Privacy Policy

Approved May 2018
Next Review: 2021

Rosehill Housing
Co-operative Limited

Contents

1. Introduction

1.1 Rosehill Housing Co-operative Limited is committed to ensuring the secure and safe management of data it holds in relation to customers, employees and other individuals. Our employees are responsible for ensuring compliance with the terms of this policy, and for managing individuals' data in accordance with the approach outlined in this policy and other documentation referred to.

1.2 We need to gather and use certain information about individuals. These can include customers (tenants, factored owners, housing applicants, etc.), employees and other individuals that we have a relationship with. We manage 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 our duties in processing that data, and the purpose of this Policy is to set out our approach for the management of such data.

2. Legislation

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

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

- the General Data Protection Regulation (EU) 2016/679 ("the GDPR");
- the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
- any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, 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

3. Personal Data

3.1 We hold 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 we hold and process is detailed within the Fair Processing Notices (also referred to as Privacy Notices).

3.1.1 "Personal Data" is that from which a living individual can be identified either by that data alone, or in conjunction with other data we hold.

3.1.2 We also hold 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. Processing of Personal Data

4.1 We are permitted to process Personal Data on behalf of data subjects provided we are doing so on one or more of the following grounds:

- Processing with the consent of the data subject (see clause 4.4);
- Processing is necessary for the performance of a contract between us and the data subject or for entering into a contract with the data subject;
- Processing is necessary for our 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 our official authority; or
- Processing is necessary for the purposes of legitimate interests.

4.2 Fair Processing Notices (Privacy Notices)

4.2.1 Privacy Notices for Customers

4.2.1.1 We have produced a Privacy Notice which we are required to provide to all customers whose Personal Data is held by us. The Notice sets out the Personal Data processed by us and the basis for that processing. The Privacy Notice is provided to all of our customers at the outset of processing their data and they will be advised of the terms of the Privacy Notice when it is provided to them.

4.2.2 Privacy Notices for Employees

4.2.2.1 We hold and process Employee Personal Data, details of the data held and the processing of that data is contained within the Employee

Privacy Notice. The Notice is provided to employees at the same time as their contract of employment.

4.3 Consent

4.3.1 We will require to use Consent as a ground of processing from time to time when processing Personal Data. We will use this ground where no other alternative ground for processing is available. In the event that we require to obtain consent to process a data subject's Personal Data, we will 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 if willing to consent. Any consent obtained by us must be for a specific and defined purpose (i.e. general consent cannot be sought).

4.4 Processing of Special Category Personal Data or Sensitive Personal Data

4.4.1 In the event that we process Special Category Personal Data or Sensitive Personal Data, we will do so in accordance with one of the following grounds of processing:

- 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; and
- Processing is necessary for reasons of substantial public interest.

5. Data Sharing

5.1 We share data with various third parties for numerous reasons in order that our day to day activities are carried out in accordance with our relevant policies and procedures. In order that we can monitor compliance by these third parties with Data Protection laws, we require the third party organisations to enter in to an Agreement with us governing the processing of data, security measures to be implemented and responsibility for breaches.

5.2 Data Sharing – Data Controllers

5.2.1 We share Personal Data from time to time with third parties who require to process personal data that we process as well. Both we and the third party will be processing that data in our individual capacities as data controllers.

5.2.2 Where we share in the processing of personal data with a third party organisation (e.g. for processing of employees' pension), we shall require the third party organisation to enter in to a Data Sharing Agreement with us.

5.3 Data Sharing - Data Processors

5.3.1 A data processor is a third party entity that processes personal data on our behalf, and are frequently engaged where we outsource services (e.g. maintenance and repair works to our houses).

5.3.1.1 A data processor must comply with Data Protection laws. Our data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify us if a data breach is suffered.

5.3.1.2 If a data processor wishes to sub-contract their processing, prior written consent must be obtained from us. Where there is a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

5.3.1.3 Where we contract with a third party to process personal data held by us, we shall require the third party to enter in to a Data Processor Agreement with us.

6. Data Storage and Security

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

6.2 Paper Storage

6.2.1 If Personal Data is stored on paper it must be kept in a secure place where unauthorised personnel cannot access it, usually in locked cabinets or cupboards. 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 secure 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 our storage provisions.

6.3 Electronic Storage

6.3.1 Personal Data stored electronically must also be protected from unauthorised use and access, this will usually be achieved by the use of restricted access arrangements and passwords. Personal Data should be password protected when being sent internally or externally to our data processors or those with whom we have entered in to a Data Sharing Agreement. Personal data must never be stored on removable media (CD, DVD, USB memory stick). Personal Data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

7. Website Use

7.1 We collect personal information from our website and we take steps to safeguard that information.

7.2 We collect the following information:

- Any personal details customers type in and submit, such as name, address, email address, etc;
- Customers' IP address (this is customers' computer's individual identification number) which is automatically logged by our web server. This is used to note customers interest in our website;
- Customers' preferences and use of email updates, recorded by emails we send them (if they select to receive email updates on products and services).

7.3 What we do with the personal information collected:

- Any personal information we collect from our website will be used in accordance with the General Data Protection Regulation (EU) 2016/679 and other applicable laws;

- We retain personal data for the purposes of either sending information customers have specifically requested from our site or in certain cases we may use customers' email addresses to send them information on our other products and services. In such cases, customers will be offered the option to opt-in for receiving this information;

- We do not distribute any personal details or gathered data to third parties.

7.4 Customers' Rights

7.4.1 Customers can ask us to update or remove any personal information we hold by emailing us at admin@rosehillhousing.co.uk or by writing to us at the address below.

Rosehill Housing Co-operative Limited
250 Peat Road
Glasgow
G53 6SA

8. Breaches

8.1 A data breach can occur at any point when handling Personal Data and we have 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 Section 8.3.

8.2 Internal Reporting

8.2.1 We take 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, or we become aware of the breach (if later), and in any event no later than six (6) hours after it has occurred or we become aware of it having occurred (if later), the Depute Director must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach has on any data subject(s);
- Rosehill must seek to contain the breach by whatever means available;
- The Depute Director 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 Section 8;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements.

8.3 Reporting to the ICO

8.3.1 The Depute Director 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 us becoming aware of the breach. The Depute Director must also consider whether it is appropriate to notify those data subjects affected by the breach.

9. Data Protection Officer

9.1. A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by Rosehill with Data Protection laws.

9.2 We have elected to **not** appoint a Data Protection Officer at this time. In the meantime, our Depute Director will be responsible for:

- monitoring our compliance with Data Protection laws and this Policy;
- co-operating with and serving as our contact for discussions with the ICO;
- reporting breaches or suspected breaches to the ICO and data subjects in accordance with Section 8.

10. Data Subject Rights

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

10.2 Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to us processing their data. These rights are notified to our tenants and other customers in our Fair Processing Notice.

10.3 Subject Access Requests

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

- 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 we do not hold the personal data sought by the data subject, must confirm that we do not hold any personal data sought by 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.

10.4 The Right to be Forgotten

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

10.4.2 Each request received by us 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 Depute Director will have responsibility for accepting or refusing the data subject's request in accordance with Section 10.4 and will respond in writing to the request.

10.5 The Right to Restrict or Object to Processing

10.5.1 A data subject may request that we restrict our processing of the data subject's Personal Data, or object to the processing of that data.

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

10.5.2 Each request received by us 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 Depute Director will have responsibility for accepting or refusing the data subject's request in accordance with Section 10.5 and will respond in writing to the request.

11. Privacy Impact Assessments ("PIAs")

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

11.2 We 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 we will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data

11.3 We will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The Depute Director is responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the Depute Director within five (5) working days.

12. Archiving, Retention and Destruction of Data

12.1 We cannot store and retain Personal Data indefinitely. We must ensure that Personal data is only retained for the period necessary. We shall ensure that all Personal data is archived and destroyed in accordance with the periods specified within the table at Appendix 1.

13. Related Documents

13.1 The following is a list of related documents that support the implementation of this Policy by our employees.

- Email and Internet Usage Policy
- Electronic Communication and ICT Security Policy
- Subject Access Requests Procedure

Appendix 1

Retention Periods for Personal Data

The table below sets out retention periods for Personal Data held and processed by Rosehill about customers (including tenants, factored owners, and waiting list applicants) and employees. It is intended to be used as a **guide only**. However, not all Personal Data can be processed and kept for the same period of time, and this will vary depending on the individual circumstances of each person whose Personal Data we hold.

Type of Record	Retention Period
Membership Records	
• Application Forms	5 years from when membership ends
• Share Certificate Stubs	Permanently
• Live Share Register	Permanently
• Former Members Register	5 Years from when membership ends
Current Tenant/House Files e.g. tenancy agreements; applications for tenancy matters such as alterations/improvements, garden assistance and adaptations; Housing Benefit Notifications; arrears letters; anti-social behaviour/neighbour complaints; records about sex offenders/offenders and ex-offenders; various correspondence	Minimum of 5 years up to duration of tenancy
• Landlord's Gas Safety Records	2 calendar years from the issue of the current certificate
• Repairs Orders/Maintenance Requests (kept on main IT system property records)	5 years on current property records, thereafter will be archived, with tenants' names redacted.
Former Tenant/House Files e.g. tenancy agreements, Housing Benefit Notifications, arrears letters, anti-social behaviour/neighbour complaints	5 years
Housing Applications e.g. main application form, medical form, supporting documentation,	5 years from when removed from waiting list for various reasons e.g. we have rehoused the applicant, removed at applicant's request, etc.
Factored Owner Files e.g. details of ownership, owners contact details, emergency contact details.	1 year following change of ownership or termination of factoring service except where there is a balance on the owner's account.

	Emergency contact details removed at change of ownership or termination of factoring service.
Employee Personnel/HR Files e.g. personal contact details, performance reviews, training records, health records, absence records, employment contracts, parental leave, documents proving the right to work in UK	Minimum of 5 years up to duration of employment
Other Employee Files • Records relating to working time	2 Years from the date on which they were made
Other Employee Data (financial) • Payroll • Income tax, NI returns, correspondence with tax office • Retirement benefits schemes • Statutory maternity/paternity and adoption pay records, calculations, certificates (e.g. MAT 1Bs) • Statutory Sick Pay records, calculations • Wages/Salary records	7 years for all such financial data
Former Employee Personnel/HR Files ☐ Job Application Form ☐ Personal Contact Information (including emergency contact details) ☐ Documents proving the right to work in UK ☐ Driving Licence, Car Insurance and MOT details	5 years from when employment ends Removed at point employment ends Removed at point employment ends 2 years after employment ceases Removed at point employment ends
Other Former Employee Files • Redundancy details, calculations of payments, refunds • Redundancy facts	6 years from the date of the redundancy 6 years
Recruitment Files • Application forms of non-shortlisted candidates	6 months

• Application forms of shortlisted candidates, interview notes	1 Year *successful candidate's paperwork will be transferred to their employee Personnel/HR file