BUIDHEANN TIGHEADAS LOCH AILLSE AGUS AN EILEIN SGITHEANAICH LTD
LOCHALSH AND SKYE HOUSING ASSOCIATION

DATA PROTECTION POLICY

Service: Corporate	Date	Staff Member
Version Number: 2		
Approved by: The Governing Body	23/03/2026	N/A
Effective From:	23/03/2026	N/A
Next Review Date: **Future Reviews by SMT**	03/2029	CE
Revision Number:		
Revision Date:		
Posted on Intranet:	27/03/2026	CEA
Posted on Website:		
Document Register updated:	27/03/2026	CEA
Previous Version archived:	27/03/2026	CEA
SSHC: Charter Standards and Outcomes:	2	
SHR: Standards of Governance and Financial Management	1.3, 2.1, 2.3, 4.3	

Scottish Social Housing Charter Relevant Standards and Outcomes

STANDARD	OUTCOME
Section:- The customer/landlord relationship 2. Communication Social landlords manage their businesses so that: • *tenants and other customers find it easy to communicate with their landlord and get the information they need about their landlord, how and why it makes decisions and the services it provides.*	This **outcome** covers all aspects of landlords' communication with tenants and other customers. This could include making use of new technologies such as web-based tenancy management systems and smart-phone applications. It is not just about how clearly and effectively a landlord gives information to those who want it. It also covers making it easy for tenants and other customers to make complaints and provide feedback on services, using that information to improve services and performance, and letting people know what they have done in response to complaints and feedback. It does not require landlords to provide legally protected, personal or commercial information.

Scottish Housing Regulator – Relevant Standards of Governance and Financial Management and Guidance

STANDARD	GUIDANCE
1 The governing body leads and directs the RSL to achieve good outcomes for its tenants and other service users.	**1.3** The governing body ensures the RSL complies with its constitution and its legal obligations. Its constitution adheres to these Standards and the constitutional requirements set out below.
2 The RSL is open about and accountable for what it does. It understands and takes account of the needs and priorities of its tenants, service users and stakeholders. And its primary focus is the sustainable achievement of these priorities.	**2.1** The RSL gives tenants, service users and other stakeholders information that meets their needs about the RSL, its services, its performance and its future plans. **2.3** The governing body is open and transparent about what it does, publishes information about its activities and, wherever possible, agrees to requests for information about the work of the governing body and the RSL.
4 The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation's purpose.	**4.3** The governing body identifies risks that might prevent it from achieving the RSL's purpose and has effective strategies and systems for risk management and mitigation, internal control and audit.

DATA PROTECTION POLICY

CONTENTS

DATA PROTECTION POLICY

1. INTRODUCTION

1.1 Lochalsh & Skye Housing Association (hereinafter the "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 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 customers (tenants, factored owners etc.), 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 The Association is a Data Controller registered with the Information Commission (Registration No: Z6024339).

1.4 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.

1.5 All Association personnel, accessing or otherwise processing personal data controlled by the Association have a responsibility for ensuring personal data is collected, stored and handled appropriately and must ensure that it is handled and processed in compliance with data protection law, this policy and the data protection principles.

1.6 Appendix 1 hereto details the Association's related policies.

2. LEGISLATION

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

2.2 **The relevant legislation in relation to the processing of data is:**

(a) the UK General Data Protection Regulation ("the UK GDPR");

(b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR") (as may be amended by the proposed Regulation on Privacy and Electronic Communications);

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

(d) the Data (Use and Access) Act 2025 and

(e) 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 Association 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 Association is detailed within the Privacy Notices at Appendix 2 and the Energy Advice Service Privacy Notice at Appendix 9 hereto and the Data Protection Addendum of the Terms and Conditions of Employment which has been provided to all employees (Appendix 4).

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. COMPLIANCE

4.1 The Association will comply with its legal obligations and the data protection principles by ensuring that personal data is:

- **processed lawfully, fairly and in a transparent manner in relation to individuals**. Individuals will be advised on the reasons for processing via a Privacy Notice. Where data subjects' consent is required to process personal data, consent will be requested in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Data Subjects will be advised of their right to withdraw consent and the process for Data Subjects to withdraw consent will be simple.

- **Collected (whether from the data subject or otherwise) for specified, explicit and legitimate purposes and not further processed by or on behalf of the controller in a manner that is incompatible with the purposes for which the controller collected the data**. For the avoidance of doubt, processing is not lawful by virtue only of it being processed in a manner that is compatible with the purposes for which the personal data was collected. If the Association wishes to use personal data for a different purpose, for example for research, the data subject will be notified prior to processing where required.

- **adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.** The Association will only collect the minimum personal data required for the purpose. Any personal data

deemed to be excessive or no longer required for the purposes collected for will be securely deleted in accordance with the Association's Retention Policy. Any personal information that is optional for individuals to provide will be clearly marked as optional on any forms.

- **accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay**. The Association will take reasonable steps to keep personal data up to date, where relevant, to ensure accuracy. Any personal data found to be inaccurate will be updated promptly. Any inaccurate personal data that has been shared with third parties will also be updated.

- **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.** The Association will hold data for the minimum time necessary to fulfil its purpose. Timescales for retention of personal data will be stated in a Retention Schedule. Data will be disposed of in a responsible manner ensuring confidentiality and security.

- **processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures**. The Association will implement appropriate security measures to protect personal data. Personal data will only be accessible to those authorised to access personal data on a 'need to know' basis. The Association personnel will keep data secure by taking sensible precautions and following the relevant Assocation policies and procedures relating to data protection.

In addition, the Association will comply with the 'Accountability Principle' that states that organisations are to be responsible for, and be able to demonstrate, compliance with the above principles.

5. PROCESSING OF PERSONAL DATA

5.1 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 clause 4.4 hereof);
- 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.

5.2 <u>Privacy Notice</u>

5.2.1 The Association has produced a Privacy Notice (PN) which it is required to provide to all customers whose Personal data is held by the

Association. 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.

5.2.2 The Privacy Notice at Appendix 2 sets out the Personal Data processed by the Association and the basis for that Processing. This document is provided to all of the Association's customers at the outset of processing their data.

5.3 Employees

5.3.1 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 Privacy Notice which is provided to prospective Employees at application stage. (Appendix 3).

5.3.2 A copy of any employee's Personal Data held by the Association is available upon written request by that employee from the Association's Chief Executive or the Association's Data Protection Officer (see Part 8).

5.4 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). Where consent is being relied on, Data Subjects are free to withhold their consent or withdraw it at any time in the future.

5.5 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 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 or 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

All the grounds for processing sensitive personal data are set out in the GDPR

and expanded on in the 2018 Act.

6. DATA SHARING

6.1 In certain circumstance the Association may share personal data with third parties. This may be part of a regular exchange of data, one off disclosures or in unexpected or emergency situations. In all cases, appropriate security measures will be used when sharing any personal data. Where data is shared regularly, a contract or data sharing agreement will be put in place to establish what data will be shared and the agreed purpose. Prior to sharing personal data, the Association will consider any legal implications of doing so. Data Subjects will be advised of the data sharing via the relevant Privacy Notice.

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

6.1.2 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 into 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.

6.2 Data Processors

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

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

6.2.2 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.

6.2.3 Where the Association contracts with a third party to process personal data held by the Association, it shall require the third party to enter into an appropriate contract or Data Protection agreement / addendum with the Association in accordance with the terms of the model Data Protection agreement / addendum set out in Appendix 6 to this Policy.

7. DATA STORAGE AND SECURITY

All Personal Data held by the Association must be stored securely, whether

electronically or in paper format.

7.1 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 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.

7.2 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 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 encrypted and 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.

8. SECURITY INCIDENT & BREACH MANAGEMENT

8.1 Occasionally the Association may experience a data security incident or personal data breach; this could be if personal data is:

- Lost: for example, misplacing documents or equipment that contain personal data through human error; via fire, flood or other damage to premises where data is stored.
- Stoles: theft or as a result of a targeted attack on the IT network (cyber-attack).
- Accidentally disclosed to an unauthorized individual; for example, email or letter sent to the wrong address.
- Inappropriately accessed or used.

8.2 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 Clause 8.4 hereof.

8.3 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 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 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 IC 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

8.4 Reporting to the IC

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 Commission ("IC") 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.

9. DATA PROTECTION OFFICER ("DPO")

9.1 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 Privacy Notice at Appendix 2 hereto.

9.2 The DPO will be responsible for:

9.2.1 monitoring the Association's compliance with Data Protection laws and this Policy;

9.2.2 co-operating with and serving as the Association's contact for discussions with the IC

9.2.3 reporting breaches or suspected breaches to the IC and data subjects in accordance with Part 8 hereof.

10. DATA SUBJECT RIGHTS

The Association will uphold the rights of data subjects to access and retain control over their personal data in accordance with its Data Subject Rights Procedure. These rights are notified to the Association's tenants and other customers in the Association's Privacy Notice. It should be noted that certain rights are subject to qualification and are not absolute.

10.1 The Association will uphold the rights of data subjects to access and retain control over their personal data in accordance with its Data Subject Rights Procedure. These rights are notified to the Association's tenants and other customers in the Association's Privacy Notice. It should be noted that certain rights are subject to qualification and are not absolute

10.2 Right to be informed.
Data subjects have the right to be informed of the reasons for processing their data in a clear, transparent and easily accessible form and informing them of all their rights, the Association does this through the provision of Privacy notices.

10.3 Right of Access / 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. The Association:

10.3.1 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.

10.3.2 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

10.3.3 where the Association does not hold the personal data sought by the data subject, must confirm that it does not hold any of the personal data sought by 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.

10.4 Right to Erasure

10.4.1 A data subject can exercise their right to erasure (otherwise known as the 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.

10.4.2 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 10.4 and will respond in writing to the request.

10.4.3 Requests for erasure will be considered and responded to by the Association by one month from the day after the date we receive the request.

10.5 Right to Restrict or Object to Processing

10.5.1 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.

10.5.1.1 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.

10.5.2 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 10.5 and will respond in writing to the request.

10.6 Right to Rectification

10.6.1 A Data Subject may request the Association to have inaccurate personal data rectified. If appropriate, a data subject may also request the Association to have incomplete personal data completed.

10.6.2 Each request received by the Association will require to be considered on its merits and legal advice will be required 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 10.6 and will respond in writing to the request.

10.7 Right to Data Portability

10.7.1 A Data Subject may request that the Association where possible, transfer their data to similar organisation in a machine-readable format.

10.7.2 Each request received by the Association will require to be considered on its merits and legal advice will be required 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 10.7 and will respond in writing to the request.

11. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

11.1 These are a means of assisting the Association in identifying and reducing the risks that our operations have on personal privacy of data subjects.

11.2 The Association shall:

11.2.1 Carry out a DPIA 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

11.2.2 In carrying out a DPIA, 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

11.3 The Association will require to consult the IC in the event that a DPIA 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 DPIA they require to notify the DPO within five (5) working days.

12. ARCHIVING, RETENTION AND DESTRUCTION OF DATA

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 periods specified within the table at Appendix 7 hereto.

12.1 The Association will treat your personal data in line with our obligations under the current data protection regulations and our own policies and procedures

12.2 Information regarding how your data will be used and the basis for processing your data is provided in the Association's Privacy Policy.

13. TRAINING

All Association personnel will be made aware of good practice in data protection and where to find guidance and support for data protection issues. Adequate and role specific data protection training will be provided during induction and annually thereafter to everyone who has access to personal data to ensure they understand their responsibilities.

14. BREACH OF POLICY

Any breaches of this policy may be dealt with in accordance with LSHA's disciplinary procedures.

15. MONITORING AND REPORTING

Regular monitoring and audits will be undertaken by the Data Protection Lead and/or DPO to check compliance with the law, this policy and associated procedures. Any concerns will be raised with the Board / Governing Body.

16. REVIEW

This document will be reviewed by the Board or Sub-Committee set up for that purpose in accordance with the requirements of the Association's Register of Policies and Procedures.

Appendix 1

RELATED POLICIES

- Freedom of Information Policy
- Complaints Handling Policy and Procedures
- Information Security (WorldPay) Policy
- IT Use and Security Policy and Procedures
- Mobile Phone Policy
- Provision of Board IT Equipment Policy and Procedures
- Secure Handling, Use, Storage and Retention of Disclosure Information Policy

---

Appendix 2 - Privacy Notice

Appendix 3 - Employee Privacy Notice

Appendix 4 - Addendum to Terms and Conditions of Employment

Appendix 5 - Data Sharing Agreement

Appendix 6 - Data Processing Agreement / Addendum

Appendix 7 - Document Retention Table

Appendix 8 - LSHA Data Audit Form

Appendix 9 - Energy Advice Service Privacy Notice

SCHEDULE OF REVISIONS		
DATE	REVISION No.	DETAILS
27/08/2021	V1.1	Updated with new SFHA Guidance – amendments made to Points 2.2/3.1/4.1/4.3.1/ 4.3.2/4.4/4.5/5.1/5.2.1/6.2/8.1/9.2/9.4.1/9.4.3/NEW 9.6/10.3/Point 11 merged with point 12/NEW point 12.
23/03/2026	V2.0	Full review – New version created