Loreburn Housing Association

Loreburn Group

Privacy Policy

Policy	**Privacy Policy**					
Version reference	**6**					
Approved by	**MC**		**LET**	**X**	**MT**	
Date of approval	**November 2023**					
Review period	**3 Yearly or as legislative or substantive changes occur**					
Review due	**November 2026**					
Policy champion	**Head of Governance & Assurance**					

List of Appendices

1. Fair Processing Notice (Customers)
2. Employee Fair Processing Notice
3. Recruitment Fair Processing Notice
4. Photograph Consent Form
5. Model Data Sharing Agreement
6. Data Sharing Risk Assessment Form (Blank)
7. Data Sharing Risk Assessment Form (Example)
8. Instructions to Encrypt Emails
9. Model Data Protection Addendum
10. Privacy Impact Assessment Template
11. Retention Periods of Data
12. GDPR Quick Reference Guide

1. Introduction

1.1 Loreburn Housing 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, governing body and volunteers 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 The Association needs to gather and use certain information about individuals. These can include tenants, customers, 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).

1.3 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. Loreburn's Data Protection Officer (DPO) is the Head of Governance & Assurance.

1.4 Any requests made under Freedom of Information must be dealt with under the Freedom of Information Policy. The requirements of GDPR will be considered in line with the Freedom of Information Request Procedure.

1.5 A GDPR Quick Reference Guide is available as Appendix 12.

2. Legislation

2.1 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 Data Protection Act 2018 and the UK General Data Protection Regulation ("the UK 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 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. Data

3.1 The Association holds a variety of Data relating to individuals, including tenants, 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 Fair Processing Notices at Appendices 1 to 3 and the Data Protection Addendum of the Terms of and Conditions of Employment which has been provided to all employees.

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 4.4);

- 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 legitimate interests.

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 at Appendices 1 to 3 set out the Personal Data processed by the Association and the basis for that Processing. This document is provided to all of the Association's tenants, customers, employees, applicants and volunteers at the outset of processing their data.

4.3 **Employees**

4.3.1 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.

4.3.2 A copy of any employee's Personal Data held by the Association is available upon written request by that employee from the Head of People & Culture.

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 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).

Photographs

Consent must be sought before taking and/or publishing photographs of tenants, customers and staff. Where this relates to photographs of children consent must be given by parents/legal guardians prior to ANY photograph being taken and/or published. Such consent will state how long the association will hold the photographs and any publishing rights. The Consent Form (Appendix 4) should be used and signed for all photos including those taken at events.

Where photographs have been provided by a third party (for example in relation to an ASB case) and contain data subjects, staff should consider whether Loreburn have a lawful basis for the processing of that data which may have been provided without consent. Advice should be sought from the DPO in relation to any queries regarding the processing, storing and sharing of any such photographs. **Staff must not share photographs provided by a third party without consent unless a lawful basis has been established and subsequently recorded by the DPO.**

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.

5. Data Sharing

5.1 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 into an Agreement with the Association 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 Association and third parties who require to process personal data that the Association process as well. 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. for processing of the employees' pension), 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 5 to this Policy. Where an agreement is not signed no information should be shared until a Risk Assessment has been completed using the Data Sharing Risk Assessment Template (Appendix 6) which is supported by the relevant Director and Authorised by the DPO. An example Data Sharing Risk Assessment can be viewed here (Appendix 7).

5.2.3 All personal data shared with Third Parties must be done so securely either by CJSM secure e-mail or through e-mail encryption. Instructions on how to send e-mails securely can be viewed here (appendix 8). If information can not be shared via encrypted email, information shall be shared via a password protected Word document and the password shared with the recipient via text message or over the phone.

5.3 Data Processors

A data processor is a third-party entity that processes personal data on behalf of the Association and are frequently engaged in certain areas of the Association's work is outsourced (e.g. payroll provider)

5.3.1 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 is suffered.

5.3.2 If a data processor wishes to sub-contact 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.

5.3.3 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 9 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

Whilst our ambition is to be a paperless organisation in the coming years, if Personal Data is being 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. As far as possible all personal data should be stored electronically and paper copies destroyed (this is not always possible as in some instances hard copies are required to be retained for a set period by legislation and audit requirements).

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 into 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 and any such devices must be authorised for use by the Data & Digital Team before they are connected to any Loreburn equipment. Personal Data should not be saved directly to mobile devices and should be stored on designated drivers and servers. Personal data should not be stored in e-mails. The information should be transferred to Homemaster or the appropriate file Drive on the system and the e-mail deleted.

6.3 **Verbal Communications**

Before any information is shared verbally and/or recorded staff must ask the required security questions (name, full address and postcode, date of birth which can be verified on Homemaster).

6.4 All calls made to and from the Association will be recorded for quality control purposes. Customers are informed of this by an automated message when they dial the switch board. When making external calls staff should advise customers that calls will be recorded for quality and monitoring purposes. Copies of calls will be retained for a period of six months.

6.5 Loreburn employees will not record face to face conversations with customers unless at the request of a customer. Where a customer requests for a face to face conversation to be recorded, the Association is entitled to request a copy of the recording. We trust that customers will not record

conversations with Lorebrun employees without advising staff that the conversation is being recorded.

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 risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported externally in accordance with 7.3 below.

7.2 **Internal Reporting**

The Association 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 or 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 (via e-mail) of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s).
- The Association's DPO is the Head of Governance & Assurance. If the DPO is not available details of the breach should be issued to the Director of Corporate Services. The DPO will notify the relevant service Director of the 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. The DPO with input from the relevant service Director will utilise the ICO self-assessment tool to consider the likelihood and severity of the risk of the breach and the actions required;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements.
- Breaches will be reported to the Audit & Compliance Sub-Committee by the Head of Governance & Assurance at the next available meeting.

7.3 **Reporting to the ICO**

The DPO 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 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. In the DPOs absence the Director of Corporate Services will notify the ICO.

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.

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 Part 7 hereof.
8.2.4 reporting breaches to the Audit & Compliance Sub-Committee at the next available meeting.

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 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 view their data held by the Association upon making a request to do so (a Subject Access Request). 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. Subject Access Requests must be reported to the Data Protection Officer as soon as possible who will coordinate and formalise the response. The Association:

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 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.

9.3.4 will record the request and outcome of the request within the SAR Register maintained by the DPO.

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 Each request received by the Association 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.

9.5 **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 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 9.5 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. The PIA template is available as Appendix 10.

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 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 Association 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") 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

11.1 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 guidelines contained within the table at Appendix 11. Further guidance will be obtained from the National Housing Federation Retention Schedule and legal advice will be sought as required. These are data retention guidelines only.

12. Monitoring & Review

12.1 The DPO will advise LET (relevant Director) of any data breaches immediately to allow a full investigation and review of existing practices to commence and any further mitigation measures to be put in place.

12.2 Details of any breaches will be reported to the Audit & Compliance Committee quarterly.

12.3 The Policy Champion is the Data Protection Officer. The Policy Champion will review this policy every two years or sooner as required as a result of legislative changes or changes to working practices following any breach review.

13. Equality & Human Rights

13.1 Loreburn aims to ensure that equality, fairness, dignity and respect are central to the way we work and how we treat our customers. We support diversity and uphold equal opportunities in all areas of our work as an employer and service provider.

13.2 Loreburn will not discriminate against tenants, staff, visitors, suppliers or others based on their age, sex, sexual orientation, race, disability, religion or belief, marital status, pregnancy and maternity or gender reassignment (collectively referred to as 'protected characteristics' in the Equality Act 2010).

14. Risk Management

14.1 Loreburn has a Risk Management Strategy, Policy and Procedure. These documents set out how the organisation will manage risk as an integral part of its governance and management systems, ensuring risks are identified, evaluated and controlled effectively.

14.2 Identifiable risks arising from this policy will be monitored and managed by the internal processes set out herein and by regular review of this and all other associated policies and procedures, ensuring risks are mitigated and Loreburn complies with all legislative requirements and regulatory and best practice guidance.

15. Responsibilities

15.1 The below table sets out the responsibilities of all staff in relation to this Policy.

Responsibilities	MC/ CEO	LET	DPO	Heads of Service	All Staff
To set the policy and direction with regards to data protection and GDPR	✓				
Ensure Loreburn H A staff have a robust understanding of GDPR and the associated risks		✓	✓	✓	
Manage compliance, ICO reporting, breach notification to LET and A&C.			✓		
Take lead on breach investigations, ICO reporting and subject access requests			✓		
Complete E-learning and any subsequent training					✓
Policy Champion			✓		

Ensure effective and clear communication regarding GDPR with stakeholders including customers			✓		✓
Reporting any concerns to Line Manager or DPO				✓	✓
Be aware of all data you collect, store and share and make sure this is done in line with this Policy					✓
Ensure all data shared with Third Parties is done so in line with the DSA and exchanged securely.			✓	✓	✓
Report any breach concern to the DPO immediately					✓
Ensure policy is reviewed as necessary			✓		