area of public health; and
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purpose or statistical purposes in accordance with Article 89(1) of the UK GDPR.

Special category personal data also needs to be processed in accordance with Schedule 1 of the Data Protection Act 2018.

5. Data Sharing

5.1 The Association shares its data with various third parties for numerous reasons in order that its day to day activities are carried out. In 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 in to an Agreement with The Association governing the processing of data, security measures to be implemented and responsibility for breaches.

5.2 Data Sharing

5.2.1 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.

5.2.2 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.

5.3 Data Processors

5.3.1 A data processor is a third party entity that processes personal data on behalf of The Association, and are frequently engaged if certain areas of The Association's work is outsourced (e.g. maintenance and repair works). Where a data processor is engaged, a data protection agreement, which meets the requirements of Article 28 of the UK GDPR must be in place before the processing commences.

6. Data Storage and Security

6.1 All Personal Data held by The Association must be stored securely, whether electronically or in paper format.

6.2 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 in accordance with The Association's storage provisions.

6.3 Electronic Storage

6.3.1 Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should be password protected when being sent internally or externally to The Association's data processors or those with whom The Association has entered in to a data sharing Agreement / data processing agreement, as appropriate. 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.

7. Breaches

7.1 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. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported externally in accordance with Clause 7.3 hereof.

7.2 Internal Reporting

The Association takes the security of data very seriously and in the unlikely event of a breach or a suspected breach taking place the following steps will be undertaken (and as may be more clearly defined in a Breach Management Procedure):

- As soon as the breach or potential breach has occurred, employees and officer must as soon as possible, and in any event no later than six (6) hours after it has occurred, notify the DPO 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 DPO must consider whether the breach is one which requires to be reported to the ICO and / or data subjects affected
- Notify third parties in accordance with the terms of any applicable data sharing agreements.

7.3 Reporting of Breaches

The DPO will advise on as to whether to report any breaches to the Information Commissioner's Office ("ICO") within 72 hours of the breach occurring. The DPO must also consider and advise as to whether it is appropriate to notify those data subjects affected by the breach.

8. Data Protection Officer ("DPO")

8.1. 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 an outsourced Data Protection Officer, RGDP LLP.

8.2 The DPO will be responsible for:

8.2.1 monitoring The Association's compliance with Data Protection laws and this Policy;

8.2.2 co-operating with and serving as The Association's contact for discussions with the ICO

8.2.3 reporting breaches or suspected breaches to the ICO and data subjects in accordance with Part 7 hereof.

9. Data Subject Rights

Data subjects' rights shall be dealt with in accordance with The Association' Data Subjects Rights Procedure.

10. Data Protection Impact Assessments ("DPIAs")

10.1 Data Protection Impact Assessments shall be conducted in accordance with The Association's Data Protection Impact Assessment Procedure.

11. Archiving, Retention and Destruction of Data

11.1 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 its Data Retention Policy and Retention Schedule.