PRIVACY POLICY

FEBRUARY 2026

LANARKSHIRE
HOUSING ASSOCIATION LTD

LANARKSHIRE
HOUSING ASSOCIATION LTD
191 Brandon Street
Motherwell ML1 1RS
Tel: (01698) 269119
Fax: (01698) 275202

PRIVACY POLICY

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

1.0 INTRODUCTION

1.1. LHA is committed to ensuring the secure and safe management of all the data it holds 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 individuals' data in accordance with the procedures outlined in this policy and documentation referred to herein.

1.2. LHA requires to gather and use certain information about individuals, including customers (tenants, sharing owners, factored owners etc), employees and other individuals that it has a relationship with.

1.3. A significant amount of data is managed by LHA from a variety of sources, and this data contains Personal Data & Sensitive Personal Data, known as Special Categories of personal data under the GDPR.

1.4. This Policy sets out LHA's duties and procedures for the management and processing of personal data.

1.5. LHA's related policies include the Data Protection Policy and the Freedom of Information Policy.

2.0 LEGISLATION

2.1 It is a legal requirement that 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:

a) The UK General Data Protection Regulation ("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)

c) The Data Protection Act 2018 ("the 2018 Act") and

d) Any legislation that, in respect of the United Kingdom, replaces or enacts into United Kingdom domestic law, the UK General Data Protection Regulation, 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.

3.0 DATA

3.1 LHA holds a variety of Data relating to individuals, including customers and employees (also referred to as Data Subjects). Data which can identify Data Subjects is known as Personal Data. The Personal Data held and processed is detailed within LHA's Fair Processing Notices.

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.

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, political opinions, or relates to health or sexual orientation). This is "Special Category Personal Data" or "Sensitive Personal Data".

4.0 PROCESSING OF PERSONAL DATA

4.1 LHA 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 4.6)
- Processing is necessary for the performance of a contract between LHA and the Data Subject or for LHA 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 interest of the Data Subject or another person; or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of LHA's official authority

4.2 LHA's Fair Processing Notice (FPN) for customers is 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 LHA has three Fair Processing Notices for customers, employees and Committee Members respectively, which set out the Personal Data processed by LHA and the basis for that processing.

4.4 FPNs are provided to all of LHA's customers at the outset of processing their data.

4.5 Employee/Committee Member 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/Committee Member Fair Processing

Notices, which are provided to employees/committee members respectively at the application stage.

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

4.7 Consent as a ground for processing will require to be used from time to time when processing Personal Data and should be used where no alternative ground for processing is available. In the event that consent is required to process a Data Subject's Personal Data, LHA 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 defined and specific purpose i.e. general consent cannot be sought. Where consent is being relied on, Data Subjects are free to withhold their consent or withdraw it at any future time.

4.8 A mandate should be sought from any elected representative (MP, MSP or Councillor) who requests data on behalf of a customer and information should not be provided without this.

4.9 In the event of processing Special Category Personal Data or Sensitive Personal Data, LHA must rely on an additional ground for processing in accordance with one of the special category grounds. These include, but are not restricted to, the following:

- The Data Subject has given explicit consent to the processing of this data for a specified purpose
- Processing is necessary for carrying out obligations or exercising rights related to employment, social security or social protection law
- Processing is necessary for health or social care
- Processing is necessary to protect the vital interest of the Data Subject or, if the Data Subject is incapable of giving consent, the vital interests of another person
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity and
- Processing is necessary for reasons of substantial public interest under law

4.10 The grounds for processing sensitive personal data are set out in the GDPR and expanded on in the Data Protection Act 2018.

DATA SHARING

4.11 Data is shared with various third parties for numerous reasons in order that LHA's day to day activities are carried out in accordance with its relevant policies and procedures. In order to monitor compliance by these third parties with Data Protection laws, LHA may require the third party organisations to enter into an Agreement with the Association governing the processing of data, security measures to be implemented and responsibility for any breaches. This will only apply in situations where the third party is a joint controller.

4.12 Personal Data is from time-to-time shared amongst LHA and third parties who require to process the same Personal Data as LHA. Whilst LHA and third parties may jointly determine the purposes and means of processing, both LHA and the third party will be processing that data in their individual capacity as data controllers.

4.13 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.

4.14 A Data Processor is a third-party entity that processes Personal Data on behalf of LHA and is frequently engaged if certain work is outsourced (e.g. maintenance and repair works).

4.15 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.

4.16 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 any data protection breaches of their sub-contractors.

4.17 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.

5.0 DATA STORAGE AND SECURITY

5.1 All Personal Data held must be stored securely, whether electronically or a hard copy format.

5.2 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, in order to ensure its secure destruction. If the Personal Data requires to be retained on a physical file, then the

employee should ensure that it is affixed to the file, which is then stored in accordance with LHA's storage provision.

5.3 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 encrypted and 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.

6.0 BREACHES

6.1 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, require to be reported externally in accordance with clause 7.2.

6.2 Regarding internal reporting, LHA takes the security of data very seriously and in the event of a breach, will take the following steps:

- As soon as it becomes known that the breach/potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the Data Protection Officer (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)

- LHA must seek to contain the breach by whichever means available

- The DPO must consider whether the breach needs to be reported to the Information Commissioner's Office (ICO) and to the Data Subject(s) affected and if so, will carry out these requirements in accordance with clause 7

- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

6.3 With respect to reporting to the Information Commissioner's Office ("ICO"), the DPO is required to report any breaches which pose a risk to the rights and freedoms of the Data Subjects 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.

6.4 LHA's Data Breach Incident Plan sets out the procedure to be followed in the event of a Data Breach.

7.0 DATA PROTECTION OFFICER (DPO)

7.1 A DPO is an individual who has an over-arching responsibility and oversight over compliance by LHA with Data Protection laws. LHA has elected to appoint the Finance and Corporate services Director as DPO and details of the DPO and how to contact them are contained on LHA's website.

7.2 The DPO will be responsible for the following:

- Monitoring LHA's 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 (where appropriate)

8.0 DATA SUBJECT RIGHTS

8.1 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.

8.2 Data Subjects have a right to request a restriction of processing their data, a right to request erasure of their Personal Data and a right to object to LHA's processing of their data. These rights are notified to tenants and other customers in the Fair Processing Notices. Such rights are subject to qualification and are not absolute.

8.3 Data Subjects are permitted to view their Personal 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 from the day after 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 a Data Subject, LHA must confirm this to the Data Subject as soon as practicably possible and in any event, not later than one month from the day after the date on which the request was made

8.4 A Data Subject can exercise their right to erasure (otherwise known as the right to be forgotten) by submitting a request in writing to LHA seeking it to erase the Data Subject's Personal Data in its entirety.

8.5 Each request received will require to be considered on its own merits and legal advice will need 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 this policy and will respond in writing to the request.

8.6 Requests for erasure will be considered and responded to by LHA, within one month from the day after the date we receive the request.

8.7 A Data Subject may request that the Association restrict its processing of their Personal Data, or object to the processing of that data.

8.8 In the event of LHA undertaking any direct marketing, a Data Subject has an absolute right to object to processing of this nature by the Association and if a written request to cease processing is received for this purpose, then LHA must do so immediately.

8.9 Each request received will require to be considered on its own merits and legal advice may be needed. It is the responsibility of the DPO to accept or refuse the Data Subject's request in accordance with this policy and the DPO will respond in writing to such requests.

8.10 A Data Subject may request that LHA rectifies inaccurate Personal Data or that incomplete Personal Data is completed. In such instances, each request will require to be considered on its own merits and legal advice may be required. The DPO is responsible for accepting or refusing the request in accordance with this policy and will respond in writing.

9.0 PRIVACY IMPACT ASSESSMENTS (PIAs)

9.1 PIAs are a means of assisting in the identification and reduction of the risks that our operations have on the personal privacy of Data Subjects.

9.2 LHA 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 & 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

9.3 LHA will consult with the ICO in the event that a PIA identifies a high level of risk which cannot be reduced or mitigated. The DPO will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA, they must notify the DPO within five (5) working days.

10.0 ARCHIVING, RETENTION AND DESTRUCTION OF DATA

10.1 LHA cannot store and retain Personal Data indefinitely and will ensure that it is only retained for the period necessary. LHA shall ensure that all Personal Data is archived and destroyed in accordance with the periods specified in the Personal Data retention period guidelines.