HOMES FOR LIFE HOUSING PARTNERSHIP

Privacy Policy

Date Issued:	25th May 2018 (Version 1)
Due Review Date:	May 2019
Number of Pages:	14 pages (including frontispiece) *(excluding Appendices)*
Objective:	To describe the Company's management of Personal Data under the General Data Protection Regulation (EU) 2016 (GDPR). *(This replaces the Company's previous Data Protection Policy.)*
Responsible:	Business Manager

Contents

1. Introduction

Homes for Life Housing Partnership (hereinafter the "Company") is committed to ensuring the secure and safe management of data held by the Company in relation to customers, staff, and other individuals. The Company'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 Company needs to gather and use certain information about individuals. These can include customers (tenants, factored owners etc.), employees and other individuals that the Company has a relationship with. The Company 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 Company's duties in processing that data, and the purpose of this Policy is to set out the procedures for the management of such data.

Appendix 1 hereto details the Company's related policies.

2. Legislation

It is a legal requirement that the Company process data correctly; the Company 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); and

(c) 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 Company 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 Company as a Service Provider is detailed within the Privacy Notice: General- at Appendix 2 hereto. The Personal Data held and processed by the Company as an Employer is detailed within the Fair Processing Notice: Employment- at Appendix 3 hereto. All Employees have been provided with a Data Protection Addendum of the Terms of and Conditions of Employment- at Appendix 4 hereto.

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 Company.

3.1.2 The Company 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 Company 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 Company and the data subject or for entering into a contract with the data subject;
- Processing is necessary for the Company'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 Company's official authority; or
- Processing is necessary for the purposes of legitimate interests.

4.2 Privacy Notice

4.2.1 The Company has produced a Privacy Notice: General (PN) which it is required to provide to all customers whose Personal data is held by the Company. That PN must be provided to the customer from the outset of processing their Personal Data and they should be advised of the terms of the PN when it is provided to them.

4.2.2 The Privacy Notice: General- at Appendix 2 hereto, sets out the Personal Data processed by the Company as a Service Provider and the basis for that Processing. This document is provided to all the Company's customers at the outset of processing their data.

4.3 Workers

4.3.1 Worker Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by the Company. Details of the data held, and processing of that data is contained within the Privacy Notice: Worker- at Appendix 3 hereto. This is provided to workers at appointment. All Employees have been provided with a Data Protection Addendum of the Terms of and Conditions of Workers - at Appendix 4 hereto.

4.3.2 A copy of any worker's Personal Data held by the Company is available upon written request by that worker from the Company's Privacy Administrator (*see part 8 below for further detail).*

4.4 Consent

Consent as a ground of processing will require to be used from time to time by the Company when processing Personal Data. It should be used by the Company where no other alternative ground for processing is available. If the Company 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 Company 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 Company processes Special Category Personal Data or Sensitive Personal Data, the Company 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.

5. Data Sharing

5.1 The Company 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 Company's relevant policies and procedures. In order that the Company can monitor compliance by these third parties with Data Protection laws, the Company will require the third-party organisations to enter in to an Agreement with the Company 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 Company and third parties who require to process personal data that the Company process as well. Both the Company and the third party will be processing that data in their individual capacities as data controllers.

5.2.2 Where the Company shares in the processing of personal data with a third party organisation (e.g. for processing of an employees' pension), it shall require the third party organisation to enter in to a Data Sharing Agreement with the Company. This will be in accordance with the terms of the model Data Sharing Agreement set out in Appendix 5 hereto or an agreed alternative offering the necessary assurance and protection.

5.3 Data Processors

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

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

5.3.2 If a data processor wishes to sub-contact their processing, prior written consent of the Company 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 Company contracts with a third party to process personal data held by the Company, it shall require the third party to enter in to a Data Protection Addendum with the Company in accordance with the terms of the model Data Protection Addendum set out in Appendix 6 hereto, or an agreed alternative offering the necessary assurance and protection .

6. Data Storage and Security

All Personal Data held by the Company 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 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 Company'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 Company's data processors or those with whom the Company has entered in to a Data Sharing Agreement. If Personal data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be stored securely at all times when not being used. Personal Data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

7. Breaches

7.1 A data breach can occur at any point when handling Personal Data and the Company 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 Company takes the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as any breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, or of anyone becoming aware of such occurrence, the Privacy Administrator (*see part 8 below for further detail)* 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 Company will seek to contain the breach by whatever means available;
- The Privacy Administrator will liaise with the Business Manager to determine whether the breach is one which requires to be reported

to the Information Commissioner's Office (''ICO'') and data subjects affected and do so in accordance with this part 7;

- Third parties will be notified, in accordance with the terms of any applicable Data Sharing Agreements

7.3 Reporting to the ICO

The Privacy Administrator will report any breaches which are assessed as posing a risk to the rights and freedoms of the data subjects who are subject of the breach. These must be reported to the ICO within 72 hours of the breach occurring. The Privacy Administrator will also liaise with the Business Manager to determine whether it is appropriate to notify those data subjects affected by the breach.

8. Privacy Administrator

8.1. Organisations deemed to be Public Bodies under Freedom of Information legislation must appoint a Data Protection Officer, with Statutory Responsibilities to ensure compliance with Data Protection requirements. So must large volume data processors. As neither of these currently apply to it, the Company has not appointed a Data Protection Officer.

8.2 However, the Company has identified a non-executive officer as key contact for and with oversight of compliance with Data Protection requirements under this Privacy Policy- the Privacy Administrator. This officer does not have the Statutory Responsibilities of a Data Protection Officer. The Privacy Administrator's details are noted on the Company's website and contained within the Privacy Notices- at Appendices 2 and 3 hereto. The Privacy Administrator will:

8.2.1 monitor the Company's compliance with Data Protection requirements under this Policy and report accordingly to the Company's Business Manager and Board;

8.2.2 co-operate with and serve as the Company's contact for discussions with the ICO;

8.2.3 liaise with the Business Manager to assess breaches or suspected breaches, and to report these as necessary to the ICO, data subjects, and any necessary third parties in accordance with Part 7 hereof.

8.2.4 advise the Chair, Vice Chair, Chair of Audit & Risk Committee, or the Company's External Auditor, as appropriate and available, if concerned that any issues identified under part 7 or 8 hereof have not been adequately addressed.

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 Company, 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 Company's processing of their data. These rights are notified to the Company's tenants and other customers in the Company's Privacy Notice- Customers- at Appendix 2 hereto. For employees and employment applicants these rights are notified in the Company's Fair Processing Notice- Employment- at Appendix 3 hereto.

9.3 **Subject Access Requests**

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

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 Company 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 be Forgotten**

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

9.4.2 Each request received by the Company 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 Privacy Administrator 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.

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

9.5.1 A data subject may request that the Company 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 Company, a data subject has an absolute right to object to processing of this nature by the Company, and if the Company receives a written request

to cease processing for this purpose, then it must do so immediately.

9.5.2 Each request received by the Company 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 Privacy Administrator 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 Company in identifying and reducing the risks that our operations have on personal privacy of data subjects.

10.2 The Company 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 Company will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The Privacy Administrator 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 Privacy Administrator within five (5) working days.

11. Archiving, Retention and Destruction of Data

The Company cannot store and retain Personal Data indefinitely. It must ensure that Personal data is only retained for the period necessary. The Company shall ensure that all Personal data is archived and destroyed in accordance with the periods specified within the table at Appendix 6 hereto.

12. Review

This policy shall be reviewed as necessary but not later than at the end of its first year, and not later than every three years thereafter.

Homes for Life Housing Partnership: Privacy Policy: Appendix 1: Schedule of Related Policies

IT, including:

- Data Security Policy
- Software Security Policy
- Company and Personal Devices Policy
- Credential Management (Password) Policy
- Change Management Policy
- Email, Internet and Social Media Policy
- Server Patching Policy

Customer Services, including:

- Allocations Policy
- Section 5 Protocal & Nominations Agreement
- Tenancy Management Policy
- Complaints Policy
- Anti- Social Behaviour Policy
- Unacceptable Actions Policy
- Debt Recovery Policy

Procurement, including:

- Procurement Policy
- Selection & Control of Contractors Policy

Personnel, including:

- Recruitment & Selection Policy
- Code of Conduct for Staff

General, including:

- Membership Policy
- Code of Conduct for Governing Body Members
- Equality & Diversity Policy

Homes for Life Housing Partnership Privacy Policy: Appendix 2: GDPR Privacy Notice: General

(How we use your personal information*)

(Note- a separate Privacy Notice: Employment covers data processing for employees and applicants for employment)*

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 about you, (which may be held on paper, electronically, or otherwise). 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?

Homes for Life Housing Partnership ("**we**" or "**us**") are a Scottish Charity (Scottish Charity Number 028542), a Company registered in terms of the Companies Acts with registered number 188299 and having their Registered Office at 57 Market Street, Haddington, East Lothian, EH 41 3JG. We take the issue of security and data protection very seriously and strictly adhere to guidelines published in the [Data Protection Act of 1998] and the General Data Protection Regulation (EU) 2016/679 which is applicable from the 25th May 2018, together with any domestic laws subsequently enacted.

We are notified as a Data Controller with the Office of the Information Commissioner under registration number Z4790842 and we are the data controller of any personal data that you provide to us.

As a Registered Social Landlord, we are not currently required to appoint a Data Protection Officer with Statutory Responsibilities under the General Data Protection Regulation, and have not opted to appoint one.

Any questions relating to this notice, our Privacy Policy and practices should be directed to our Privacy Administrator- Alison Hume, Corporate Services Officer- tel 01620 829300 or email alison@homesforlife.co.uk, or at our office at 57 Market Street, Haddington, East Lothian, EH41 3JG.

How we collect information from you and what information we collect

We collect information about you:

- when you apply for housing with us- whether for affordable rent or ownership, become a tenant or sharing owner, request services/ repairs, enter into a factoring agreement with ourselves howsoever arising or otherwise provide us with your personal details
- when you apply to become a member or director;
- from your use of our online services, whether to report any tenancy/ factor 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);

We may collect the following information about you:

- name;
- address;
- household details;
- telephone number;
- current and previous accommodation;
- e-mail address;
- National Insurance Number;
- Next of Kin or other emergency contact;
- Relevant personal characteristics such as disability, medical conditions, gender, ethnic group and preferred language
- Employment details;
- Income details, including benefits entitlement; and
- Banking details

We may 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; and
- Reports as to the conduct or condition of your tenancy, including references from previous tenancies, and complaints of anti-social behaviour.

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
- 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 or supplies which materially affect you;
- for all other purposes consistent with the proper performance of our operations and business; 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 only by our employees 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 but not restricted to 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, including necessary surveys or testing, 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
- For reference requests- from landlords or mortgage providers

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

Your information will only be 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.

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 minimum periods outlined in the table at Appendix 7 of our Privacy Policy, after which this will be destroyed if it is no longer required for the reasons it was obtained. Our Privacy Policy is available on our website or from our Registered Office.

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 yours we hold; and
- object to receiving any marketing communications from us.

These rights may be subject to restrictions and/or exemptions under the regulation..

If you would like to exercise any of these rights please contact our Privacy Administrator - Alison Hume, Corporate Services Officer- tel 01620 829300 or email alison@homesforlife.co.uk, or at our **Registered Office** at 57 Market Street, Haddington, East Lothian, EH41 3JG.

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:

The Information Commissioner's Office – Scotland
45 Melville Street, Edinburgh, EH3 7HL
Telephone: 0131 244 9001

Homes for Life Housing Partnership: Privacy Policy: Appendix 7: Data Retention Periods

The table below sets out minimum retention periods for Personal Data held and processed by the Company. It is intended to be used as a guide only. The Company 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 1 year from date of interviews. Successful applicants documents will be transferred to personal file *(see above).*
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, 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	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 & Universal Credit Notifications	Duration of Tenancy
Tenancy and sharing owner files	Duration of Tenancy
Former tenants' and owners' files *(key info only)*	5 years
Third Party documents, including 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