Policy Name	Data Protection Policy
Policy Category	Corporate & Governance
Policy Number	CG019
Officer Responsible	Chief Executive
Application	Lochaber Housing Association
Date to Board of Management	20th May 2021
Next Review Date	May 2026

1.0 INTRODUCTION AND GENERAL INFORMATION

1.1 The Data Protection Legislation (comprising of the Data Protection Act 2018 and the GDPR) is recognised by many service providers as important in protecting the rights of individuals in respect of any personal data that is kept about them, whether on a computer or in a filing system. As a Registered Social Landlord (RSL), Lochaber Housing Association (the Association) endorses the principles outlined in the Data Protection Legislation, and this procedure outlines our approach in this regard.

1.2 The Association takes all reasonable steps to ensure that our practices in the handling of personal data are of a high standard and comply with the Data Protection Legislation. This includes, for example, using self-assessment and internal audit to help flag up areas requiring attention.

1.3 This Data Protection Policy (this Policy) is intended for use by the Association's staff:

- when processing any personal data, including collecting, accessing, using, sharing or amending personal data as part of their day-to-day activities;
- when they are faced with a request from a data subject that relates to their personal data, whether this be a tenant or sharing owner or factored owner telephoning to enquire about their own rent account or a request for information on a tenancy matter from a third party, such as the Department for Work and Pensions (DWP) or a complaint regarding how their personal data is used by the Association; or
- when they require guidance on what personal data should be retained (and for how long) once it is no longer relevant to the Association carrying out its day-to-day business.

1.4 In drafting this Policy, the Association has tried to cover the vast majority of ways in which personal data is likely to be requested or retained. Exceptionally, however, the procedure may be silent on how to deal with a query that is made. In such circumstances, the Data Protection Officer will decide on whether the disclosure is to be made/information to be retained – with appropriate legal advice in cases where this is considered advisable.

1.5 The following is a glossary of key terms in the Data Protection Legislation:

- Information Commissioner's Office (the ICO) – the ICO is the body responsible for enforcing and monitoring compliance with the Data Protection Legislation in the UK;
- controller – the organisation that determines the purposes for which, and manner in which personal data is used, in our case, the Association;
- data subject – this refers to any living individual who the personal data relates to. Examples of data subjects that the Association holds personal data for are: tenants, whether former, current or prospective, board members, staff, owner occupiers, suppliers, contractors and individuals who interact with the Association;
- personal data – this is information that relates to and identifies (either directly or indirectly) an individual from information which is held by the Association. It also includes any expression of opinion or view about an individual or their circumstances. Examples of personal data relating to individuals includes their name, age, data of birth, contact details, marital status, housing history, financial status and allowance benefits and grants claimed;
- special category personal data – this is personal data revealing an individual's: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, and genetic or biometric data where processed for the purpose of uniquely identifying an individual;
- processing – any operation performed on personal data, including obtaining, recording, storing, using, disclosing and deleting; and
- processor – the organisation that processes personal data on behalf of the controller.

1.6 In this Policy, "GDPR" means the retained EU law version of the General Data Protection Regulation (EU) 2016/679) (EU GDPR) as it forms part of the law of Scotland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time).

2.0 DATA PROTECTION PRINCIPLES

2.1 The Association will operate in accordance with the principles outlined in the Data Protection Legislation. Personal data held by the Association will therefore be:

(i) obtained and processed lawfully, fairly and in a transparent manner;

(ii) obtained only for specified, explicit and legitimate purposes, and will not be used for any other purpose;

(iii) adequate, relevant and limited to what is necessary in relation to the purpose for which it is obtained or kept;

(iv) accurate and, where necessary, kept up-to-date;

(v) kept in a form which permits identification of individuals for no longer than is necessary for the purpose; and

(vi) handled in a manner ensuring appropriate security including protection against unlawful processing or accidental loss, destruction or damage.

(vii) care is taken when emailing information in that the correct recipient is selected from the address book

(viii) care should be exercised within the content of the email to ensure that no data is forwarded that would breach data protection legislation

The Data Protection Legislation also includes a principle of 'accountability', which requires the Association to take responsibility for its data processing and to be able to demonstrate compliance with the above data protection principles.

3.0 RESPONSIBILITIES FOR COMPLIANCE

3.1 The Data Protection Officer has overall responsibility for data protection within the Association, and for ensuring that our entry in the ICO's Register is accurate and up to date. This will be checked annually upon renewal.

3.2 The Data Protection Officer will also assist in implementing the requirements of the Data Protection Legislation by:

- providing advice and support to all departments on all matters relating to compliance with the Data Protection Legislation;
- disseminating information relating to the Data Protection Legislation; and
- responding to requests from data subjects in relation to the personal data that the Association holds about them.

3.3 Staff will be informed about data protection issues, and their rights in relation to their own personal data. Separate guidance relating specifically to the Association as an employer has been issued by EVH and this should be referred to where required.

3.4 All staff have a responsibility to fully comply with the requirements of the Data Protection Legislation and this Policy. When involved in collecting personal data, staff will explain how the Association will use the information by providing a copy of or access to the Association's privacy notice.

4.0 DAILY USE OF THIS POLICY

Disclosure of Information

4.1 As a general rule of thumb, the Association should not disclose information about someone to a third party without providing the individual with a privacy notice that clearly explains the disclosure. A data subject must be given access to

a privacy notice when the Association collects their personal data (or within one month of receiving personal data if not received directly from data subject).

4.2 Staff do, however, regularly have to disclose personal data about someone to:

- the person themselves;
- their legal appointee; or
- someone acting on their behalf.

4.3 The critical point for staff is to ensure that, prior to disclosure, they are satisfied that the person asking for the information is being truthful about their identity (and steps have been taken to verify their identity where appropriate) and, where the enquirer is not the tenant, that the Association can legally disclose the data subjects personal data to them.

4.4 The Association will therefore adopt the "key question" approach already used by many companies in the UK. This involves the tenant having to respond correctly to a unique question that they would definitely know the answer to, for example, what is your date of birth? Where the enquirer is not the tenant, but a representative, staff must ensure that:

- there is a signed mandate on file;

AND

(a) the key questions can be answered (in the case of a friend or relative);

OR

(b) the staff member can check the telephone number and call back (in the case of another agency or professional representative).

4.5 Where there is any uncertainty, referral should be made to the Data Protection Officer.

4.6 All contractors, consultants, partners or other associates or agents of the Association that process personal data on behalf of the Association as processors must be subject to written contractual obligations regarding how they use such personal data before any personal data is disclosed. Staff should always check with Corporate Services before disclosing any personal data to such contractors, consultants, partners or other associates or agents.

Basis and purposes for processing personal data

4.7 Before any personal data is processed by the Association for the first time, the Association will:

- review the purposes of the particular processing activity and select the most appropriate lawful basis under the Data Protection Legislation. The lawful bases most commonly used by the Association are that:

  (a) the individual has consented – this is only appropriate where it is not a precondition of a service or another lawful basis applies and does not apply to staff personal data;

(b) the processing is necessary for the performance of or to take steps to enter into a contract with the individual – this will apply to our tenants, staff and individuals requesting services from the Association;

(c) the processing is necessary to comply with a legal obligation – the Association needs to process certain personal data under law, such as staff personal data for HMRC reporting purposes and tenant personal data under the housing legislation in Scotland;

(d) the processing is necessary to perform a task in the public interest or official authority vested in the Association – this will relate to processing required for the Association's functions as a RSL; or

(e) the processing is necessary for the Association's or a third party's legitimate interests – provided that the legitimate interests are not overridden by the interests of the individual and does not relate to the Association's public functions as a RSL;

where special category personal data is involved in the processing activity, identify the most appropriate special condition for processing in addition to a lawful basis above. Although there are others, the special conditions most commonly used by the Association are that:

(a) the individual has explicitly consented – this is only appropriate where it is not a precondition of a service or another lawful basis applies and does not apply to staff personal data;

(b) the processing is necessary for the Association to perform our obligations or exercise rights under employment law – this would apply to staff personal data, for example, to maintain attendance and performance records;

(c) the processing is necessary for the Association to establish, exercise or defend legal claims; or

(d) the processing is necessary for substantial public interest reasons – such as the Association exercising our statutory functions, equality monitoring, health or social care purposes, or preventing / detecting unlawful acts;

- always ensure that the Association's decision as to which lawful basis applies is documented, to help demonstrate compliance with the data protection principles;
- information about the purposes, lawful basis and special condition (if applicable) of the processing can be found within the relevant privacy notice provided to individuals.

Retaining Information

4.8 The Association will only retain personal data about a data subject when this is required in order for day-to-day business to be undertaken. The Document Retention Schedule provides the detail on the type of information the Association retains, together with details of the retention period.

4.9 All personal data is treated as both confidential and sensitive by the Association. This means that access to it will be strictly controlled and will be on a "need to know" basis – this also applies to access by the Association's staff. "Need to know" would cover, for example, a member of staff acting on a colleague's behalf when that person is not available, such as to discuss an application for housing.

4.10 Personal data is stored securely. Where this is in paper files, these are placed in lockable cabinets when not in use; computer files are password protected.

4.11 It is unavoidable that, from time to time, files and other information may have to be removed from the Association's office, for example, to carry out a house visit. Staffs are required to take the utmost care not to misplace or lose any personal data and report any losses immediately in accordance with Section 6 of this Policy.

Documentation and records

4.12 The Association keeps written records of processing activities, including:

- the name and details of the Association;
- the purposes of the processing of personal data by the Association;
- a description of the categories of individuals and categories of personal data processed by the Association;
- categories of recipients of personal data with whom the Association shares personal data;
- if we are required to transfer personal information outwith the EU, we will provide information regarding the safeguards that we have put in place with the recipient country to protect the personal information;
- details of how long the Association keeps personal data in line with the retention periods set out in the Document Retention Schedule; and
- a description of technical and organisational security measures put in place to keep personal data secure.

5.0 DATA SUBJECT RIGHTS

5.1 Data subjects have the following rights in relation to their personal data held by the Association:

- right to be informed - data subjects have the right to be informed about how, why and on what basis that personal data is processed – the Association will issue and make accessible privacy notices from

time to time in a concise, transparent, intelligible and easily accessible form, using clear and plain language;

- right of access – data subjects have the right to obtain confirmation that their personal data is being processed by the Association and to obtain access to it and certain other information, by making a Subject Access Request (SAR);
- right to rectification – data subjects have the right to have personal data corrected if it is inaccurate or incomplete. The Data Protection Legislation states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact;
- right to erasure – data subjects have the right to have their personal data erased in certain circumstances;
- right to object – data subjects have the right to object to the processing of their personal data where the Association carries out the processing for certain purposes;
- right to data portability – data subjects have the right to obtain personal data provided to the Association by the individual for that individual's own reuse;
- rights in relation to automatic decision making – data subjects have the right to object to decisions being taken by automated means which produce legal effects concerning an individual or similarly significantly affect an individual; and
- right to restrict processing – data subjects have the right to restrict the processing of personal data in certain circumstances.

5.2 Data Subjects are permitted to view their personal data held by the Association in either written or electronic form upon making a request to do so by making a SAR. Upon receipt of a request by a data subject, the Association must respond to the SAR within one month of the date of receipt of the request. The Association:

- must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies by law (for example, where the information includes personal data of third parties) and include information on how the personal data provided is processed by the Association; or

- where the Association does not hold the personal data sought by the data subject, must confirm that is does not hold any of the requested personal data to the data subject as soon as practically possible, and in any event, not later than one month form the date on which the request was made.

5.3 Where staff receive a request from an individual that relates to their personal data and they are not authorised to handle such a request, staff must immediately notify the Data Protection Officer of the request. The Data Protection Legislation only gives the Association 30 days to respond to requests so staff should not delay in notifying the Data Protection Officer.

5.4 Data subjects can seek to exercise the above rights against the Association in writing, by email or verbally. Such requests do not have to refer to the legislation, 'data protection' or 'personal data' and often requests may cite the incorrect legislation (for example, they may refer to 'freedom of information' where they are seeking access to their own personal data). The Association must ensure that we recognise requests under the Data Protection Legislation so that the Association complies with the relevant statutory obligations.

5.5 More information on data subject rights is included within the Association's data subject requests procedure.

6.0 PERSONAL DATA BREACHES

6.1 A personal data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal data is stored;
- unauthorised access to or use of personal data either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the Association.

6.2 The Association will:

- where required, report a personal data breach to the ICO without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- notify the affected data subjects immediately if a personal data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

6.3 It is important that staff report any suspected or actual personal data breach to the Data Protection Officer immediately. The Data Protection Officer will be responsible for recording and reporting personal data breaches and staff should not notify either the ICO or data subjects themselves under any circumstances.

7.0 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

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

7.2 The Association shall: carry out a DPIA before undertaking a project of 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 the Association will adapt the template produced by ICO when completing a DPIA.

7.3 In the event that the DPIA identifies a high level of risk which cannot be reduced the Data Protection Officer will be responsible for consulting with the ICO as required under the Data Protection Legislation.

8. ROLE OF INTERNAL AUDIT DATA PROTECTION

8.1 Failure to observe practices that help the Association comply with the Data Protection Legislation could expose the Association to a certain degree of risk. Keeping this Policy up to date and ensuring that staff are aware of its contents is one way of helping guard against any legal breaches. As an added safeguard, the internal auditors will be required to comment on data protection at least once in every three years.

9. BREACH OF THIS POLICY

9.1. This Policy is mandatory and therefore any employees, including others who obtain, handle, process and share personal data on behalf of the Association, must adhere to the rules of this Policy. Any breach of this Policy will be taken seriously and may result in disciplinary action (in the case of an employee) and / or personal criminal liability for data subjects involved in negligent or deliberate breaches. Failure by staff to comply with this Policy could amount to misconduct, which is a disciplinary matter.

9.2. A failure to comply with this Policy could also expose the Association to enforcement action by the ICO, which could result in monetary penalties being issued against the Association and to complaints and claims for compensation from affected data subjects being made against the Association. There may also be negative publicity as a result of a breach that is made public.

9.3. The Association may review or amend this Policy at any time and will inform its staff of any amendments.