Privacy Policy – Final Draft

Policy Implementation Checklist	
Document Status	Version 3 – 24 October 2018
Policy Guardian:	Chief Executive
Policy Author:	Temporary Customer Services Director
Policy Title:	Privacy Policy
Approved by Chief Executive on:	
Approved by Policy Working Group on:	21 August 2018
Approved by Linthouse Management Committee on:	13 November 2018
Effective from:	14 November 2018
Due for Review on:	November 2021
Regulatory Standards:	
Policy and Other Linkages:	Scottish Federation of Housing Associations (SFHA) Charitable Model Rules (Scotland) 2013 (as amended 2015).
Training Completed on:	
Plan Tested on:	
Posted on Website on:	
Staff Sign off as Read and Training Completed	
Management Committee Sign off as Read and Training Completed	

1. INTRODUCTION

1.1 Linthouse Housing Association (hereinafter ”LHA”) is committed to ensuring the secure and safe management of data held by LHA in relation to data subjects, staff and other individuals. LHA’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.

1.2 LHA needs to gather and use certain information about individuals. These can include data subjects (tenants, factored owners etc.), employees, Management Committee members, LHA members, volunteers and other individuals with whom LHA has a contractual relationship. LHA 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).

1.3 This Policy sets out LHA’s duties in processing that data, and the purpose of this Policy is to set out the guidelines for the management of such data.

1.4 A list of appendices concludes this policy. Many of these individual appendices are operational in their nature and are lengthy; and are based on standard template documentation developed by the SFHA, GWSF and T C Young. As such, they are not reproduced in their entirety, but the list of appendices summarises their content. Provision of the full documents is available on request.

1.5 LHA recognises its statutory obligations with regard to Data Protection. Moreover, LHA is fully committed to the safe and secure processing of personal data because it is ‘the right thing to do’ not only from a legal and business perspective, but additionally from an ethical and moral perspective.

2. LEGISLATION

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

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. DATA

3.1 LHA 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 LHA is detailed within the Fair Processing Notices. Contents of a range of Notices used for GDPR purposes are summarised in the List of Appendices to this policy. However, LHA uses the following definitions.

3.2 "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 LHA. Personal Data can also take the form of close circuit television (CCTV) images or other moving images. It also includes photographic images, telephone calls or biometric data i.e. fingerprint data or other verification data.

3.3 LHA also holds Personal Data that is sensitive in nature (e.g. 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 LHA is permitted to process Personal Data on behalf of data subjects listed in paragraph 1.2 above, provided it is doing so on one of the following grounds:

- Processing with the consent of the data subject (see clause 4.6 below);
- Processing is necessary for the performance of a contract between LHA and the data subject or for entering into a contract with the data subject;
- Processing is necessary for LHA'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 LHA's official authority; or
- Processing is necessary for the purposes of legitimate interests.

Fair Processing Notice

4.2 LHA has produced a Fair Processing Notice (FPN) which it is required to be provided to all data subjects whose personal data is held by LHA. FPN's must be provided to the data subject from the outset of processing their Personal Data and they will be advised of the terms of the FPN when it is provided to them.

4.3 The Fair Processing Notice referred to at Appendix 2 on the List of Appendices sets out the Personal Data processed by LHA and the basis for that processing. This document is provided to all of LHA's data subjects at the outset of processing their data.

Employees

4.4 Employee Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by LHA. 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.

4.5 A copy of any employee's Personal Data held by LHA is available upon written request by that employee from LHA's Business Support and Corporate Services Officer (BSCSO).

Consent

4.6 Consent as a ground of processing will require to be used from time to time by LHA when processing Personal Data. It should be used by LHA where no other alternative ground for processing is available. In the event that LHA 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 LHA must be for a specific and defined purpose (i.e. general consent cannot be sought).

Processing of Special Category Personal Data or Sensitive Personal Data

4.7 In the event that LHA processes Special Category Personal Data or Sensitive Personal Data, LHA 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 courts are acting in their judicial capacity; and
- Processing is necessary for reasons of substantial public interest.

5 DATA SHARING

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

Data Sharing

5.2 Personal data is from time to time shared amongst LHA and third parties who require to process personal data that LHA processes as well. Both LHA and the third party will be processing that data in their individual capacities as data controllers.

5.3 Where LHA shares in the processing of personal data with a third-party organisation (e.g. for processing of the employees' pension), it will require the third-party organisation to enter in to a Data Sharing Agreement with LHA in accordance with the terms of the model Data Sharing Agreement described at Appendix 3 in the list of Appendices to this Policy.

5.4 LHA will ensure that sharing of data with third parties is for a legitimate business reason and that the management of these arrangements are subjected to protocols or other appropriate forms of written agreement. We appreciate that the sharing of such data should be notified to individuals through Fair Processing Notices (FPN's). Whilst those issued to date (August 2018) to comply with GDPR requirements are cast in wide and comprehensive terms regarding the list of organisations with whom we can share data for legitimate business purposes, LHA will periodically review and re-issue FPN's to reflect any new data sharing arrangements put in place as our business is developed.

Data Processors

5.5 Data processors are third-party entities that process personal data on behalf of LHA, and are frequently engaged if certain of LHA's work is outsourced (e.g. payroll, maintenance and repair works).

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

5.7 If a data processor wishes to sub-contact their processing, prior written consent of LHA 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.

5.8 Where LHA contracts with a third party to process personal data held by LHA, it shall require the third party to enter in to a Data Protection Addendum with LHA in accordance with the terms of the model Data Protection Addendum described at Appendix 4 in the list of Appendices to this Policy. This will fully explain the data processor's required behaviours in handling personal data on behalf of LHA, including the requirements of Paragraphs 5.5 – 5.8 of this policy.

6 DATA STORAGE AND SECURITY

6.1 LHA will take all reasonable steps to ensure that all Personal Data held will be stored securely, whether electronically or in paper format.

Paper Storage

6.2 This policy endorses good practice in paper storage management, which is broadly based on the following. 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 LHA's storage provisions.

6.3 LHA's Workplace standard sets out what is expected from employees and other individuals using LHA equipment. This includes a 'clear desk' policy with regard to personal or sensitive data and its storage; and also to visual display unit security and other aspects of workplace security.

Electronic Storage

6.4 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 LHA's data processors or those with whom LHA 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 will be encrypted and will 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 LHA 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 below.

Internal Reporting

7.2 LHA takes the security of data very seriously and in the event of a breach will take the following steps:

- As soon as the breach or potential breach has occurred, and in any event no later than one working day after it has occurred, the Data Protection Officer (DPO) or LHA's Designated Officer 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);
- LHA must seek to contain the breach by whatever means available;
- The DPO or LHA's Designated Officer must consider 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 clause 7;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements
- LHA is trialling appropriate software – Zonefox – to mitigate the risk of breaches of our IT security. We will also ensure our IT support provider (currently Brightridge) actively manages the risks with IT security breaches.

Reporting to the ICO

7.3 The Chief Executive (CEO) will assume responsibilities for the reporting of breaches to the ICO. The (CEO) will be advised on such matters by the DPO or LHA's Designated Officer. LHA recognises that we 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, within 72 hours of the breach occurring. The CEO with advice from the DPO or LHA's Designated Officer, and in considering whether it is appropriate to notify those data subjects affected by the breach, may also take legal advice or advice directly from the ICO. The CEO will nominate a staff member to perform these functions during periods of the CEO's absence on leave.

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 LHA with Data Protection laws. Currently (August

2018) LHA has not appointed a Data Protection Officer. However, LHA appreciates that when Freedom of Information legislation is extended to housing associations, this appointment will become mandatory.

8.2 LHA has recently (August 2018) commenced a comprehensive staffing restructure. LHA will consider how the management of GDPR functions is accommodated in its new structure, and with this the possible timing and designation of a DPO. In the interim, the Temporary Customer Services Director is acting as LHA's Designated Officer for managing GDPR obligations and will continue to do so until the termination of his contract. At this point, arrangements are in place to transfer these responsibilities on a further interim period to the Head of Customer Solutions, pending the completion of the staffing restructure.

8.3 The DPO or LHA's Designated Officer under interim arrangements will be responsible for:

- Managing and monitoring LHA's compliance with Data Protection laws and this Policy;
- In conjunction with the Chief Executive, co-operating with and serving as LHA's contact for discussing breaches with 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 LHA, 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 LHA's processing of their data. These rights are notified to LHA's tenants and other data subjects in LHA's Fair Processing Notice.

Subject Access Requests (SAR's)

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

- 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 LHA 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.

- Will ensure that each request received by LHA 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.

LHA recognises that there is a presumption against charging fees for Subject Access Requests, except in limited circumstances such as repeat requests, highly onerous requests (where charges must relate to administrative costs), or the request is manifestly unfounded . In this regard, LHA will act in accordance with the ICO's regulatory guidance, *The Guide to GDPR – Rights of Access Section*.

The Right to be Forgotten

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

9.5 Each request received by LHA 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. At the discretion of the CEO, the DPO or LHA's Designated Officer 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.

The Right to Restrict or Object to Processing

9.6 A data subject may request that LHA restrict its processing of the data subject's Personal Data, or object to the processing of that data.

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

9.8 Each request received by LHA 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 or LHA's Designated Officer 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 LHA in identifying and reducing the risks that our operations have on personal privacy of data subjects.

10.2 LHA will:

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

- LHA will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The Data Protection Officer ("DPO") or LHA's Designated Officer 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 ICO within five (5) working days.

11 ARCHIVING, RETENTION AND DESTRUCTION OF DATA

11.1 LHA cannot store and retain Personal Data indefinitely. It must ensure that Personal Data is only retained for the period necessary. LHA will develop Data Retention Guidance, as referred to at Appendix 5 in the list of Appendices to this policy.

11.2 A number of sources of information will be used to inform this document, again as detailed in the List of Appendices to this policy. These sources are considered unsatisfactory at the moment in that they are very lengthy and in places they are contradictory. However, this will be a key working document for all staff in managing their GDPR responsibilities. It is therefore intended to produce a simple, easily understood document that can be easily used by staff. We will ensure this document is compliant and it will be informed by the opinions of our internal auditors

12 REVIEW

12.1 This policy will be subject to review every three years, or sooner in the event of legislative or regulatory developments. Management Committee will ensure that this policy and any future revisions are fully compliant with prevailing legislative and regulatory requirements.

LIST OF APPENDICES

The following comprises a list of appendices and a description of their contents.

Provision of hard copies of the full documents is available on request for any member of the Policy Working Group or Management Committee.

App	Title	Description of Contents
1	Association's related policies	LHA Rules; Standing Orders; Openness and Confidentiality
2	Fair Processing Notice	Based on SFHA/ GWSF/ T C Young templates
3	Model Data Sharing Agreement	Based on SFHA/ GWSF/ T C Young templates
4	Model Data Processor Addendum	Based on SFHA/ GWSF/ T C Young templates
5	Table of Duration of Retention of certain Data	To be derived from • Best practice • Professional bodies' codes • Previous National Housing Federation Guidance • Previous SFHA/ GWSF guidance
6	Contract of Employment – Data Protection Clause	Insertion of two clauses into employment contracts detailing: • Entitlement for our employees to access LHA holds about them • Provision of Fair Processing Notice to all employees • Provision of Privacy Policy • Employee confirmation that by signing employment contract, they have read and understood LHA Privacy Policy • LHA's potential requirement to process sensitive personal data of employees • Obtaining of employee's consent for processing of any additional personal data