Organisational Policy

Group Data Protection and Privacy Policy

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

1. Introduction

Argyll Community Housing Association Limited (ACHA) is a registered social landlord (RSL) registered with the Scottish Housing Regulator (SHR), a registered cooperative and community benefit 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.

Argyll Community Housing Association and Argyll Homes for All (the ACHA Group) is committed to ensuring the secure and safe management of data held by the Group in relation to customers, staff and other individuals. The Group'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 Group needs to gather and use certain information about individuals. These can include customers (tenants, factored owners etc.), employees and other individuals that the Group has a relationship with. The Group 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 GDPR).

This Policy sets out the Group'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. The Law and Good Practice

It is a legal requirement that the Group process data correctly; the Group 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 UK General Data Protection Regulation ("the 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) any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the GDPR, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of Personal Data and privacy as a consequence of the United Kingdom leaving the European Union;
(d) the Data Protection Act 2018; and
(e) any amendments to the above legislation which is passed in future connected to the collection and use of personal data

It is designed to protect personal information which is collected in various formats. The GDPR reinforces the principle that personal information remains the property of the individual who is giving their permission for an organisation to use that Personal Data. Individuals have rights over the Personal Data, including the right of access to any records of information held aboutthem. The rights of individuals are detailed in Appendix 1.

The 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”. This definition may be amended by subsequent updates to data protection legislation and the most recent legislative definition should be used.

The GDPR also recognises that certain Personal Data, if improperly or unlawfully used, could have significant negative repercussions on the individual in question. Such Personal Data is termed ‘special category Personal Data’ and there are additional requirements that the Group must meet when handling this data. Examples of special category Personal Data is Personal Data related to a person’s:

racial or ethnic origin	political opinions	religious or philosophical beliefs
trade union membership	genetic data	biometric data
health	sex life	sexual orientation

Personal Data relating to criminal offences is also given additional protection in the GDPR and the Group shall only use such data in accordance with those requirements.

Where any new collection or use of special category Personal Data or criminal offence Personal Data is being considered, advice should be obtained from the Data Protection Officer (discussed below)

The 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 (where these are individuals and not companies) and their employees;
- Private owners;
- Factored owners.

3. GDPR Principles

The GDPR sets out 7principles which should govern the Group's approach to collecting and using Personal Data. These are that Personal Data being used by the Group must be:

- Processed (e.g. used) lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (e.g. the Group should have a clear reasons for using Personal Data and not use Personal Data for a new purpose except where certain conditions are met);
- Adequate, relevant and limited to what is necessary in relation to the purposes for which the Personal Data in question is processed (e.g. the Group should avoid collecting more Personal Data than is needed in order to fulfil an identified purpose);
- 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 (e.g. the Group should not keep Personal Data for longer than is needed and should not hold on to Personal Data 'just in case');
- Used and held in a manner that is secure and protects Personal Data from loss, destruction, damage or unlawful use or access;
- Used alongside measures and procedures the Group maintains to demonstrate compliance with the principles.

4. Our Policy Objectives

The Group needs to use and gather certain Personal Data – for example the Personal Data of employees, tenants and other customers. This will involve managing a significant amount of Personal Data from a variety of sources and using it for different reasons. Where the Group collects and uses Personal Data we are committed to ensure we are doing so in accordance with the data protection principles set out above.

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, boardmembers, tenants and applicants and other customers.

6. Fair Processing Notices

The GDPR requires the Group to provide detailed, specific information to an individual about how the Group will use that individual's Personal Data. This information should be provided by giving the individual a Fair Processing Notice (although there will be some circumstances where different methods may be more appropriate in which case the Data Protection Officer should be consulted).

The Group produces a range of Fair Processing Notices which can be found at the location below.

Notices can be found www.acha.co.uk. They should be provided to individuals when

ACHA collects, receives or begins to use an individual's Personal Data. There are limited exceptions to this and where you consider an exception might apply you should speak to the Data Protection Officer to confirm the position.

7. Processing of Personal Data

The term 'processing' relates to the Group's collection and use of Personal Data in any method. Where processing Personal Data, the Group must have a lawful basis for doing so. There are a number of lawful bases set out in the GDPR and ones that the Group will commonly rely on are set out below:

- The individual has given their consent;
- Processing is necessary for the performance of a contract between the Group and the individual or for entering into a contract with the individual;
- Processing is necessary for the Group's compliance with a legal obligation;
- Processing is necessary to protect the vital interests of the individual or another person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the Group's official authority; or
- Processing is necessary for the purposes of legitimate interests.

As noted above, additional requirements must be met when the Group collects and uses special category Personal Data or criminal offence data and further advice should be sought on this when relevant.

8. Consent

Consent as a ground of processing will require to be used from time to time by the Group when collecting and using Personal Data. It should be used by the Group where no other alternative ground for processing is available. Any consent must be informed and freely given and can be withdrawn at any time.

The Group has a form that should be used when obtaining consent. The form has guidance notes that should be referred to.

9. Data Sharing

The Group 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 Group's relevant policies and procedures. This may involve sharing Personal Data with third parties.

Before sharing Personal Data with third parties the Group must ensure certain safeguards and, where appropriate, contractual arrangements are in place. This includes, but is not limited to: ensuring there is a clear lawful purpose for sharing the data; confirming that the third party has appropriate security measures in place to keep Personal Data shares secured and ensuring that individuals whose data might be shared are aware of this (either through our Fair Processing Notice or via other means).

Where any third party is acting as the Group's 'data processor' or the Group and the third party are joint data controllers, there must be a written contract in place that contains certain provisions concerning the use of Personal Data in accordance with the requirements of the GDPR. Where sharing Personal Data with another independent data controller, there should be clear arrangements in place for the protection and use of the Personal Data.

Advice from the Data Protection Officer should be obtained before Personal Data is shared with any new third party, or where the Group is already sharing Personal Data with a third party, before any new type Personal Data is shared or Personal Data is shared for a new purpose.

10. Data Storage and Security

All Personal Data held by the Group must be stored securely, whether electronically or in paper format.

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 Group's storage provisions.

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) to keep Personal Data secure.

You must 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.

11. Breaches

A data breach can occur at any point when handling Personal Data and the Group 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.

The Group maintains a separate procedure document on handling data breaches which should be followed in the event of a breach. It can be accessed www.acha.co.uk.

12. Privacy Impact Assessments (PIAs)

These are a means of assisting the Group in identifying and reducing the risks that our operations have on personal privacy of individuals.

The Group shall carry out a PIA 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.

When conducting a PIA, the Group shall include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the Personal Data.

The ICO shall be consulted where a PIA identifies a high level of risk which cannot be reduced. The Data Protection Officer will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the Data Protection Officer within five (5) working days.

13. Retention of Personal Data

The Group cannot store and retain Personal Data indefinitely. It must ensure that Personal Data is only retained for the period necessary. The Group shall ensure that all Personal Data is archived and destroyed in accordance with the periods specified within the Group's Data Retention Policy. This policy can be accessed at www.acha.co.uk.

If a genuine requirement to retain Personal Data beyond the period in the above policy is identified, approval will be sought from the Data Protection Officer to continue retaining said Personal Data. The Data Protection Officer may refuse to approve the holding of such Personal Data in which case it should be destroyed/archived as necessary.

14. Responsibility

The Group's Data Protection Officer (whose details are noted below) has lead management for the Group's compliance with Data Protection Law. This will include effective implementation and regular review of this Policy.

Further details on responsibilities associated with this Policy are set out in Appendix 2.

15. Demonstrating Compliance

The GDPR requires the Group to show how we comply with the data protection principles.To demonstrate compliance with the accountability 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

16. Data Protection Officer

Bruce West
Director of Finance and IT

Argyll Community Housing Association
Dalriada House
Lochgilphead

Email: bruce.west@acha.co.uk

17. Policy Review

We ensure that this Data Protection and Privacy policy is reviewed on a 5 yearly basis.

Policy Owner	Director of Finance & IT
Policy Creation Date	May 2023
Version Number	2.0
Date Last Amended	May 2018
Review Period	5 Years
Previous Review Dates	May 2018
Review Committee	Policy Committee
Next Review Date	30 April 2028

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 the following rights:

Right to be informed
- Providing fair processing notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly ifaimed at children;
- Keeping a record of how we use Personal Data to demonstrate compliance with theneed 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.

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 a request to restrict, block, or otherwise suppress theprocessing of Personal Data in certain circumstances.

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 directlyto another controller if requested.

Right to object

- We must respect the right of an individual to object to data processing in certain circumstances – although individuals may always object to direct marketing and those objections should be upheld.

Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making andprofiling which will have a significant impact on them. Individuals retain their right to object to such automated processing, have therationale explained to them, and request human intervention.

The Group maintains a separate set of procedures for managing certain data subject right requests.

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 becompromised

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;
- Seek guidance from the Data Protection Officer if you are unsure about what the Group must do to comply with Data Protection Law;
- Raise any requests from individuals regarding their Personal Data to the Data Protection Officer;
- Raise any concerns, notify any breaches or errors, and report anything suspicious orcontradictory to this policy or our legal obligations without delay to the Data Protection Officer.

Chief Executive responsibilities

- Overall accountability for complying with data protection obligations for the Group

Director responsibilities

- Accountable for securing departmental data protection obligations;
- Creating a culture of good data protection practice with the department;
- Supporting managers to ensure data protection obligations, including the Data

Protection policy are complied with.

Manager responsibilities

- Securing compliance with data protection obligations, including the Data Protection Policy, for services managed;
- Promoting good data protection practice for service managed;
- Supporting staff managed to meet their data protection obligations.

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.