Data Protection Policy

April 2018

Our Commitment

ACHA and AHFA are committed to provide equal opportunities across all services and to avoid discrimination. This policy is intended to assist ACHA and AHFA in putting this commitment into practice. Compliance with this policy should also ensure that employees do not commit unlawful acts of discrimination.

This policy can be made available in other formats, for example in large print, audio-format or Braille: the document may also be available in other languages, in full or summary form, as appropriate.

Contents

Section 1:	**Introduction**
Section 2:	**The Law and Good Practice**
Section 3:	**GDPR Principles**
Section 4:	**Our Policy Objectives**
Section 5:	**Implementing our Policy Objectives**
Section 6:	**Responsibility**
Section 7:	**Data Protection Officer**
Section 8:	**Demonstrating Compliance**
Section 9:	**Policy Review**

1. Introduction

Argyll Community Housing Association Limited (ACHA) is a registered social landlord (RSL) registered with the Scottish Housing Regulator (SHR), an industrial and provident society registered with the Financial Conduct Authority (FCA) and a charity registered with the Office of the Scottish Charity Regulator (OSCR).

Argyll Homes for All Limited (AHFA) is a company registered with the Companies Registrar.

Together ACHA and AHFA form the ACHA Group and this policy applies to the whole ACHA Group.

The key legislation, referred to throughout this policy is:

- The General Data Protection Regulation

2. The Law and Good Practice

The General Data Protection Regulation (GDPR) came into force on 25th May 2018 and replaced the Data Protection Act 1998 (DPA). It is designed to protect personal information which is collected in various formats. GDPR reinforces the principle that personal information remains the property of the individual who are giving their permissions for an organisation is use that personal data. Individuals have rights over the personal data, including the right of access to any records of information held about them. The rights of individuals is detailed in section xxx.

GDPR defines personal data as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

GDPR covers everyone involved in the Group’s business or activities and includes:

- Employees and applicants for employment
- Board and Committee members
- Tenants and applicants for housing
- Clients and grant recipients
- Contractors and consultants

3. GDPR Principles

The GDPR sets out 6 principles of data protection and these are as follows:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing form archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is in inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Our Policy Objectives

The Group is committed to the data protection principles of GDPR of:

- Collect minimum personal data
- Control the access of personal data
- Keep personal data for the minimum time necessary and delete thereafter

5. Implementing our Policy Objectives

The Group's policy is to respect the privacy of all individuals, including employees, board members, tenants and applicants

The Group will protect all personal data, particularly in relation to employees, board members, tenants and applicants and accepts responsibility for the safe handling of personal data by other people or companies, which may be involved in the Group's activities.

The Group will comply with the data protection principles as outlined by GDPR.

The Director of Finance and IT acts as the Data Protection Officer for the Group.

6. Responsibility

The protection of personal data is the responsibility of each employee and board member.

7. Data Protection Officer

Bruce West
Director of Finance and IT
Argyll Community Housing Association
Dalriada House
Lochgilphead

Email: bruce.west@acha.co.uk

8. Demonstrating Compliance

GDPR requires the Group to show how we comply with the data protection principles.

To demonstrate compliance with the accountable principle, the Group will:

- Implement appropriate technical and organizational measures that ensure and demonstrate compliance e.g. staff training, internal audits of processing activities, reviews of policies
- Maintain relevant documentation on processing activities
- Implement measures that meet the principles of data protection by design and default
- Use data protection impact assessments where appropriate

9. Policy Review

We ensure that this Data Protection policy is reviewed on a 3 yearly basis.

Policy Owner	Director of Finance & IT
Policy Creation Date	April 2018
Version Number	1.0
Date Last Amended	New
Review Period	3 Years
Previous Review Dates	New
Review Committee	Policy Committee
Next Review Date	31 March 2021

Appendix 1

Rights of individuals
Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise thee following rights:

Right to be informed
- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency

Right of access
- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

Right to rectification
- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete
- This must be done without delay, and no later than one month.

Right to erasure
- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing

Right to restrict processing
- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

Right to data portability
- We must provide individuals with their data so that they can reuse it for their own purposed or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making and profiling. Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Appendix 2

Group Responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

Employee responsibilities

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay to the Information Commissioner's Office (ICO)

Data Protection Officer responsibilities

- Keeping the board updated about data protection responsibilities, risks and
- issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by us
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

- Addressing data protection queries from clients, target audiences or media outlets adhere to data protection laws and the company's Data Protection Policy

IT Manager's responsibilities

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data