PRIVACY POLICY

(*Note Lanarkshire Housing Association hereinafter referred to as LHA)

1. POLICY STATEMENT

1.1. LHA is committed to ensuring the secure and safe management of data held by the Association in relation to customers, staff and other individuals. LHA staff members have a responsibility to ensure compliance with the terms of this policy and to manage individual's 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 customers (tenants, sharing owners, factored owners etc.), employees and other individuals that LHA has a relationship with.

1.3. 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).

1.4. This Policy sets out LHA'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

2.1. It is a legal requirement that LHA processes data correctly. The collection, handling and storing of personal information must be 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 Regulations on Privacy and Electronic Communications); and
c) Any legislation that, in respect of the UK, replaces or enacts into UK 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 UK 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 the data subjects) which is known as Personal Data. The Personal Data held and processed is detailed within the Fair Processing Notices (**Appendices 1a, 1b & 1c**) and the Data Protection Addendum of the Terms and Conditions of Employment which have been provided to all employees.

3.2. "Personal Data" is that from which alone a living individual can be identified either by that data alone or in conjunction with other data held by LHA.

3.3. LHA 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 or 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. It 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 4.5);
- 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 the compliance with a legal obligation;
- Processing is necessary to protect the vital interest 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 purpose of legitimate interests.

4.2. LHA has produced a Fair Processing Notice (FPN) (**Appendix 1a**) which is required to be provided to all customers whose Personal Data is held. The 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.

4.3. Employee/Committee Personal Data and Special Category Personal Data or Sensitive Personal Data is held and processed. Details of the data held and processing of that data is contained within the Employee/Committee Fair Processing Notice (**Appendix 1b and 1c**) which is provided to employees/committee at the same time as their Employment Contract/Committee Induction.

4.4. A copy of the employee's Personal Data is available upon written request by the employee from the Finance & Corporate Services Director.

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

4.6. In the event of processing Special Category Personal Data or Sensitive Personal Data, it must be done 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 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. Data is shared 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 to monitor compliance by these third parties with Data Protection laws, LHA will require the third party organisations to enter into an Agreement governing the processing of data, security measures to be implemented and responsibility for any such breaches.

5.2. Personal data is shared between 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 capacity as data controllers.

5.3. Where LHA 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 into a Data Sharing Agreement in accordance with the terms of Data Sharing Agreement (**Appendix 2**).

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

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

5.6. If a data processor wishes to sub-contract their processing, prior written consent must be obtained from LHA. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

5.7. Where LHA contracts with a third party to process personal data held by the Association, it shall require the third party to enter into a Data Protection Addendum in accordance with the terms of the Data Protection Addendum (**Appendix 3**).

6. DATA STORAGE AND SECURITY

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

6.2. 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 LHA's storage provision.

6.3. 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 the Association has entered into a Data Sharing Agreement. If Personal Data is stored on removable media (i.e. CD, DVD, USB memory stick) then that removable media must be stored securely at all times when not in use. 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.

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

- As soon as the breach/potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the 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 breach must be contained as far as possible and by whatever means available;
- The Data Protection Officer (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 the Data Sharing Agreements.

7.3. The DPO is required 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 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.

8. DATA PROTECTION OFFICER (DPO)

8.1. A DPO is an individual who has an over-arching responsibility and oversight over compliance within LHA with Data Protection laws. LHA has elected to appoint the Planning & Research Manager as DPO and these details will be noted on the website and contained within the Fair Processing Notice.

8.2. The DPO will be responsible for the following:

- Monitoring compliance with Data Protection laws and this Policy;
- Co-operating with and serving as LHA's nominated contact for any discussions with the ICO;
- Reporting breaches/suspected breaches to the ICO and data subjects in accordance with clause 7.

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 tenants and other customers in the Fair Processing Notice.

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

9.5. Each request received 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.

9.6. 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.

9.7. In the event of LHA undertaking any direct marketing, a data subject has the absolute right to object to processing of this nature, and if a written request to cease processing is received for this purpose, then it must be actioned immediately.

9.8. Each request received will require to be considered on its own merits and legal advice may be needed in relation to such requests. It is the responsibility of the DPO to accept or refuse the data subject's request in accordance with clauses 9.5 to 9.7 inclusive. The response to the data subject on whether to accept or reject the request must be made in writing by the DPO.

10. PRIVACY IMPACT ASSESSMENTS

10.1. Privacy Impact Assessments (PIAs) are a means of assisting in the identification and reduction of the risks that our operations have on personal privacy of data subjects.

10.2. The Association shall:

- Carry out a PIA before undertaking a project or processing activity which poses a high risk to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and processing 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 details of any security measures that require to be taken to protect the personal data.

10.3. LHA will consult with 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 must notify the DPO 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 shall ensure that all Personal Data is archived and destroyed in accordance with the periods specified at the table in **Appendix 4**.

12. DATA BREACH INCIDENT PLAN

12.1. LHA is obliged to have in place a framework designed to ensure the security of all personal data during its lifecycle. This Plan (**Appendix 5**) sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security across the organisation.

LIST OF APPENDICES