PRIVACY POLICY

Date Approved: January 2020

Next Review: January 2023

Contents

1. Introduction

Spire View Housing Association Limited (hereinafter the "Association") 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.

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).

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. Legislation

It is a legal requirement that the Association 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 General Data Protection Regulation (EU) 2016/679 ("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) the Data Protection Act 2018 ("the 2018 Act"); and

(d) 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. Data

3.1 The Association holds a variety of data relating to individuals, including customers and employees (also referred to as Data Subjects). Data which can identify living Data Subjects is known as Personal Data. The Personal Data held and processed by the Association is detailed within the Association's Fair Processing Notice which is distributed to you at the outset of collecting and processing your data.

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 held by the Association.

3.1.2 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 known as Special Category Personal Data or Sensitive Personal Data.

4. Processing of Personal Data

4.1 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 4.4 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; or
- 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;

4.2 Fair Processing Notice

4.2.1 The Association has produced a Fair Processing Notice (FPN) (Appendix 1) 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.

4.2.2 The Fair Processing Notice 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

4.3 Employees

4.3.1 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 prospective Employees at application stage.

4.3.2 A copy of any employee's Personal Data held by the Association is available upon request by that employee from the Association's Data Protection Officer (see part 8).

4.4 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 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). Where consent is being relied on, Data Subjects are free to withhold their consent or withdraw it at any future time.

4.5 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 rely on an additional ground for processing in accordance with one of the Special Category grounds. These include, but are not restricted to, the following:

- 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, social security, or social protection law;
- Processing is necessary for health or social care;
- 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 under law.

All the grounds for processing Special Category Personal Data are set out in Article 9(2) of the GDPR and expanded on in the 2018 Act.

5. Data Sharing

5.1 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 may 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.

5.2 Data Sharing

5.2.1 Personal Data is from time to time shared amongst the Association and third parties who require to process the same Personal Data as the Association. Whilst the Association and third parties may jointly determine the purposes and means of processing, both the Association and the third party will be

processing that data in their individual capacities as data controllers.

5.2.2 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.

5.3 Data Processors

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).

5.3.1 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.

5.3.2 If a data processor wishes to sub-contract 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.

5.3.3 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 Processor Agreement with the Association.

6. Data Storage and Security

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

6.1 Paper Storage

If Personal Data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. Employees should ensure that no Personal Data is left in a place 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 the Association's storage provisions.

6.2 **Electronic Storage**

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 encrypted or password protected and 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.

7. Breaches

7.1 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.

7.2 Internal Reporting

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 it becomes known that a breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the Association's 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 whichever means available;
- The DPO must consider whether the breach is one which requires to be reported to the ICO and to the Data Subjects affected and, if appropriate, will do so in accordance with this clause 7;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

7.3 Reporting to the ICO

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 becoming aware of the breach or potential breach. The DPO will also consider whether it is appropriate to notify those Data Subjects affected by the breach.

8. Data Protection Officer ("DPO")

8.1 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 appointed a Data Protection Officer (DPO) as required. The Association's DPO's details are Gillian Spence, GillianSpence@spireview.org.uk and are also noted on the Association's website and contained within the Association's Fair Processing Notices.

8.2 The DPO will be responsible for:

8.2.1 Monitoring the Association's compliance with Data Protection laws and this Policy;

8.2.2 Co-operating with and serving as the Association's contact for communication with the ICO; and

8.2.3 Reporting breaches or suspected breaches to the ICO and Data Subjects in accordance with Part 7 hereof.

9. Data Subject Rights

9.1 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.

9.2 Data Subjects have a right to request a restriction of processing their data, a right to request erasure of their Personal Data, 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. Such rights are subject to qualification and are not absolute.

9.3 **Subject Access Requests**

Data Subjects are permitted to view their Personal 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:

9.3.1 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.

9.3.2 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

9.3.3 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.

9.4 **The Right to Erasure**

9.4.1 A Data Subject can exercise their right to erasure by submitting a request to the Association seeking that the Association erase the DataSubject's Personal Data in its entirety.

9.4.2 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.

9.4.3 Requests for Erasure will be considered and responded to by the Association within one month of the date of receipt of the request.

9.5 **The Right to Restrict or Object to Processing**

9.5.1 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.

9.5.1.1 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.

9.5.2 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 9.5 and will respond in writing to the request.

9.6 The Right to Rectification

9.6.1 A Data Subject may request the Association to have inaccurate Personal Data rectified. If appropriate, a Data Subject may also request the Association to have incomplete Personal Data completed.

9.6.2 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 9.6 and will respond in writing to the request.

10. Privacy Impact Assessments ("PIAs")

10.1 These are a means of assisting the Association in identifying and reducing the risks that our operations have on personal privacy of Data Subjects.

10.2 The Association shall:

10.2.1 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

10.2.2 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

10.3 The Association will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced or mitigated. The 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.

11. 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 terms of their retention guidelines (Appendix 2).

Appendix 1

Spire View Housing Association Limited

GDPR Fair Processing Notice

(How we use your personal information)

This notice explains what information we collect, when we collect it and how we use this. During the course of our activities we will process personal data (which may be held on paper, electronically, or otherwise) about you and we recognise the need to treat it in an appropriate and lawful manner. The purpose of this notice is to make you aware of how we will handle your information.

Who are we?

Spire View Housing Association Limited, a Scottish Charity (Scottish Charity Number SC033266), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 2295RS and having their Registered Office at 43 Tharsis Street, Roystonhill, Glasgow, G21 2JF ("**we**" or "**us**") take the issue of security and data protection very seriously and strictly adhere to guidelines published in the Data Protection Act of 2018 ("the 2018 Act") and the General Data Protection Regulation (EU) 2016/679 ("GDPR"), together with any domestic laws subsequently enacted.

We are registered as a Data Controller with the Office of the Information Commissioner under registration number Z6952147 and we are the data controller of any personal data that you provide to us.

Our Data Protection Officer is Gillian Spence, GillianSpence@spireview.org.uk 0141 559 5644

Any questions relating to this notice and our privacy practices should be sent to Gillian Spence, GillianSpence@spireview.org.uk 0141 559 5644

How we collect information from you and what information we collect

We collect information about you to enable us to perform our contractual obligations. You, in turn, are under a contractual obligation to provide the data requested from you to enable performance of the contract (e.g. the tenancy agreement you are party to):

- when you apply for housing with us, become a tenant, request services/ repairs, enter in to a factoring agreement with ourselves howsoever arising or otherwise provide us with your personal details
- when you apply to become a member;
- from your use of our online services, whether to report any tenancy or factoring related issues, make a complaint or otherwise;
- from your arrangements to make payment to us (such as bank details, payment card numbers, employment details, benefit entitlement and any other income and expenditure related information);
- from CCTV images captured by our CCTV cameras

We collect the following information about you. If you are a tenant, under the terms of the tenancy agreement, you are required to provide us with the following information.

- name;
- address;
- telephone number;
- e-mail address;
- National Insurance Number;
- Demographic information – ethnicity, race, age, date of birth, nationality;
- Share membership number;
- Payment card reference;
- Next of Kin;
- Household members;
- Bank Account details;
- Payment Card Numbers;
- Employment details, taxpayer identification numbers, tax reference codes;

- Medical Information to process an application/transfer application/undertake sheltered duties/process medical adaptation requests;
- Membership details;
- Hearing impairments;
- Health & safety information to process insurance claims;
- Disability;
- Benefits information from DWP/Housing Benefit Department;
- Passport or driving licence numbers;

We receive the following information from third parties:

- Benefits information, including awards of Housing Benefit/ Universal Credit and any overpayments requests
- Payments made by you to us;
- Complaints or other communications regarding behaviour or other alleged breaches of the terms of your contract with us, including information obtained from Police Scotland, Local Authorities or other housing providers;
- Reports as to the conduct or condition of your tenancy, including references from previous tenancies, and complaints of anti-social behaviour;
- Health related information

Why we need this information about you and how it will be used

We need your information and will use your information:

- to enable us to enter a contract with you;
- to undertake and perform our obligations and duties to you in accordance with the terms of our contract with you;
- to enable us to supply you with the services and information which you have requested;
- to enable us to respond to your repair request, housing application and complaints made;
- to analyse the information we collect so that we can administer, support and improve and develop our business and the services we offer;
- to contact you in order to send you details of any changes to our services which may affect you;

- for all other purposes consistent with the proper performance of our operations and business, including newsletters, website and our annual report;
- to protect your interests and / or the interest of others;
- to meet our legal obligations; and
- to contact you for your views on our products and services.

Sharing of Your Information

The information you provide to us will be treated by us as confidential and will be processed within the UK/EEA.

We may disclose your information to other third parties who act for us for the purposes set out in this notice or for purposes approved by you, including the following:

- if we enter into a joint venture with or merged with another business entity, your information may be disclosed to our new business partners or owners;
- if we instruct repair or maintenance works, your information may be disclosed to any contractor;
- if we are investigating a complaint, information may be disclosed to Police Scotland, Local Authority departments, Scottish Fire & Rescue Service and others involved in any complaint, whether investigating the complaint or otherwise;
- if we are updating tenancy details, your information may be disclosed to third parties (such as utility companies and the Local Authority);
- if we are investigating payments made or otherwise, your information may be disclosed to payment processors, Local Authority and the Department for Work & Pensions;
- if we are conducting a survey of our products and/ or service, your information may be disclosed to third parties assisting in the compilation and analysis of the survey results;
- to obtain legal advice or take legal action;

- to adhere to our statutory requirements to report to the Scottish Housing Regulator and notify the Local Authority in the event of court proceedings being raised to recover possession of a tenancy;
- if you wish to access our Welfare Rights service;
- to allow you to make payment to us through third party organisations;
- to Sheriff Officers, debt collection agencies and tracing agents in connection with any enforcement action;
- if we are processing any insurance claim made against us we will forward the claim to our insurers

Unless we have a lawful basis for disclosure, we will not otherwise share, sell or distribute any of the information you provide to us without your consent.

Transfers outside the UK and Europe

We will only store your information within the UK and EEA.

Security

When you give us information we take steps to make sure that your personal information is kept secure and safe.

We store your data securely in both electronic and paper format. Where a physical copy of any data is stored it is stored in a locked filing cabinet or drawer. Electronic copies of personal data are stored on our system which is accessed through password entry. Any information transmitted electronically is transmitted securely and password protected where appropriate.

Further information regarding security and storage of data can be found in our Privacy Policy.

How long we will keep your information

We review our data retention periods regularly and will only hold your personal data for as long as is necessary for the relevant activity, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you.

Our full retention guidelines schedule is contained within our Privacy Policy, a copy of which can be obtained from our office or on our website at www.spireview.org.uk

Your Rights

You have the right at any time to:

- ask for a copy of the information about you held by us in our records;
- ask us to correct any inaccuracies of fact in your information;
- request that we restrict your data processing
- data portability
- Rights related to automated decision making including profiling
- make a request to us to delete what personal data of your we hold; and
- object to receiving any marketing communications from us.

  If you would like to exercise any of your rights above please contact our DPO Gillian Spence on GillianSpence@spireview.org.uk 0141 559 5644. **You should note that your rights under the GDPR and 2018 Act are not absolute and are subject to qualification.**

- If you have any complaints about the way your data is processed or handled by us, please contact Gillian Spence on GillianSpence@spireview.org.uk 0141 559 5644

If you remain unsatisfied after your complaint has been processed by us, you also have the right to complain to the Information Commissioner's Office in relation to our use of your information. The Information Commissioner's contact details are noted below:

45 Melville Street, Edinburgh, EH3 7HL

Telephone: 0303 123 1115

Email: Scotland@ico.org.uk

The accuracy of your information is important to us - please help us keep our records updated by informing us of any changes to your email address and other contact details.

Appendix 2

Data Retention Periods

The table below sets out retention periods for Personal Data held and processed by the Association. It is intended to be used as a guide only. The Association recognises that not all Personal Data can be processed and retained for the same duration, and retention will depend on the individual circumstances relative to the Data Subject whose Personal Data is stored.

Type of record	Suggested retention time
Membership records	5 years after last contact
Personal files including training records and notes of disciplinary and grievance hearings	5 years to cover the time limit for bringing any civil legal action, including national minimum wage claims and contractual claims
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of the redundancy
Application forms, interview notes	Minimum 6 months to a year from date of interviews. Successful applicants documents should be transferred to personal file.
Documents proving the right to work in the UK	2 years after employment ceases.
Facts relating to redundancies	6 years if less than 20 redundancies. 12 years if 20 or more redundancies.
Payroll	3 years after the end of the tax year they relate to
Income tax, NI returns, correspondence with tax office	At least 3 years after the end of the tax year they relate to
Retirement benefits schemes – notifiable events, e.g. relating to incapacity	6 years from end of the scheme year in which the event took place
Pensioners records	12 years after the benefit ceases
Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence	3 years after the end of the tax year to which they relate
Parental Leave	18 years
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years
Wages/salary records,	6 years

expenses, bonuses	
Records relating to working time	2 years from the date they were made
Accident books and records and reports of accidents	3 years after the date of the last entry
Health and Safety assessments and records of consultations with safety representatives and committee	Permanently
Health records	During employment and 3 years thereafter if reason for termination of employment is connected to health
Board Members Documents	5 years after cessation of membership
Documents relation to successful tenders	5 years after end of contract
Documents relating to unsuccessful form of tender	5 years after notification
Applicants for accommodation	5 years
Housing Benefits Notifications	Duration of Tenancy
Tenancy files	Duration of Tenancy
Former tenants' files (key info)	5 years
Third Party documents re care plans	Duration of Tenancy
Records re offenders. Ex-offenders (sex offender register)	Duration of Tenancy
Lease documents	5 years after lease termination
ASB case files	5 years/end of legal action
Board meetings/residents' meetings	1 year
Minute of factoring meetings	Duration of appointment