50 YEARS OF Reidvale Housing Association

DATA PROTECTION POLICY

September 2026

Document Identifier:	CRP15
Adoption Date:	October 2026
Review Date:	October 2029

CONTENTS

1. POLICY SCOPE 3
2. POLICY OBJECTIVE 3
3. GOVERNANCE 3
4. DEFINITIONS 4
5. RESPONSIBILITIES 5
6. IMPLEMENTATION GUIDELINES 6
7. PROCEDURES 6
8. INDIVIDUAL RIGHTS 9
9. DATA PROTECTION COMPLAINTS 10
10. DATA PROTECTION BY DESIGN AND DPIAS 10
11. INTERNATIONAL TRANSFERS 10
12. BREACH OF POLICY 10
13. COMMUNICATION GUIDELINES 11
14. REVIEWING AND MONITORING 11
15. APPROVAL 12

APPENDIX 1 – EQUALITY AND HUMAN RIGHTS IMPACT ASSESSMENT 13

1. POLICY SCOPE

1.1 Reidvale Housing Association (Reidvale) is a controller for the personal data it determines how and why to process. Reidvale is registered with the Information Commissioner's Office under registration number Z5914204.

1.2 This policy applies to all personal data processed by or on behalf of Reidvale about living identifiable individuals, regardless of the format, system or location in which the information is held. It applies to personal data processed on Reidvale premises, through Reidvale systems, while working remotely, and on authorised mobile or removable devices.

1.3 The policy applies to all Management Committee members, officers, employees, temporary workers, volunteers, associates and any other person who processes personal data on Reidvale's behalf. In this policy these groups are referred to collectively as Reidvale personnel.

1.4 The policy covers personal data relating to tenants, applicants, household members, factored owners, staff, contractors, Management Committee members, complainants, witnesses, residents and other people whose information Reidvale processes.

2. POLICY OBJECTIVE

2.1 The objective of this policy is to ensure that Reidvale processes personal data lawfully, fairly, transparently and securely, protects the rights and freedoms of individuals, and can demonstrate compliance with applicable data protection law.

2.2 The policy sets the minimum organisational standards for collecting, using, sharing, retaining, securing and disposing of personal data. It also establishes responsibility for individual rights, personal data breaches, data protection complaints, data protection impact assessments and oversight of processors.

3. GOVERNANCE

3.1 This policy is governed by the UK data protection framework, including:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Data (Use and Access) Act 2025.

- Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), where applicable.

3.2 Reidvale will also have regard to relevant guidance and codes issued by the Information Commissioner's Office (ICO). Guidance does not replace the law, but Reidvale will take it into account when deciding how to comply.

3.3 This policy should be read alongside Reidvale's Notifiable Events Policy, Data Subject Rights Procedure, Information Security Incident and Personal Data Breach Management Procedure, Retention Policy, Data Protection Impact Assessment Procedure and relevant information security policies and procedures.

4. DEFINITIONS

- **Personal data:** information relating to an identified or identifiable living individual. Examples include names, contact details, tenancy information, financial information, identifiers, correspondence and CCTV images.

- **Special category data:** personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data used for identification, health data, or data concerning a person's sex life or sexual orientation.

- **Criminal offence data:** personal data relating to criminal convictions and offences, allegations, proceedings or related security measures. This is not special category data, but it is subject to separate statutory safeguards.

- **Processing:** any operation performed on personal data, including collecting, recording, organising, storing, accessing, using, sharing, amending, restricting, deleting or destroying it.

- **Controller:** the organisation that determines the purposes and means of processing personal data.

- **Processor:** an organisation or person that processes personal data on behalf of a controller and on the controller's documented instructions.

- **Data subject:** the living individual to whom personal data relates.

- **Personal data breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- **Data Protection Impact Assessment (DPIA):** a documented assessment used to identify and reduce data protection risks in processing that is likely to result in a high risk to individuals.

- **ICO:** the Information Commissioner's Office, the UK regulator for data protection law.

5. RESPONSIBILITIES

5.1 **The Management Committee** has ultimate responsibility for ensuring that Reidvale meets its data protection obligations. The Management Committee provides strategic oversight and receives significant compliance concerns and assurance information.

5.2 **Data Protection Lead - Jamie Mallan, Head of Corporate and Strategy** has day-to-day responsibility for coordinating data protection compliance, including rights requests, data protection complaints, personal data breaches, records of processing and supporting evidence of compliance. The Data Protection Lead will seek DPO advice where required.

5.3 **Data Protection Officer (DPO) - RGDP LLP** provides independent advice, monitors compliance, advises on DPIAs, supports engagement with the ICO and reports significant concerns to the highest management level as appropriate. Reidvale remains responsible for its compliance decisions.

5.4 **Managers** must ensure that processing within their areas is documented, staff follow this policy and related procedures, access is appropriate, data quality and retention are managed, and proposed changes to processing are escalated where a DPIA or DPO advice is required.

5.5 **All Reidvale personnel** must only process personal data for authorised purposes, follow this policy and related procedures, keep personal data secure, complete required training, and report suspected incidents, breaches or compliance concerns promptly.

5.6 **Processors and contractors** must comply with the applicable contractual data protection requirements and only process Reidvale personal data within their authorised role and instructions.

6. IMPLEMENTATION GUIDELINES

6.1 Reidvale will implement this policy through documented governance, proportionate technical and organisational measures, staff training and operational procedures. The following requirements apply to all processing:

6.2 A clear purpose and appropriate lawful basis must be identified before personal data is processed. Additional statutory conditions must be identified where special category or criminal offence data is processed.

6.3 Individuals must receive appropriate privacy information about how their personal data is used, unless a lawful exception applies.

6.4 Only personal data that is adequate, relevant and necessary for the purpose will be collected or used.

6.5 Personal data must be kept accurate where accuracy is relevant to the purpose and corrected without undue delay when inaccuracies are identified.

6.6 Personal data must not be retained for longer than necessary. Retention and secure disposal will follow Reidvale's Retention Policy and Schedule.

6.7 Access to personal data must be limited to authorised people with a genuine need to know, supported by appropriate security controls.

6.8 New or materially changed processing must consider data protection by design and default and whether a DPIA is required.

6.9 Sharing, processor arrangements and any international transfers must be assessed and documented before they take place.

6.10 Requests from individuals and data protection complaints must be recognised and escalated promptly so statutory timescales can be met.

7. PROCEDURES

7.1 Detailed operational steps are maintained in Reidvale's supporting procedures. The requirements below form part of this policy and must be followed when the relevant processing takes place.

8. DATA PROTECTION PRINCIPLES

8.1 **Lawfulness, fairness and transparency:** Personal data will be processed lawfully, fairly and transparently. Reidvale will identify and document an

appropriate lawful basis. Where consent is relied upon, it must be freely given, specific, informed, unambiguous and as easy to withdraw as it is to give. Privacy information will explain the purposes of processing and other information required by law.

8.2 **Purpose limitation:** Personal data will be collected for specified, explicit and legitimate purposes and will not be used for an incompatible purpose. Where Reidvale proposes a new use, it will assess compatibility and provide updated privacy information where required.

8.3 **Data minimisation:** Reidvale will only collect and use personal data that is adequate, relevant and limited to what is necessary. Optional information will be identified as optional where appropriate.

8.4 **Accuracy:** Reasonable steps will be taken to keep personal data accurate and up to date where required. Inaccurate information will be corrected or erased without undue delay and relevant recipients will be informed where the law requires.

8.5 **Storage limitation:** Personal data will be retained only for as long as necessary for the purpose and in line with the Retention Policy and Schedule. Disposal must preserve confidentiality and security.

8.6 **Integrity and confidentiality:** Appropriate technical and organisational measures will protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

8.7 **Accountability:** Reidvale is responsible for compliance and will maintain appropriate records and evidence to demonstrate that compliance.

9. LAWFUL PROCESSING AND TRANSPARENCY

9.1 The lawful basis for processing must be determined by the purpose and circumstances of the activity. Reidvale will not rely on a lawful basis merely because it is operationally convenient. Where special category data is processed, an Article 9 condition and any required Data Protection Act 2018 Schedule 1 condition must also be identified. Criminal offence data will only be processed where permitted by law and with appropriate safeguards.

9.2 Privacy notices will explain, in clear and accessible language, how Reidvale uses personal data. PECR requirements will also be considered where Reidvale carries out relevant electronic communications, marketing or similar activities.

10. DATA SHARING

10.1 Reidvale may share personal data where there is a clear purpose and lawful basis. Sharing may form part of a routine arrangement, a one-off disclosure, or an urgent or emergency response. Before sharing, Reidvale will consider necessity, proportionality, confidentiality, the recipient's role, the information required and the security of the transfer.

10.2 Regular sharing arrangements will be documented in an appropriate contract, data sharing agreement or other written arrangement according to the parties' legal roles and the level of risk. Privacy information will describe sharing where required. A data sharing agreement does not itself create a lawful basis for disclosure.

11. DATA PROCESSORS

11.1 Where Reidvale appoints a processor, it will use only processors that provide sufficient guarantees that appropriate technical and organisational measures will be implemented. A written contract meeting applicable data protection requirements must be in place before processing begins.

11.2 The processor must act only on documented instructions from Reidvale, except where the law requires otherwise.

11.3 Appropriate confidentiality and security obligations must apply.

11.4 The processor must assist Reidvale with relevant rights requests, security obligations, breach management and DPIAs as required by the contract.

11.5 Sub-processors must not be appointed without the prior specific or general written authorisation required by the contract, and equivalent data protection obligations must flow down to them.

11.6 The contract must address return or deletion of personal data and Reidvale's audit and assurance rights.

12. SECURITY INCIDENTS AND PERSONAL DATA BREACHES

12.1 All suspected information security incidents and personal data breaches must be reported immediately through Reidvale's Information Security Incident and Personal Data Breach Management Procedure. Examples include lost records or equipment, theft, cyber incidents, information sent to the wrong recipient, inappropriate access, or unauthorised use.

12.2 The Data Protection Lead will coordinate containment, investigation, risk assessment, recording and any required notification, with DPO advice and

support. Relevant IT suppliers or contractors will be involved where the incident affects systems they support.

12.3 Where a personal data breach is likely to result in a risk to individuals, Reidvale will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Where the breach is likely to result in a high risk to individuals, Reidvale will communicate it to affected individuals without undue delay unless a lawful exception applies.

12.4 Where an information security incident, personal data breach or other data protection compliance failure may be material, significant or exceptional, the Data Protection Lead will ensure that it is considered promptly in accordance with Reidvale's Notifiable Events Policy.

13. INDIVIDUAL RIGHTS

13.1 Reidvale will uphold individual rights in accordance with data protection law and its Data Subject Rights Procedure. Rights apply differently depending on the lawful basis, purpose and circumstances of processing. Reidvale will therefore assess each request on its facts rather than assume every right applies in the same way.

13.2 **Right to be informed:** Individuals will be given clear privacy information about the collection and use of their personal data.

13.3 **Right of access:** Individuals can request confirmation that their personal data is being processed and access to their personal data and relevant supplementary information.

13.4 **Right to rectification:** Inaccurate personal data will be corrected without undue delay and incomplete data completed where appropriate.

13.5 **Right to erasure:** Individuals can request erasure where the statutory conditions apply. The right is not absolute.

13.6 **Right to restriction:** Processing will be restricted where the statutory conditions apply.

13.7 **Right to data portability:** Where the right applies, eligible personal data will be provided in a structured, commonly used and machine-readable format and transmitted to another controller where technically feasible.

13.8 **Right to object:** Objections will be considered in accordance with the lawful basis and purpose of processing, including the stronger right to object to direct marketing.

13.9 **Automated decision-making safeguards:** Where Reidvale uses solely automated processing to make a significant decision about an individual, it will apply the safeguards required by current data protection law, including appropriate information and routes for human intervention, representation and challenge where applicable.

14. DATA PROTECTION COMPLAINTS

14.1 Reidvale will provide individuals with a clear way to raise complaints about how their personal data has been handled. A data protection complaint does not need to use legal terminology and must be recognised by its substance.

14.2 Reidvale will acknowledge a data protection complaint within 30 days of receipt. It will take appropriate steps to investigate the complaint without undue delay, keep the complainant informed of progress, and communicate the outcome without undue delay. Complaints will be recorded and used to identify recurring issues or improvements. Individuals will be informed of their right to complain to the ICO where appropriate.

15. DATA PROTECTION BY DESIGN AND DPIAS

15.1 Reidvale will consider data protection from the outset of new projects, systems, services, policies and material changes to processing. Appropriate measures will be designed into processing and default settings so that only personal data necessary for each purpose is processed.

15.2 Where proposed processing is likely to result in a high risk to the rights and freedoms of individuals, Reidvale will complete a DPIA before the processing begins. New policies involving personal data will be reviewed by the Data Protection Lead to determine whether DPO advice or a DPIA is required. DPIAs will be completed in accordance with Reidvale's DPIA Procedure and the DPO will be consulted where required by law.

16. INTERNATIONAL TRANSFERS

16.1 Where personal data is transferred or made accessible outside the United Kingdom, Reidvale will first confirm that the transfer is lawful and that an appropriate UK transfer mechanism, safeguard or applicable exception is in place. The assessment and supporting documentation will be proportionate to the transfer and its risks.

17. BREACH OF POLICY

17.1 Failure to comply with this policy may expose individuals and Reidvale to harm, regulatory action and reputational damage. Breaches by personnel may be addressed under Reidvale's disciplinary procedures and contractual remedies may be used where a supplier or contractor fails to meet its obligations.

18. COMMUNICATION GUIDELINES

18.1 This policy will be made available to Reidvale personnel and communicated through induction, training and relevant internal guidance. Managers must ensure that staff understand the parts of the policy that apply to their roles.

18.2 All Reidvale personnel with access to personal data will receive data protection training during induction and at least once every two years thereafter. Additional role-specific or refresher training will be provided where responsibilities or risk justify it. Personnel will be told where to obtain guidance and support.

18.3 Individuals will be informed about Reidvale's processing through appropriate privacy notices and other rights information. Relevant data protection requirements will be communicated to processors, contractors and partner organisations through contracts, instructions and sharing arrangements. The policy will be made available externally where appropriate.

19. REVIEWING AND MONITORING

19.1 The Data Protection Lead and DPO will monitor compliance through proportionate reviews and audits. Monitoring will take account of rights requests, data protection complaints, personal data breaches and near misses, DPIAs, processor assurance, training completion, records of processing, retention activity and relevant audit findings or feedback.

19.2 Significant concerns, repeated non-compliance or material residual risks will be escalated to the Management Committee. Where Reidvale decides not to follow material DPO advice, the decision, reasons, responsible risk owner and safeguards should be documented.

19.3 This policy will be reviewed at least every three years by the DPO, with the Data Protection Lead, and earlier where there is a material change in law, regulatory guidance, Reidvale's processing, organisational structure, identified risk, or lessons from an incident or complaint.

20. APPROVAL

20.1 This policy was approved by the Management Committee on Wednesday, 30th October 2026 and takes effect from that date.

20.2 Document owner: Data Protection Officer, RGDP LLP.

20.3 Operational lead: Head of Corporate and Strategy.

APPENDIX 1 – EQUALITY AND HUMAN RIGHTS IMPACT ASSESSMENT

<table>
<tr><td>Who is intended to benefit from this policy?</td><td colspan="2">☒ Existing Tenants
☒ New Tenants
☒ People on waiting lists
☒ Governing body members
☒ Staff
☒ The wider community</td></tr>
<tr><td>Which protected characteristics have been considered and how could they be affected?</td><td colspan="2">☒ Age
☒ Disability
☒ Gender reassignment
☒ Marriage and civil partnership
☒ Pregnancy and maternity
☒ Race
☒ Religion or belief
☒ Sex
☒ Sexual Orientation</td></tr>
<tr><td>If no differential impact is identified, provide a brief explanation and confirm that no further assessment is required.</td><td colspan="2">No adverse differential impact is identified. The policy establishes consistent minimum protections for personal data and applies across Reidvale's services and workforce. Some people may require adjustments to access privacy information or exercise their rights, so accessibility and communication needs must be considered. No further full assessment is required at this stage, subject to the monitoring described below.</td></tr>
<tr><td>Have those affected by the policy been involved?</td><td colspan="2">No specific external consultation is recorded for this policy. It primarily gives effect to statutory data protection duties rather than changing service eligibility or entitlement. The policy has been reviewed from a data protection and governance perspective. Feedback from rights requests, complaints, incidents, staff and service users should inform future reviews.</td></tr>
<tr><td rowspan="2">Describe the likely positive or negative impact(s) that the policy could have on the groups identified above</td><td>POSITIVE</td><td>NEGATIVE</td></tr>
<tr><td>Stronger privacy and confidentiality protections. Consistent handling of rights and complaints. Reduced risk of inappropriate disclosure or discriminatory use of sensitive information.</td><td>No inherent adverse impact is expected. Potential barriers can arise if information or rights processes are inaccessible, overly digital, or require disproportionate evidence. These risks are</td></tr>
</table>

	Clear accountability and escalation routes.	addressed through reasonable adjustments, an alternative communication routes.
What reasonable adjustments or ongoing monitoring is required?	Provide privacy and rights information in accessible formats on request. Offer appropriate non-digital or assisted routes where required. Make reasonable adjustments for disability and communication needs. Use proportionate identity checks. Monitor complaints, rights requests, incidents and feedback for evidence of unequal impact or recurring barriers.	
Which human rights will be affected by this policy	• Right to respect for private and family life, home and correspondence • Right to freedom of expression, to receive & impart information & ideas • Right to an effective remedy • Prohibition of discrimination	
Describe how this policy will deliver human rights equally.	The policy supports respect for privacy by requiring lawful, necessary, proportionate and secure processing. It requires accessible routes for people to exercise data protection rights and complain, and it requires fair treatment without discrimination. Where privacy rights interact with freedom of expression or disclosure obligations, Reidvale will assess the competing rights and legal duties on the facts rather than applying an automatic restriction.	