# Shire Housing Association

# Data Protection Policy

## 1. Introduction

Shire Housing Association (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 process data correctly; 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 Data Protection Act 2018 (which brings the GDPR into UK law);

(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 other 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) which is known as Personal Data. The Personal Data held and processed by the Association is detailed within the Employee Fair Processing Notice and the general public Fair Processing Notice.

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 "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;
- 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; or
- Processing is necessary for the purposes of the Association's legitimate interests or the legitimate interests of a third party, provided that such processing does not override the individual rights and freedoms of the data subject.

**4.2 Fair Processing Notice**

4.2.1 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.

4.2.2 The Fair Processing Notices set out the Personal Data processed by the Association and the basis for that Processing. The general or public Fair Processing Notice is provided to all of the Association's customers at the outset of processing their data, and the Employee Fair Processing Notice is provided to all employees at the outset of their employment.

### 4.3 Employees

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 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, or take some other form of affirmative action, 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).

### 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 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.

It is worth noting that the UK Data Protection Act 2018 defines what should be considered to be a "substantial public interest" for the purposes of processing Special Category Personal Data or criminal conviction data. Most processing of Special Category Personal Data by the Association will fall within scope of this "substantial public interest" ground.

## 5. Data Sharing

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.

### 5.1 Data Sharing

5.2.1 Personal data is from time to time shared amongst the Association and third parties who require to process personal data for their own separate purposes. 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. sharing with other housing associations or sharing with other public bodies), it shall require the third party organisation to enter in to a Data Sharing

Agreement with the Association in accordance with the terms of the model Data Sharing Agreement set out in Appendix 3 to this Policy.

### 5.2 Data Processors

A data processor is a third party entity that processes personal data on behalf of the Association in the delivery of its services to the Association (e.g. payroll, maintenance and repair works).

5.2.1 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 occurs.

5.2.2 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.

5.2.3 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 Protection Addendum with the Association in accordance with the terms of the model Data Protection Addendum set out in Appendix 4 to this Policy.

## 6. Data Storage and Security

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

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 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 with appropriate access controls in place.

## 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 serious 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 event of a breach will take the following steps:

- As soon as the Association becomes aware that a breach has or may have occurred, the DPO must be notified of the breach or potential breach and be provided with all information available about the breach or potential breach;
- 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

7.3 **Reporting to the ICO**

The DPO will require to report any breaches which pose a serious 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, or the ICO may instruct the Association 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 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.

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 discussions with the ICO

8.2.3 Reporting breaches or suspected breaches to the ICO and data subjects in accordance with clause 7 hereof.

## 9. Data Subject Rights

9.1 Certain rights are provided to data subjects under the GDPR. Data Subjects are entitled to a copy of 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 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.

9.3 **Subject Access Requests**

Data Subjects are permitted to a copy of their data held by the Association upon making a request to do so (a Subject Access Request) free of charge. 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.

9.3.1 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.

9.3.2 Where the personal data comprises data relating to other data subjects, the Association must consider: (i) whether it has the consent of those other data subject to release their data; or (ii) whether it would be reasonable in all the circumstances to release their data. If the Association does not have consent and does not consider it reasonable to release this data, then steps must be taken to remove or redact any third party data from the information to be released to the requester.

9.3.3 Where the Association does not hold the personal data sought by the data subject, the Association 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 be Forgotten**

9.4.1 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.

9.4.2 The right to be forgotten is not an absolute right. Where the Association is legally bound to retain certain information, or it has a legitimate interest to retain information, it is entitled to refuse a request to be forgotten. Each request received by the Association will require to be considered on its own merits. 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. Where a request is refused, the DPO will explain the rationale of this decision when responding to the requester.

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. 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.

## 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 Special Categories of Personal Data, or the implementation of a new IT system for storing and accessing Personal Data which may give rise to security risks, or any processing which requires Personal Data to be transferred to a location outside of the European Economic Area; 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. 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 periods specified at Appendix 5.

**Appendices**

Appendix 1- Fair Processing Notice;

Appendix 2- Employee Fair Processing Notice; (issued separately to staff)

Appendix 3- Data Sharing Agreement; (available on request)

Appendix 4- Data Protection Addendum (available on request)

Appendix 5- Data Retention

**Appendix 1**

## Shire Housing Association
## GDPR Fair Processing Notice
## (How We Use Your Personal Information)

This Fair Processing Notice explains what information Shire Housing Association collects about you, when we collect it and how we use this. It complies with Data Protection legislation including the General Data Protection Regulation. During the course of our business activities we will process personal data, which may be held on paper, or electronically.

If you have any queries about this Fair Processing Notice, how we use your personal information, or if you require a copy of this Fair Processing Notice in an alternative format (such as large print, Braille or an audio recording), you can contact Shire Housing Association at:

Shire Housing Association
Netherthird House
Cumnock, Ayrshire
KA18 3DB
info@shirehousing.com
01290 421130

Our Data Protection Officer is Jim Munro, Director. Any questions relating to this notice and our privacy practices should be sent to ***dp@shirehousing.com***

We collect information about you:

- 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 of the Association;
- when you apply for a job;
- from your use of our online services, whether to report any tenancy/ factor related issues, make a complaint or otherwise;
- our website also gathers information from on-line cookies;
- CCTV images if you visit our office; and

- 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).

We collect the following information about you:

- name;
- address;
- telephone number;
- e-mail address;
- National Insurance Number;
- Next of Kin;
- proof of your identity / photo ID;
- health information including disability; and
- ethnicity.

We receive the following information from third parties:

- Benefits information, including awards of Housing Benefit/ Universal Credit;
- 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;
- Reports as to the conduct or condition of your tenancy, including references from previous tenancies, and complaints of anti-social behaviour;
- Health information from East Ayrshire Health and Social Care Partnership. For example, to allow us to progress adaptations to your home;
- Welfare information about you or your family from East Ayrshire Council Social Services; and
- Enquiries on your behalf and with your consent from local councillors, MSPs and MPs.

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

We need your information and will use your information:

- to undertake and perform our obligations and duties to you in accordance with the terms of our contract with you- through a Scottish Secure Tenancy Agreement, or a Written Statement of Service (through the Property Factors (Scotland) Act 2011);
- 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 or supplies which may affect you; and
- to contact you for your views on our products and services.

## What is our legal basis for using your personal information?

We will only use your personal information where it is permitted by law and where:

- we need to use your personal information to perform our contract with you;
- we need to use your personal information to comply with our legal or regulatory obligations as a housing association and registered charity;
- you have given us your consent to use your personal information for a particular purpose (if consent is needed we will ask this from you separately); and
- it is in our legitimate interests to process your personal information (such as our legitimate interests to identify improvements in our services to you, and our legitimate interests to obtain feedback on our services) and there is no disadvantage to you or risk to your personal information.

If you do not provide us with the personal information we request from you, we may not be able to offer you our services, or continue to administer any services that you have with us.

## Sharing of Your Information

The information you provide to us will be treated by us as confidential and will be processed only by our employees or third party suppliers based within the UK/EEA.

We may disclose your information to other third parties 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 merge 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 Local Authority);
- If we are investigating payments made or otherwise, your information may be disclosed to payment processors, Local Authority and the Department of 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

Unless required to do so by law, 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

The information you provide to us will only be transferred and/or stored 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 including:

- Network passwords for data servers;
- Lock screen with password activation;
- Each authorised user has a private password known only to themselves to access Capita Housing Management Software;
- Regular prompts for password amendments
- Application Permissions and access restricted to those who require
- Internet Firewall;
- Anti-virus/malware software;
- Password protected mobile devices;
- Secure office environment including CCTV coverage;
- Strict control of the use of memory sticks; and
- Clear Desk Policy-Ensuring no personal data is left on staff desks when the office is closed.

## 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. Generally, we will hold your information for the duration of your tenancy.

After the relevant retention period has expired, the information will be securely destroyed or otherwise put beyond use.

Our Information Retention and Deletion Policy is included at Appendix 5.

## 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
- require us to correct any inaccuracies in your information
- make a request to us to delete what personal data of your we hold
- object to receiving any marketing communications from us
- ask for a copy of your personal information to be provided to you or a third party in a portable format
- where we have sought your consent to process your personal information, you have a right to withdraw your consent at any time

If you would like to exercise any of your rights above please contact us at info@shirehousing.com.

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 Office contact details are noted below:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
https://ico.org.uk/concerns/
0303 123 1113

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 5

## 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.

We will generally keep your information for the following minimum periods:

| | |
|---|---|
| Applications for accommodation | Duration of Tenancy |
| Housing Benefits Notifications/Universal Credit Notifications | Duration of Tenancy |
| Tenancy files | Duration of Tenancy |
| Former tenants' files (key info) | Duration of Tenancy unless debt left on account |
| 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 |
| Membership records | Permanently |
| Personal files including training records and notes of disciplinary and grievance hearings | 6 years after employment ends. 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 | 6 months date of interviews for unsuccessful applicants. Successful applicants' documents should be transferred to personal file. |
| Documents proving the right to work in the UK | Duration of employment. |
| Facts relating to redundancies | 6 years if less than 20 redundancies. 12 years if 20 or more redundancies. |
| Payroll | 6 years from termination date |
| Income tax, NI returns, correspondence with tax office | 6 years from termination date |
| Retirement benefits schemes – notifiable events, e.g. relating to incapacity | 6 years from termination date |
| Pensioners records | 6 years from termination date |
| Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence | 6 years from termination date |
| Parental Leave | 18 years |

| | |
|---|---|
| Statutory Sick Pay records, calculations, certificates, self-certificates | 6 years from termination date |
| Wages/salary records, expenses, bonuses | 6 years |
| 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 | During employment |
| Health records | During employment |
| Board Members Documents | Permanently |
| Documents relation to successful tenders | 5 years after end of contract |
| Documents relating to unsuccessful form of tender | 6 months after notification and standstill period expires and if no challenges received. If challenge received retain for 5 years after notification. |
| Board meetings/residents' meetings | Permanently |
| Minute of factoring meetings | Duration of appointment |

after which this will be destroyed if it is no longer required for the reasons it was obtained.

Our full retention schedule is available at www.shirehousing.co.uk or at our office.