DATA PROTECTION POLICY

Date Approved	Proposed Review Date
27 April 2023	April 2025

Introduction

Abronhill Housing Association (referred to herein as 'AHA') is a Data Controller registered with the Information Commissioner's Office (Registration No: Z4852919).

AHA is committed to ensuring the lawful, fair and transparent management of personal data. This policy sets out how we will do this.

All directors, associates, officers, members, employees, volunteers, committee members (temporary and permanent) (referred to herein as 'AHA personnel') have a responsibility to ensure compliance with this policy and associated Appendices which set out AHA's commitment to process personal data in accordance with the relevant legislation including:

- UK General Data Protection Regulation.
- UK Data Protection Act 2018 (DPA 2018).
- Privacy and Electronic Communications Regulations 2003 (PECR).

Scope

This Policy applies to all personal data held by AHA that relates to living identifiable individuals regardless of the category of data or the format of the data. Personal data is any data which could be used to identify a living individual including, for example, name, address, email, postcode, CCTV image and photograph and video recordings. Special Category personal data is any information relating to racial or ethnic origin, political opinions, religious beliefs, health (mental and physical), sexual orientation, Trades Union membership and criminal convictions, including suspicion of criminal activity.

This policy applies to personal data held or accessed on AHA premises and systems or accessed remotely via home or mobile working. Personal data stored on personal and removable devices is also covered by this policy.

Responsibilities for Compliance

The Directors are ultimately responsible for ensuring that AHA meets its legal obligations.

Failure to comply with data protection legislation could lead to financial penalties, regulatory action, as well as reputational damage.

All AHA personnel, accessing or otherwise processing personal data controlled by AHA 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 regulations, this policy and the data protection principles.

The Finance/Administration Officer, with advice and assistance from the Data Protection Officer (DPO), RGDP LLP, is responsible for:

- monitoring compliance with this policy and data protection legislation;
- managing personal data breaches and data subject rights requests;
- recording and maintaining appropriate records of processing activities and the documented evidence required for compliance.

Compliance

AHA will comply with its legal obligations and the **data protection principles** by ensuring that personal data is:

- **processed lawfully, fairly and in a transparent manner in relation to individuals**. Individuals will be advised on the reasons for processing via a Privacy Notice. Where data subjects' consent is required to process personal data, consent will be requested in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Data Subjects will be advised of their right to withdraw consent and the process for Data Subjects to withdraw consent will be simple.

- **collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**. Personal data will only be used for the original purpose it was collected for and these purposes will be made clear to the data subject. If AHA wishes to use personal data for a different purpose, for example for research, the data subject will be notified prior to processing.

- **adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed**. AHA will only collect the minimum personal data required for the purpose. Any personal data deemed to be excessive or no longer required for the purposes collected for will be securely deleted in accordance with AHA's Retention Policy. Any personal information that is optional for individuals to provide will be clearly marked as optional on any forms.

- **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**. AHA will take reasonable steps to keep personal data up to date, where relevant, to ensure accuracy. Any personal data found to be inaccurate will be updated promptly. Any inaccurate personal data that has been shared with third parties will also be updated.

- **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**. AHA will hold data for the minimum time necessary to fulfil its purpose. Timescales for retention of personal data will be stated in a Retention Schedule. Data will be disposed of in a responsible manner ensuring confidentiality and security.

- **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**. AHA will implement appropriate security measures to protect personal data. Personal data will only be accessible to those authorised to access personal data on a 'need to know' basis. AHA personnel will keep data secure by taking sensible precautions and following the relevant AHA policies and procedures relating to data protection.

In addition, AHA 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.

Data Sharing

In certain circumstances AHA 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.

Prior to sharing personal data, AHA 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 AHA engages Data Processors to process personal data on its behalf, it will ensure that:

- Data processors have appropriate organisational and technical security measures in place;
- No sub-processors are used without prior written consent from AHA;
- An appropriate contract or agreement is in place detailing the obligations; and requirements placed upon the data processor.

Security Incident & Breach Management

Occasionally AHA may experience a data security incident or personal data breach; this could be if personal data is:

- Lost: for example, misplacing documents or equipment that contain personal data through human error; via fire, flood or other damage to premises where data is stored.
- Stolen: theft or as a result of a targeted attack on the IT network (cyber-attack).
- Accidently disclosed to an unauthorised individual: for example, email or letter sent to the wrong address.
- Inappropriately accessed or used.

All security incidents or personal data breaches will be reported to and managed by the Data Protection Lead, the Finance / Administration Officer, who will be advised and assisted by the DPO.

The Information Commissioner's Office and the individuals affected will be notified promptly, if required.

All security incidents and personal data breaches will be managed in accordance with AHA's Breach Notification Policy.

Individual Rights

AHA will uphold the rights of data subjects to access and retain control over their personal data in accordance with its Data Subject Rights & SAR Policy. AHA will comply with individuals':

- **Right to be Informed** – by ensuring individuals are informed of the reasons for processing their data in a clear, transparent and easily accessible form and informing them of all their rights.

- **Right to Access** – by ensuring that individuals are aware of their right to obtain confirmation that their data is being processed; access to copies of their personal data and other information such as a privacy notice and how to execute this right.

- **Right to Rectification** – by correcting personal data that is found to be inaccurate. AHA will advise data subjects on how to inform us that their data is inaccurate. Inaccuracies with be rectified without undue delay.

- **Right to Erasure** (sometimes referred to as 'the right to be forgotten') – AHA will advise data subjects of their right to request the deletion or removal of personal data where processing is no longer required or justified.

- **Rights to Restrict Processing** – AHA will restrict processing when a valid request is received by a data subject and inform individuals of how to exercise this right.

- **Right to Data Portability** – by allowing, where possible, data to be transferred to similar organisation in a machine-readable format.

- **Right to Object** – by stopping processing personal data, unless legitimate grounds can be demonstrated for the processing which override the interest, rights and freedoms of an individual, or the processing is for the establishment, exercise or defence of legal claims.

Data Protection by Design

AHA has an obligation to implement technical and organisational measures to demonstrate that data protection has been considered and integrated into its processing activities.

When introducing any new type of processing, particularly using new technologies, it will take account of whether the processing is likely to result in a high risk to the rights and freedoms of individuals and consider the need for a Data Protection Impact Assessment (DPIA).

All new policies including the processing of personal data will be reviewed by the Finance/Administration Officer to ensure compliance with the law and establish if a DPIA is required. Advice and assistance will be provided by the DPO and if it is confirmed that a DPIA is required, it will be carried out in accordance with AHA's DPIA Procedure.

Training

All AHA personnel will be made aware of good practice in data protection and where to find guidance and support for data protection issues. Adequate and role specific data

protection training will be provided during induction and annually thereafter to everyone who has access to personal data to ensure they understand their responsibilities.

Breach of Policy

Any breaches of this policy may be dealt with in accordance with AHA's disciplinary procedures.

Monitoring and Reporting

Regular monitoring and audits will be undertaken by the Finance / Administration Officer and/or DPO to check compliance with the law, this policy and associated procedures. Any concerns will be raised with the Company Director/s.

Policy Review

This policy will be reviewed every 24 months or when required to address any weakness in the procedure or changes in legislation or best practice.

Dated	20 April 2023
Document Owner	Finance / Administration Officer
Approved By	
Review Date	April 2025