PRIVACY POLICY (2019)

1.0 INTRODUCTION

Ochil View Housing Association Ltd (hereinafter "the Association") is committed to ensuring the secure and safe management of personal information held by the Association in relation to customers, employees and other individuals (also referred to as data subjects). The Association's staff members have a responsibility to ensure compliance with the terms of this Policy, and to manage individuals' personal information in accordance with the procedures outlined in this Policy and documentation referred to herein.

The Association needs to gather and use certain personal information about data subjects. These can include current or former customers (applicants, tenants, factored owners etc.), employees and other individuals that the Association has a relationship with. The Association manages a significant amount of personal information, from a variety of sources. This personal information contains personal information and sensitive personal information (known as special categories of personal information under the General Data Protection Regulation (GDPR)). The Association needs to gather and use this personal information for a number of specific and lawful purposes relevant to its activities and functions as a registered social landlord in Scotland.

This Policy sets out how the Association complies with its data protection obligations and seeks to protect personal information that it handles and uses as part of its activities and functions as a registered social landlord in Scotland, regardless of the medium on which that personal information is stored or where it is stored. The purpose of the Policy is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access during their work with the Association.

The Association is committed to complying with its data protection obligations, and to being concise, clear and transparent about how it obtains and uses personal information and how (and when) it deletes that personal information once it is no longer required.

The Association recognises that the correct and lawful treatment of personal information will maintain confidence in the Association and is conducive to successful business operations. Protecting the confidentiality and integrity of personal information is a critical responsibility that the Association always takes seriously. The Association is exposed to potential fines of up to EUR 20 million or 4% of its total annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of data protection legislation.

The Association's Data Protection Officer (DPO) is responsible for informing and advising the Association and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Association's policies. If members of staff have any questions or comments about the content of this Policy or if they need further information, they should contact the DPO.

The **Appendix** hereto details the Association's related policies and documentation.

2.0 LEGISLATION

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

The relevant legislation in relation to the handling and use of personal information is:

(a) the GDPR and Data Protection Act 2018; and
(b) any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the GDPR or any other law relating to data protection, the handling and use of personal information and privacy as a consequence of the United Kingdom leaving the European Union.

3.0 PERSONAL INFORMATION

3.1 The personal information handled and used by the Association is detailed within the Fair Processing Notice (FPN) within the Appendix hereto and the Data Protection Addendum of the Terms of and Conditions of Employment which has been provided to all employees.

3.1.1 "Personal information" is information from which a living individual can be identified either by that information alone, or in conjunction with other information held by the Association. An example would be a tenant's name or the address of a property.

3.1.2 The Association also holds personal information 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" or "sensitive" personal information.

4.0 HANDLING AND USE OF PERSONAL INFORMATION

4.1 The Association will comply with the following data protection principles when handling and using personal information in carrying out its activities and functions:

4.1.1 the Association will handle and use personal information lawfully, fairly and in a transparent manner;
4.1.2 the Association will collect personal information for specified, explicit and legitimate purposes only, and will not handle and use it in a way that is incompatible with those legitimate purposes, unless the handling and use has been first notified to the data subject;

4.1.3 the Association will only handle and use personal information that is adequate, relevant and necessary for the above specified, explicit and legitimate purposes;

4.1.4 the Association will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;

4.1.5 the Association will keep personal information for no longer than is necessary for the purposes for which the personal information is handled and used; and

4.1.6 the Association will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful handling and use, and against accidental loss, destruction or damage.

4.2 The Association must have a legal reason to justify its handling and use of personal information, which must include one or more of the following:

- ✓ the consent of the data subject;
- ✓ the performance of a contract between the Association and the data subject;
- ✓ compliance with a legal obligation to which the Association is subject;
- ✓ the vital interests of the data subject or another person; or
- ✓ the Association's or another person's legitimate interests except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject.

4.3 In determining whether the Association can rely on its legitimate interests as the legal reason, the Association will conduct an assessment and keep a record of it to justify its decision. The Association will keep the assessment under review and repeat it if circumstances change.

4.4 The Association may from time to time need to handle and use sensitive personal information as part of its activities and functions as a registered social landlord in Scotland. The Association will only handle and use sensitive personal information if it has a legal reason to justify its handling and use of sensitive personal information, which must include one or more of the following:

- ✓ explicit consent of the data subject;
- ✓ carrying out obligations or exercising rights related to employment or social security;
- ✓ protection of the vital interests of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- ✓ the establishment, exercise or defence of legal claims,
- ✓ reasons of substantial public interest; and
- ✓ the personal information has been manifestly made public by the data subject.

4.5 Except where the handling and use of personal information is based on consent, the Association must generally be satisfied that the handling and use is necessary for the relevant legal reason (i.e. there is no other reasonable way to achieve that purpose).

4.6 Before handling and using any new sensitive personal information, staff must notify the DPO of the proposed handling and use in order that the DPO may assess whether one or more of the above legal reasons is satisfied. Staff must not handle

and use the sensitive personal information until the DPO has carried out this assessment and the data subject has been informed by way of FPN of the purposes for which it is being carried out and the legal reasons for it.

4.7 The Association must include information about the relevant purpose for the handling and use and the legal reason(s) within its FPN.

4.8 **Fair Processing Notice ("FPN")**

4.8.1 The Association has produced a FPN which it is required to provide to all customers whose personal information is handled and used by the Association. That FPN, or a summary of it with clear instruction on how to access the full document, must be provided to the customer from the outset of the handling and use of their personal information and they should be advised of the terms of the FPN when it is provided to them.

4.8.2 The FPN within the Appendix hereto sets out the personal information handled and used by the Association and the legal reason for its handling and use. This document, or the summary referred to in 4.8.1, is provided to all of the Association's customers at the outset.

4.9 **Employees**

4.9.1 Employee personal information and, where applicable, special category personal information or sensitive personal information, is handled and used by the Association. Details are contained within the Employee FPN which is provided to employees at the same time as their contract of employment. Existing employees have already been provided with this FPN.

4.9.2 An employee can request a copy of their personal information held by the Association from the Association's DPO.

4.10 **Consent**

Consent may be used by the Association to justify its handling and use of personal information. It should be used by the Association where no other alternative ground is available. A data subject consents to handling and use of their personal information if they indicate agreement either by a statement or positive action. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity are unlikely to be enough. If consent is given in a document which deals with other matters, then consent must be kept separate from those other matters. Data subjects must be easily able to withdraw consent at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if personal information is to be handled and used for a different and incompatible purpose which was not disclosed when the data subject first provided their consent via the relevant FPN. If the Association requires to obtain consent to handle and use a data subject's personal information, it shall obtain or record that consent in writing. The consent provided by the data subject must be freely given and the data subject must not be forced to provide consent. Any consent to be obtained by the Association must be for a specific and defined purpose (i.e. general consent cannot be sought).

5.0 PERSONAL INFORMATION SHARING

5.1 The Association shares personal information 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 handling and use of personal information, security measures to be implemented and responsibility for breaches.

5.2 Personal Information Sharing

5.2.1 Personal information is from time to time shared amongst the Association and third parties who require to handle and use personal information. Both the Association and the third party will be handling and using that information in their individual capacities as data controllers.

5.2.2 The Association shall enter into a Data Sharing Agreement with the third party in accordance with the terms of the model Data Sharing Agreement set out within the Appendix to this Policy.

5.3 Data Processors

Where the Association uses external organisations to handle and use personal information on its behalf, such as its contractors and service providers, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of the Association's personal information. Contracts with external organisations must provide that:

5.3.1 the organisation may act only on the Association's written instructions;

5.3.2 employees of the organisation handling and using the personal information are subject to a duty of confidence;

5.3.3 appropriate measures are taken to ensure the security of the personal information;

5.3.4 sub-contractors are only engaged by the organisation with the Association's prior consent and under a written contract;

5.3.5 the organisation will assist the Association in providing subject access and allowing data subjects to exercise their data protection rights;

5.3.6 the organisation will assist the Association in meeting its obligations in relation to the security of the personal information, the notification of data breaches and privacy impact assessments (PIAs);

5.3.7 the organisation will delete or return all personal information to the Association as requested at the end of the contract; and

5.3.8 the organisation will submit to audits and inspections, provide the Association with whatever information the Association needs to ensure that they are

meeting their data protection obligations, and tell the Association immediately if the organisation is asked to do something that could breach data protection laws.

Before any new agreement involving the handling and use of personal information by an external organisation on behalf of the Association is entered into, or an existing agreement is amended, staff must seek approval of its terms by the DPO.

6.0 PERSONAL INFORMATION STORAGE AND SECURITY

The Association will use appropriate technical and organisational measures (based on its size, available resources, volume of personal information and risks) to keep personal information secure, and to protect against unauthorised or unlawful handling and use and against accidental loss, destruction or damage. These may include:

6.1.1 making sure that, where necessary, personal information is encrypted;

6.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services. Confidentiality means only those who need to know and are authorised to use personal information can access it. Integrity means that the personal information is accurate and suitable for the purpose for which it is handled and used by the Association. Availability means that authorised users can access the personal information when they need it for authorised purposes;

6.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

6.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the handling and use of the personal information.

7.0 DATA SECURITY BREACHES

A data security breach can occur at any point when handling personal information and the Association has reporting duties in the event of such a breach occurring. The Association will handle and respond to data security breaches in accordance with its Data Security Breach Management Policy.

8.0 DATA SUBJECT RIGHTS

8.1 Data subjects have rights when it comes to how the Association handles and uses their personal information. These include rights to:

8.1.1 withdraw consent to the handling and use of their personal information at any time;

8.1.2 receive certain information about the Association's personal information activities;

8.1.3 request access to their personal information that the Association holds about them;

8.1.4 ask the Association to erase their personal information if it is no longer necessary in relation to the purposes for which it was collected or handled and used or to rectify inaccurate personal information or to complete incomplete personal information;

8.1.5 restrict the handling and use of their personal information in specific circumstances;

8.1.6 challenge the handling and use of their personal information by the Association which has been justified based on the Association's legitimate interests;

8.1.7 request a copy of an agreement under which personal information is transferred by the Association to another organisation based outside of the European Economic Area (EEA);

8.1.8 prevent the handling and use of their personal information that is likely to cause damage or distress to the data subject or anyone else;

8.1.9 be notified of a data breach which is likely to result in high risk to their rights and freedoms;

8.1.10 make a complaint to the Information Commissioner's Office (ICO) about the Association's handling and use of their personal information; and

8.1.11 in limited circumstances, receive or ask for their personal information to be transferred to a third party in a structured, commonly used and machine-readable format.

8.2 The identity of the data subject exercising any of the rights listed above must be verified.

8.3 Staff must immediately forward any such request received by them to the DPO. The Association will handle and respond to requests in accordance with its Data Subject Request Policy.

9.0 PRIVACY IMPACT ASSESSMENTS

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

9.2 The Association shall:

9.2.1 Carry out a PIA before undertaking a project or handling and using personal information, particularly using technology, 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 information or the operation of a CCTV system; and

9.2.2 In carrying out a PIA, include a description of the handling and use of personal information, its purpose, an assessment of the need for the handling and use, 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 information.

9.3 The Association will require to consult the ICO if 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 require to notify the DPO within five (5) working days and they must cease from handling and using the personal information immediately.

10.0 ARCHIVING, RETENTION AND DESTRUCTION OF PERSONAL INFORMATION

The Association cannot store and retain personal information indefinitely. It must ensure that personal information is only retained for the period necessary. The Association shall ensure that all personal information is archived and destroyed in accordance with its Data Retention Policy.

11.0 DOCUMENTATION AND RECORDS

11.1 The Association will keep written records of its personal information activities, including:

11.1.1 its name and contact details, including the contact details of the DPO;

11.1.2 the purposes of handling and using personal information;

11.1.3 a description of the categories of data subjects and categories of personal information handled and used by the Association;

11.1.4 categories of recipients of personal information handled and used by the Association;

11.1.5 where relevant, details of transfers to countries outside the EEA, including documentation associated with how the Association protects the personal information after transfer;

11.1.6 how long the Association keeps personal information; and

11.1.7 a description of the technical and organisational security measures that the Association has in place to protect the security of personal information.

11.2 As part of the Association's record of personal information activities, the Association documents:

11.2.1 information required for its FPNs;

11.2.2 records of consent;

11.2.3 controller-processor contracts;

11.2.4 the location of personal information within the Association's systems;

11.2.5 PIAs; and

11.2.6 records of data security breaches.

11.3 If the Association handles and uses sensitive personal information or criminal records information, the Association will keep written records of:

11.3.1 the relevant purpose(s) for which the handling and use takes place, including (where required) why it is necessary for that purpose;

11.3.2 the legal reason for the Association's handling and use; and

11.3.3 whether the Association retains and erases the personal information in accordance with its Data Retention Policy and, if not, the reasons for not following the policy.

11.4 The Association will conduct regular audits of the personal information that it handles and uses and update its documentation accordingly, including by:

11.4.1 distributing questionnaires and interviewing staff to obtain a complete picture of personal information activities; and

11.4.2 reviewing policies, procedures, contracts and agreements to address areas, such as retention, security and information sharing.

11.5 The Association documents its personal information activities in electronic form, so it can add, remove and amend information easily.

12.0 STAFF OBLIGATIONS

12.1 Staff are responsible for keeping their personal information up to date. Staff should let the Association know if the information they have provided to the Association changes, for example, if they move to a new house.

12.2 Staff may have access to a range of personal information during their employment and staff must help the Association to meet its data protection obligations.

12.3 If staff have access to personal information, they must:

12.3.1 only access the personal information that they have authority to access, and only for authorised purposes;

12.3.2 only allow other staff to access personal information if they have appropriate authorisation;

12.3.3 only allow third parties to access personal information if they have specific authority to do so from the DPO or their line manager;

12.3.4 ensure that any sharing of personal information complies with the FPN provided to data subjects and the third party with whom it is shared agrees to put appropriate security measures in place to protect the personal information;

12.3.5 keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other appropriate precautions);

12.3.6 not remove personal information, or devices containing personal information (or which can be used to access it), from the Association's premises, unless appropriate security measures are in place (such as encryption or password protection) to secure the information and the device; and

12.3.7 not store personal information on local drives or on personal devices that are used for work purposes.

12.4 Staff should contact the DPO if they are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

12.4.1 handling and use of personal information without a legal reason;

12.4.2 any data security breach;

12.4.3 access to personal information without the proper authorisation;

12.4.4 personal information not kept or deleted securely;

12.4.5 removal of personal information, or devices containing personal information (or which can be used to access it), from the Association's premises without appropriate security measures being in place; or

12.4.6 any other breach of this Policy.

13.0 INTERNATIONAL TRANSFERS OF PERSONAL INFORMATION

The Association may only transfer personal information outside the EEA on the basis that that recipient country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards so far as data protection is concerned. Further advice must be obtained from the DPO.

14.0 TRAINING

The Association will ensure that staff are adequately trained regarding their data protection responsibilities. Staff whose roles require regular access to personal information will receive additional training to help them understand their duties and how to comply with them.

15.0 CONSEQUENCES OF FAILURE TO COMPLY

15.1 The Association takes compliance with this Policy very seriously. Failure to comply with the Policy:

15.1.1 puts at risk the data subjects whose personal information is being handled and used by the Association;

15.1.2 carries the risk of significant civil and criminal sanctions for the Association; and

15.1.3 may, in some circumstances, amount to a criminal offence by a member of staff.

15.2 Due to the importance of this Policy, failure to comply with any requirement of it may lead to disciplinary action for a member of staff under the Association's procedures, and this action may result in dismissal for gross misconduct. If an external organisation breaches this Policy, they may have their contract terminated by the Association with immediate effect.

15.3 Any questions or concerns about this Policy should be directed to the DPO.

16.0 REVIEW

This policy will be regularly monitored and formally reviewed in accordance with the Association's data protection obligations and the Association may amend, update or supplement it from time to time and at least every 3 years or earlier, if required by changes in legislation.

Anne Smith
Director of Finance and Corporate Services/Depute Chief Executive

September 2019

Policy Review Consultation Process

Considered by the Management Team on	2nd September 2019
Considered by the Finance, Audit & Corporate Governance Committee on	12th September 2019
APPROVED BY THE MANAGEMENT COMMITTEE ON	**26th September 2019**
Date of Next Review	**September 2022**

Appendix 1

Related Policies

Data Breach Management Policy

Information Security Policy

Data Retention Policy

E-mail, Internet and Social Media Policy

Information Technology Systems Code of Conduct

Data Subject Request Policy

Related Documentation

Appendix 2 Fair Processing Notices

Appendix 3 Data Sharing Agreement

Appendix 4 Data Processor Addendum