REIDVALE HOUSING ASSOCIATION

Privacy Policy

Policy Approved	28.06.23
Due for Review	June 2026
Author	

POLICY SUMMARY

Purpose:	The Privacy policy sets out the Association's duties in processing data and the purpose of this Policy is to set out the procedures for the management of such data.
Guidance:	The Association is a company under the Co-operative and Community Benefit Societies Act 2014, and a company regulated by the Financial Conduct Authority (FCA). Statutory Guidance The Scottish Social Housing Charter Requirements of the Scottish Housing Regulator
Regulatory Compliance	Standard 1: The governing body leads and directs the RSL to achieve good outcomes for its tenants and other service users. Standard 2: The RSL is open about and accountable for what it does. It understands and takes account of the needs and priorities of its tenants, service users and stakeholders. And its primary focus is the sustainable achievement of these priorities. Standard 3: The RSL manages its resources to ensure its financial well-being, while maintaining rents at a level that tenants can afford to pay. Standard 4: The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation's purpose. Standard 5: The RSL conducts its affairs with honesty and integrity. Standard 6: The governing body and senior officers have the skills and knowledge they need to be effective.
Linked Policies	All policies
Financial Impact	Low
Risk Assessment	Medium
Date Reviewed:	June 2023
Date approved by Management Committee:	28 June 2023

Contents Page no.

1. INTRODUCTION

1.1 Reidvale Housing Association (RHA) is a community based organisation based in Dennistoun. Our core business is the provision of affordable housing and related services. RHA is committed to ensuring the secure and safe management of data held by the Association in relation to customers, staff and other individuals. The Association'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.

1.2 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 Categories of Personal Data under the GDPR).

1.3 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. AIMS AND OBJECTIVES

2.1 The aims and objective of this policy is to ensure the secure and safe management of data held by the Association in relation to customers, staff and other individuals.

3. LEGAL AND REGULATORY FRAMEWORK

3.1 Reidvale Housing Association, a registered society under the Cooperative and Community Benefit Societies Act 2014, a registered social landlord and regulated by the Financial Conduct Authority (FCA).

3.2 We are regulated by the Scottish Housing Regulator (SHR). Their Regulatory Framework sets out seven Standards of Governance and Financial Management. Relevant to this Policy are particular elements under these standards:

- Standard 1: The governing body leads and directs the RSL to achieve good outcomes for its tenants and other service users.
- Standard 2: The RSL is open about and accountable for what it does. It understands and takes account of the needs and priorities of its tenants, service users and stakeholders. And its primary focus is the sustainable achievement of these priorities.
- Standard 3: The RSL manages its resources to ensure its financial well-being, while maintaining rents at a level that tenants can afford to pay.
- Standard 4: The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation's purpose.

- Standard 5: The RSL conducts its affairs with honesty and integrity.

- Standard 6: The governing body and senior officers have the skills and knowledge they need to be effective.

3.3 It is a legal requirement that the Association process data correctly; the Association must collect, handle and store personal information in accordance with the relevant legislation.

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

a) The UK GDPR;
b) The Data Protection Act 2018
c) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and,
d) any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law including .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

4. PRIVACY POLICY

4.1 DATA

4.1.1 The Association holds a variety of 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 the Fair Processing Notice at Appendix 1 hereto and the Data Protection Addendum of the Terms of and Conditions of Employment which has been provided to all employees.

4.1.2 “Personal Data” is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by the Association.

4.1.3 The Association also holds Personal data that is sensitive in nature (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”.

4.2 PROCESSING OF PERSONAL DATA

4.2.1 The Association 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 RHA wishes to use personal data for a different purpose, 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.* RHA 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. 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.* The Association 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*. The Association will hold data for the minimum time necessary to fulfil its purpose. Timescales for retention of personal data will be stated in the 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*. RHA 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. Employees will keep data secure by taking sensible precautions and following the relevant RHA policies and procedures relating to data protection.

  In addition, RHA 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.

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

  - Processing with the consent of the data subject (see clause 4.5 hereof).

- Processing is necessary for the performance of a contract between the Association and the data subject or for entering into a contract with the data subject.

- 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.

- Processing is necessary for the purposes of legitimate interests.

4.3 FAIR PROCESSING NOTICE

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

4.3.2 The Fair Processing Notice at Appendix 1 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.

4.4 EMPLOYEES

4.4.1 Employee Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by the Association. 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.

4.4.2 A copy of any employee's Personal Data held by the Association is available upon written request by that employee from the Association's Interim Director.

4.5 CONSENT

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. In the event that the Association requires to obtain consent to process a data subject's Personal Data, it shall obtain that consent in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant consent form, where possible, if willing to consent. Any consent to be obtained by the Association must be for a specific and defined purpose (i.e. general consent cannot be sought) and the data subject should be advised of their right to withdraw their consent.

4.6 PROCESSING OF SPECIAL CATEGORY PERSONAL DATA OR SENSITIVE PERSONAL DATA

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 or otherwise in accordance with the law:

- 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 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.

4.7 DATA SHARING

4.7.1 The Association shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with the Association's relevant policies and procedures. 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.

4.7.2 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.

4.7.3 In certain circumstances the Association 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 personal data.

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

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

4.7.4 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

4.8 DATA PROCESSORS

4.8.1 A data processor is a third party entity that processes personal data on behalf of the Association, and are frequently engaged if certain of the Association's work is outsourced (e.g. payroll, maintenance and repair works).

4.8.2 A data processor must comply with Data Protection laws. The Association's data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify the Association if a data breach is suffered.

4.8.3 If a data processor wishes to sub-contact their processing, prior written consent of the Association must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

4.8.4 Where the Association contracts with a third party to process personal data held by the Association, it shall require the third party to enter in to a Data Protection Addendum with the Association.

4.9 DATA STORAGE AND SECURITY

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

4.10 PAPER STORAGE

4.10.1 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.

4.11 ELECTRONIC STORAGE

4.11.1 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. 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.

4.12 BREACHES

4.12.1 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.

4.13 INTERNAL REPORTING

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

- Lost e.g. 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, e.g. email or letter sent to the wrong address.
- Inappropriately accessed or used.

4.13.2 The Association takes the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the DPO must be notified 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 Association must seek to contain the breach by whatever means available.
- The DPO must consider whether the breach is one which requires to be reported to the ICO and data subjects affected and do so in accordance with this clause 7.
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements.

4.14 REPORTING TO THE ICO

4.14.1 The DPO will require to report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the Information Commissioner's Office ("ICO") within 72 hours of the breach occurring. The DPO must also consider whether it is appropriate to notify those data subjects affected by the breach.

4.15 DATA PROTECTION OFFICER

4.15.1 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 a Data Protection Officer whose details are noted on the Association's website and contained within the Fair Processing Notice at Appendix 3 hereto.

4.15.2 The DPO will be responsible for:

- Monitoring the Association's compliance with Data Protection laws and this Policy;
- Co-operating with and serving as the Association's contact for discussions with the ICO;
- Reporting breaches or suspected breaches to the ICO and data subjects in accordance with Part 7 hereof.

4.16 DATA SUBJECT RIGHTS

4.16.1 Certain rights are provided to data subjects under the GDPR. Data Subjects are entitled to view the personal data held about them by the Association, whether in written or electronic form.

4.16.2 Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to the Association's processing of their data. These rights are notified to the Association's tenants and other customers in the Association's Fair Processing Notice.

4.17 SUBJECT ACCESS REQUESTS

4.17.1 Data Subjects are permitted to view their data held by the Association upon making a request to do so (a Subject Access Request). Upon receipt of a request by a data subject, the Association must respond to the Subject Access Request within one month of the date of receipt of the request. The Association:

- Must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law;
- where the personal data comprises data relating to other data subjects, must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the Subject Access Request; or,
- where the Association does not hold the personal data sought by the data subject, must confirm that it does not hold any personal data sought to the data subject as soon as practicably possible, and in any event, not later than one month from the date on which the request was made.

4.18 THE RIGHT TO BE FORGOTTEN

4.18.1 A data subject can exercise their right to be forgotten by submitting a request in writing to the Association seeking that the Association erase the data subject's Personal Data in its entirety.

4.18.2 Each request received by the Association will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.4 and will respond in writing to the request.

4.19 THE RIGHT TO RESTRICT OR OBJECT TO PROCESSING

4.19.1 A data subject may request that the Association restrict its processing of the data subject's Personal Data, or object to the processing of that data.

4.19.2 In the event that any direct marketing is undertaken from time to time by the Association, a data subject has an absolute right to object to processing of this nature by the Association, and if the Association receives a written request to cease processing for this purpose, then it must do so immediately.

4.19.3 Each request received by the Association will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.5 and will respond in writing to the request.

4.20 PRIVACY IMPACT ASSESSMENTS ("PIAs")

4.20.1 These are a means of assisting the Association in identifying and reducing the risks that our operations have on personal privacy of data subjects.

4.20.2 The Association 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; and,

- In carrying out a PIA, 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

4.20.3 The Association will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The Data Protection Officer ("DPO") 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 DPO within five (5) working days.

4.21 ARCHIVING, RETENTION AND DESTRUCTION OF DATA

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 retention schedule.

5. STAFF TRAINING

5.1 Reidvale Housing Association will ensure that all staff receive appropriate and regular training on data protection.

6. EQUALITY AND DIVERSITY

6.1 Reidvale Housing Association is an equal opportunities organisation. We are committed to providing an environment of respect, understanding, encouraging diversity and eliminating discrimination. No person or group of persons applying for housing and housing services will be treated less favourably than any other persons or groups of persons because of their age, disability, gender reassignment, marriage and civil partnership, pregnancy or maternity, race, religion or belief, sex, or sexual orientation.

7. COMPLAINTS

7.1 Although we are committed to providing high levels of service, we accept that there may be occasions where a service user may not be satisfied with the service received from the Association. We value all complaints and use this information to help us improve our service. Any service user, complying with the procedure, but remaining dissatisfied with any aspect of the service they have received have the right to submit a complaint to the Association in accordance with the Complaints Handling Procedure.

8. POLICY REVISION

8.1 The Association undertakes to carry out a comprehensive review of all aspects of this policy at least every three years. The review will take account of legislative changes, new policy guidance, best practice advice and the views of service users.