PORT OF LEITH
HOUSING ASSOCIATION

DATA MANAGEMENT POLICY 2018 (revised 2019)

FULL REVIEW TRACKING

Policy Owner	Director of Finance and Corporate Services
Document Author(s)	ICT Manager
Communication & Training Methods	Training will be provided to all staff through mandatory sessions. The employee induction process will be updated to include data protection session.
Date Last Approved	May 2018
Approved By	Leadership Team
Review Cycle	3 yearly
Next Review Date	June 2021
The Policy has a direct link to the following PoLHA policies and procedures	IT Security Policy Procurement Procedures CCTV and Call Recording Policy
This policy complies with the requirements of these legal and/or regulatory documents	General Data Protection Regulations (EU); Privacy and Electronic Communications Regulations (EU) Freedom of Information (Scotland) Act 2002 The Freedom of Information (Scotland) Act 2002 (Designation of Persons as Scottish Public Authorities) Order 2019

REVISION TRACKING

Revisions are minor changes which are made between Full Reviews which might be needed because of new ideas or changes

Revision Date	Part of doc revised	Reason for revision	Approved by
01/10/2019	Section 14 – new section on Managing Email	Extension of FoISA act to RSLs and the implications of keeping out-of-date records.	LT

1. BACKGROUND / INTRODUCTION

1.1 The Association and subsidiary companies must comply with the EU General Data Protection Regulations, henceforth referred to as (the) GDPR, effective from 25 May 2018.

1.2 The GDPR applies to 'personal data' meaning any information relating to a living identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

1.3 This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier.

1.4 The GDPR has the concept of "special category" personal data. Under GDPR personal data in this category is: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.

1.5 For the purposes of GDPR, children are classed as individuals under the age of 13. Children have the same rights as adults over their personal data.

1.6 The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

2. POLICY STATEMENT

2.1 The Association is committed to a policy of protecting the rights and privacy of individuals in accordance with the GDPR.

2.2 The Association will maintain registration with the Information Commissioner's Office, henceforth referred to as (the) ICO, in accordance with the requirements of the GDPR.

2.3 The Association will translate any of its documents into alternative formats and will translate documents into other languages on request.

3. SCOPE AND APPLICABILITY

3.1 The GDPR applies to 'controllers' and 'processors':

- A controller determines the purposes and means of processing personal data. Port of Leith Housing Association is the controller for the Association and all subsidiary companies
- A processor is responsible for processing personal data on behalf of a controller (ie a third party such as a contractor, mail bureau).

3.2 The GDPR places specific legal obligations on the Association (and its staff) as a controller. For example, the Association is required to maintain records of personal data and processing activities.

3.3 The GDPR places further obligations on the Association to ensure our contracts with processors comply with the GDPR.

3.4 The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

3.5 The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

4. SPECIFIC RESPONSIBILITIES

4.1 The Director of Finance and Corporate Services

4.1.1 The Director of Finance and Corporate Services has overall responsibility for data protection within the Association, and for ensuring that our registration with the ICO is accurate and up-to-date.

4.1.2 The Director of Finance and Corporate Services has specific responsibility for personal information held on employees. The Association will comply with all current Codes of Practice on Recruitment, Employee Records, Monitoring at Work and Information on Employees Health. Staff will be informed about data protection issues, and their rights to access their own personal data through the staff handbook and induction courses.

4.2 Departmental Directors

4.2.1 All Directors will assist in implementing the requirements of the GDPR by:

- Providing support to all departments on all matters relating to compliance with the GDPR
- Disseminating information relating to the GDPR
- Responding to requests from individuals to access personal information we hold about them.

4.3 Operational Managers

Operational Managers must ensure that:

- Personal data processed by their department is included in the Association's "Record of Data Processing Activities" (Appendix I), is supported by a lawful basis and is processed in accordance with the principles of the GDPR
- Data subjects are made aware of the Association's data processing
- Subject access requests from individuals are responded to within one calendar month of the request, unless a legitimate reason not to do so exists

- Data sharing agreements are in place with third-party organisations, and that third-party organisations have appropriate policies and procedures in place to safeguard data that is shared
- Data breaches, or suspected data breaches, are reported to the Director of Finance and Corporate Services without delay
- Data processing consent records are maintained
- Data Privacy Impact Assessments are conducted.

4.4 The ICT Manager

The ICT Manager is specifically responsible for:

- Maintaining the Association's technical security measures
- Providing advice to colleagues on data protection matters
- Co-ordinating the technical response to suspected and confirmed data breaches.

4.5 All Staff

4.5.1 All staff have a responsibility to fully comply with the requirements of the GDPR and this policy.

5. PRINCIPLES OF THE GDPR

5.1 The principles for processing personal data under the GDPR are as follows:

5.2 Personal data shall be:

a. Processed lawfully, fairly and in a transparent manner in relation to individuals
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes will be compatible with the initial purposes

c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

e. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to

implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

f. 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.

6. Lawful Basis

6.1 The Association must have a valid lawful basis in order to process personal data.

6.2 There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the Association's purpose and relationship with the individual.

6.3 Most lawful bases require that processing is 'necessary'. If the Association can reasonably achieve the same purpose without the processing, it will not have a lawful basis.

6.4 The Association will determine the lawful basis before processing begins, and this will be documented in this policy **(Appendix I).** The Association will not use a different lawful basis at a later date without good reason.

6.5 The Association's privacy notice will include the lawful basis for processing as well as the purposes of the processing.

6.6 When processing special category data the Association will identify both a lawful basis for general processing and an additional condition for processing this type of data.

6.7 **Consent**: the individual has given clear consent for the Association to process their personal data for a specific purpose. (It is not permissible for a child to consent to data processing. Parental consent is required if this is the lawful basis for processing the personal data).

6.8 **Contract**: the processing is necessary for a contract the Association has with the individual, or because they have asked the Association to take specific steps before entering into a contract.

6.9 **Legal obligation**: the processing is necessary for the Association to comply with the law (not including contractual obligations).

6.10 **Vital interests**: the processing is necessary to protect someone's life.

6.11 **Public task**: the processing is necessary for the Association to perform a task in the public interest or for the Association's official functions, and the task or function has a clear basis in law.

6.12 **Legitimate Interests**: the processing is necessary for the Association's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply when the Association classed as a public authority processing data to perform official tasks).

7. Individual Rights

7.1 The GDPR provides the following rights for individuals:

- **The right to be informed:** The Association will provide data subjects with a privacy notice and will strive to be completely transparent over how personal data is used
- **The right of access:** Upon request, the Association will confirm to an individual that their personal data is being processed and within one calendar month provide access to any relevant records. Requests should be made through the Association's "Data Subject Access Request" form
- **The right to rectification:** The Association will rectify any inaccurate information once made aware of the inaccuracy
- **The right to erasure:** The Association will consider requests for the deletion or removal of personal data, and will process the deletion should there be no grounds preventing deletion (see the ICO website for grounds for refusal)
- **The right to restrict processing:** The Association will restrict processing of personal data in the following circumstances:

    1. Where the accuracy of personal data has been contested by the individual
    2. Where the individual has objected to the processing and the Association is considering a response
    3. When processing is unlawful and the individual opposes erasure and requests restriction instead
    4. When personal data is no longer needed by the Association but the individual requires the data to establish, exercise or defend a legal claim.

- **The right to data portability**: The right to data portability requires data controllers to transfer data to a new service provider upon request. This right is not relevant to the data sets and purposes which the Association uses
- **The right to object**: Data subjects have the right to object to the Association processing their personal data. This right is unlikely to be relevant to the data sets and purposes which the Association uses
- **Rights in relation to automated decision making and profiling**: As the Association does not currently have processes involving automated decision making and profiling, this right is not relevant to the Association.

7.2 If a data subject wishes to exercise any of their rights under the GDPR, please notify the Operational Manager in your department. The CCTV and Call Recording policy and procedures should be followed when dealing with the subject access request.

8. Accountability and Governance

8.1 The Association's accountabilities and governance for data protection are laid out in Section 4 of this policy.

8.2 When the Association uses a third party (a data processor) to process personal data a written contract with the processor is required to fulfil the obligations of the GDPR. The data sharing agreement must contain the following:

- The subject matter and duration of the processing
- The nature and purpose of the processing
- The type of personal data and categories of data subject
- The obligations and rights of the controller.

8.3 The Association holds a template for data sharing which should be used when transferring data to a third party.

8.4 The datasets that we share, along with whom we share, is listed in Appendix I.

9. Security

9.1 The Association will ensure that personal data is processed in a secure manner, and has data breach detection software in place.

9.2 The Association's IT Security Policy provides a full record of technical and organisational measures used to protect personal data.

10. International Transfers

10.1 The Association does not permit the transfer personal data outside the European Union. Additionally, the Association's data-sharing agreements with third-party organisations expressly forbids data processors transferring data that the Association controls outside the European Union.

11. Personal Data Breaches

11.1 Where a data breach is likely to risk people's rights and freedoms, the GDPR introduces a duty on the Association to report any personal data breach to the ICO. This must be done within 72 hours of becoming aware of the breach, where feasible.

11.2 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will inform those individuals without undue delay.

11.3 The Association will keep a record of any personal data breaches, regardless of whether we are required to notify.

12. Data Protection Officer

12.1 The Association has appointed a Data Protection Officer to comply with the GDPR.

13. Privacy by Design and Data Privacy Impact Assessments

13.1 Under GDPR the Association has a requirement to take a "privacy by design" approach to minimise risks. This involves designing processes, products or systems with privacy in mind. The key tool for the Association in adopting "privacy by design" is the use of Data Protection Impact Assessments (DPIAs).

13.2 Under GDPR, DPIAs are required when:

- using new technologies
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

13.3 Examples of high risk processing provided by the ICO include:

- systematic and extensive processing activities, including profiling, and where decisions have legal effects – or similarly significant effects – on individuals
- large scale processing of special categories of data or personal data in relation to criminal convictions or offences. This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms eg based on the sensitivity of the processing activity
- large scale, systematic monitoring of public areas (CCTV)

13.4 When reviewing policies or developing project initiation documents, staff will evaluate the requirement for privacy impact assessment using the Association's DPIA framework.

14. Managing Email

14.1 Emails may need to be considered when we handle information requests under GDPR and Freedom of Information. Emails should be drafted carefully (ie be brief, factual and polite) and time should be taken to review the content of an email before it is sent.

14.2 It is the responsibility of all staff to manage their emails appropriately. Staff members should identify emails **(sent and received)** that are significant corporate records and move them from personal mailboxes to a shared mailbox relevant to a specific department or the "Contact Management" system on QL. **Personal mailboxes should not be used as a filing area for official Association documents.**

14.3 Ultimately the decision on whether an email is classed as a significant corporate record is a judgement call that each individual will have to make. If an email is evidence of a business transaction, a decision taken, a negotiation or dealings with a customer/client, it is likely to be a significant corporate record.

14.5 When managing emails in a shared mailbox, the relevant owner (typically manager or director) is responsible for ensuring that the appropriate retention and filing of emails is conducted.

14.6 It is the responsibility of all staff and Board Members to ensure that sensitive data is kept secure and is always protected. The privacy and confidentiality of information sent outside the Association's network by email cannot be guaranteed, even in cases where encrypted email systems are in place. Care must therefore be taken when using email to communicate.

14.7 Emails that are either personal or not classed as significant corporate records should be deleted once they are no longer required.

14.8 The email server is configured to delete all emails stored in Outlook personal mailboxes and any Association archive folders after one year.

GLOSSARY:

Personal Mailboxes: The personal mailbox is the email account that is assigned to a named member of staff. The contents relate to all email, calendar items, tasks and notes that are visible to the member of staff when using Outlook.

Shared Mailboxes: Shared mailboxes are available through Microsoft Outlook, and as the name suggests are accessible by authorised individuals.

Encrypted Email Systems: Messages with some external bodies are sent and received using an encryption system. This makes the email unreadable whilst in transit from one email system to another. However, once unencrypted by the recipient, the content of the email can be forwarded on in an insecure format.

APPENDIX I

Record of Data Processing Activities

Data Set	Purpose(s)	Responsibility	Data Subjects	Transfers/ Disclosures to third parties (who, where, contract)	Lawful Basis
Payroll/staff Records	to enable payment of staff (salary and sick pay)	HR Manager	All employees	Payroll supplier based in UK, contract contains data processing provisions	CONTRACT Processing is necessary for the performance of the contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering the contract
Tenant Record	to enable the association to deliver services to the customer	Housing Manager/Customer Advice Manager	All current tenants (MMR, Social and Shared)	Part of this data is passed to different agencies including Allpay, TB Mackays, City of Edinburgh Council, Support agencies, Police Scotland and other repairs contractors	CONTRACT Processing is necessary for the performance of the contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering the contract

Data Set	Purpose(s)	Responsibility	Data Subjects	Transfers/ Disclosures to third parties (who, where, contract)	Lawful Basis
Tenant Record	to ensure the Association meeting the legislation it is operating under	Housing Manager/Customer Advice Manager	All current tenants (MMR, Social and Shared)	Part of this data is passed to different agencies including Allpay, TB Mackays, City of Edinburgh Council, Support agencies, Police Scotland and other repairs contractors	LEGAL OBLIGATION Processing is necessary for compliance with a legal obligation to which the controller is subject
Former Tenant Records	To enable the Association to deliver services to the customer and ensure it's meeting the legislation it is operating within	Housing Manager/Customer Advice Manager	Former tenants (MMR, Social and Shared)	Part of this data is passed to different agencies including, Allpay, TB Mackays, City of Edinburgh Council, Support agencies, Police Scotland and other repairs contractors	LEGAL OBLIGATION Processing is necessary for compliance with legal obligation to which the controller is subject. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party
Community Works Service Users records	To enable the Association to deliver services to its Community Works customers	CW manager	Current Community Works service users	Only with express permission of the service user and for Health and Safety purposes ie to a prospective employer or support agency.	CONSENT The data subject has given consent to the processing of their personal data for one or more specific purposes

Data Set	Purpose(s)	Responsibility	Data Subjects	Transfers/ Disclosures to third parties (who, where, contract)	Lawful Basis
Former Community Works Service users records	To track outcomes. Minimum information required will be name of service user, date of progression and nature of progression (eg full time job as a shop assistant).	CW Manager	Former Community Works service users	Employers but only with the express permission of the user.	CONSENT The data subject has given consent to the processing of their personal data for one or more specific purposes
Tenant Support Service Users records	To enable the Association to deliver services to its customers	Housing Manager	Current TSS service users	Yes – consent mandate completed. Information shared with DWP; CEC; creditors; support agencies	CONSENT The data subject has given consent to the processing of their personal data for one or more specific purposes
Former Tenant Support Service users records	n/a – information not kept for former tenants	Housing Manager	Former TSS service users	No	CONSENT The data subject has given consent to the processing of their personal data for one or more specific purposes

Data Set	Purpose(s)	Responsibility	Data Subjects	Transfers/ Disclosures to third parties (who, where, contract)	Lawful Basis
Members information	To provide information allowing the Association to send information to the member	Corporate Services Manager	Members of the Association	No	LEGITIMATE INTERESTS Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except whose such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.
Job applicants information	To allow the Association to assess a job application in line with its recruitment and selection policy, demographic information is held to monitor that the Association is getting a pool of applicants from across many different backgrounds	Corporate Services Manager	Applicants	This information is mainly used by the Association but can be passed to different agencies when testing is required	LEGITIMATE INTERESTS Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party expect whose such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

Data Set	Purpose(s)	Responsibility	Data Subjects	Transfers/ Disclosures to third parties (who, where, contract)	Lawful Basis
Board of Management Information	To allow the Association to contact the Board Members with relevant information regarding the board meetings, ethnic origin information is used for monitoring	Corporate Services Manager	Board Members	This information is used to send Board papers and correspondence to Board Members	LEGITIMATE INTERESTS Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party expect whose such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

Data Set	Purpose(s)	Responsibility	Data Subjects	Transfers/ Disclosures to third parties (who, where, contract)	Lawful Basis
Factored owners information	Required to gain consent for works, keep owners informed of statutory obligations, bill factored owners for services and keep a record of the factoring conditions for the development as votes are taken.	Maintenance Manager	Factored owners	Name, property address and voting record needs to be kept in perpetuity as we need to document formal decisions taken by the owners about communal assets and these decisions form part of the factoring conditions for the block. Other owners who have joint liability may in some situations be given information about outstanding debt. Contact information is private to the individual owner.	LEGAL OBLIGATION Processing is necessary for compliance with a legal obligation to which the controller is subject
Former factored owners information	To document scheme decisions that permanently affect the factoring conditions at the development	Maintenance Manager	Factored owners	Other owners	LEGAL OBLIGATION Processing is necessary for compliance with a legal obligation to which the controller is subject

Data Set	Purpose(s)	Responsibility	Data Subjects	Transfers/ Disclosures to third parties (who, where, contract)	Lawful Basis
Tenants household records	Ensure property is suitable for family composition. Also allow the Association to serve legal notices on household when required.	Housing Manager	Tenants	Part of this data is passed to different agencies including Allpay, TB Mackays, City of Edinburgh Council, Support agencies, Police Scotland	LEGAL OBLIGATION Processing is necessary for compliance with a legal obligation to which the controller is subject
Private owners (where POLHA not appointed Factor)	To allow us to arrange communal works with our neighbours when there is no managing agent; sometimes we will sign contracts to manage the project too.	Maintenance Manager	Private Owners	None	LEGAL OBLIGATION Processing is necessary for compliance with a legal obligation to which the controller is subject

Data Set	Purpose(s)	Responsibility	Data Subjects	Transfers/ Disclosures to third parties (who, where, contract)	Lawful Basis
Mid Market Rent Applications	To check the applicant meets the criteria for Mid Market Rent.	Customer Advice Manager	Applicants	We send Endsleigh information for credit checks. We complete an online form containing full name, date of birth, email, mobile, of applicant, potential address of property for rent, rent per calendar month. Bank Information is given to Allpay via website to set up Direct Debit for rent.	LEGITIMATE INTERESTS Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party expect whose such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.
Contractors/ Single persons	Pay for goods and services received	All	Contractor	BACS payments	LEGAL OBLIGATION Processing is necessary for compliance with a legal obligation to which the controller is subject
CCTV footage	Safety and security of tenants	Maintenance Manager	Customers and staff	Police Scotland (upon completion of paperwork)	LEGITIMATE INTERESTS Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party expect whose such interests are overridden by the interests or fundamental rights and freedoms of the data subject

Data Set	Purpose(s)	Responsibility	Data Subjects	Transfers/ Disclosures to third parties (who, where, contract)	Lawful Basis
					which require protection of personal data.
Call recording	Quality assessment service delivery of Customer Advice Team, investigate complaints, investigate unacceptable behaviour	Customer Advice Manager	Staff and any callers to Customer Advice telephone lines		LEGITIMATE INTERESTS Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party expect whose such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

APPENDIX II

PRIVACY NOTICE – FOR CUSTOMERS

HOW WE USE YOUR PERSONAL INFORMATION

This notice explains what information we collect, when we collect it and how we use it. During the course of our activities we will process personal data (which may be held on paper, electronically, or otherwise) about you and we recognise the need to treat it in an appropriate and lawful manner. The purpose of this notice is to make you aware of how we will handle your information.

Who are we?

Port of Leith Housing Association, a Scottish Charity (Scottish Charity Number SC027945), and having their Registered Office at 108 Constitution Street, Leith, Edinburgh, EH6 6AZ ("**we**" or "**us**") take the issue of security and data protection very seriously and strictly adhere to guidelines published in the [Data Protection Act of 1998] and the General Data Protection Regulation (EU) 2016/679 which is applicable from 25 May 2018, together with any domestic laws subsequently enacted.

We are notified as a Data Controller with the Office of the Information Commissioner under registration number Z5626639 and we are the data controller of any personal data that you provide to us.

Any questions relating to this notice and our privacy practices should be addressed to the Association's Chief Executive.

How we collect information from you and what information we collect

We collect information about you:

- when you apply for housing with us, become a tenant, request services/ repairs, enter into a factoring agreement with us or otherwise provide us with your personal details
- when you apply to become a member
- when you use our online services, whether to report any tenancy/ factor related issues, make a complaint or otherwise
- when you make arrangements to make payment to us (such as bank details, payment card numbers, employment details, benefit entitlement and any other income and expenditure related information).

We collect the following information about you:

- name
- address
- telephone number
- e-mail address
- National Insurance Number

- Next of Kin
- Details of any dependents.

We receive the following information from third parties:

- Benefits information, including awards of Housing Benefit/ Universal Credit
- Payments made by you to us
- Complaints or other communications regarding behaviour or other alleged breaches of the terms of your contract with us, including information obtained from Police Scotland
- Reports on the conduct or condition of your tenancy, including references from previous tenancies, and complaints of antisocial behaviour
- Medical information for the purposes of managing your tenancy.

Why we need this information about you and how it will be used

We need your information and will use your information:

- to undertake and perform our obligations and duties to you in accordance with the terms of our contract with you
- to enable us to supply you with the services and information which you have requested
- to enable us to respond to your repair request, housing application and complaints made
- to analyse the information we collect so that we can administer, support and improve and develop our business and the services we offer
- to contact you to send you details of any changes to our suppliers which may affect you
- for all other purposes consistent with the proper performance of our operations and business
- to contact you for your views on our products and services.

Sharing of your information

The information you provide to us will be treated by us as confidential and will be processed only by our employees within the UK/EEA. We may disclose your information to other third parties who act for us for the purposes set out in this notice or for purposes approved by you, including the following:

- If we enter into a joint venture with or merge with another business entity, your information may be disclosed to our new business partners or owners
- If we instruct repairs or maintenance works, your information will be disclosed to any contractor

- If we are investigating a complaint, information may be disclosed to Police Scotland, local authority departments, Scottish Fire & Rescue Service and others involved in any complaint, whether investigating the complaint or otherwise
- If we are updating tenancy details, your information may be disclosed to third parties (such as utility companies and the local authority)
- If we are investigating payments made or otherwise, your information may be disclosed to payment processors, the local authority and the Department of Work & Pensions
- If we are conducting a survey of our products and/or service, your information may be disclosed to third parties assisting in the compilation and analysis of the survey results
- Health and Safety Executive and Scottish Public Services Ombudsman.

Unless required to do so by law, we will not otherwise share, sell or distribute any of the information you provide to us without your consent.

Transfers outside the UK and Europe

Your information will only be stored within the UK and EEA.

Security

When you give us information we take steps to make sure that your personal information is kept secure and safe.

How long we will keep your information

We review our data retention periods regularly and will only hold your personal data for as long as is necessary for the relevant activity, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you.

We will generally keep your information for the minimum periods set out in our retention policy, after which this will be destroyed if it is no longer required for the reasons it was obtained.

Your rights

You have the right at any time to:

- ask for a copy of the information about you held by us in our records
- require us to correct any inaccuracies in your information
- make a request to us to delete the personal data we hold about you
- object to receiving any marketing communications from us.

If you would like to exercise any of your rights above please contact us at info@polha.co.uk.

You also have the right to complain to the Information Commissioner's Office in relation to our use of your information. The Information Commissioner's contact details are noted below:

The Information Commissioner's Office – Scotland

45 Melville Street, Edinburgh, EH3 7HL

Telephone: 0131 244 9001

Email: Scotland@ico.org.uk

The accuracy of your information is important to us - please help us keep our records up to date by informing us of any changes to your email address and other contact details.

APPENDIX III

RETENTION PERIODS

The Association has adopted the Scottish Federation of Housing Association's guidance on retention periods. These are as follows:

Type of record	Retention time
Membership records	5 years after last contact
Personal files including training records and notes of disciplinary and grievance hearings	5 years to cover the time limit for bringing any civil legal action, including national minimum wage claims and contractual claims
Redundancy details, calculations of payments, refunds	6 years from the date of the redundancy
Application forms, interview notes	Minimum 6 months to a year from date of interviews. Successful applicants' documents should be transferred to personal file
Documents proving the right to work in the UK	2 years after employment ceases
Facts relating to redundancies	6 years if less than 20 redundancies. 12 years if 20 or more redundancies
Payroll	3 years after the end of the tax year they relate to
Income tax, NI returns, correspondence with tax office	At least 3 years after the end of the tax year they relate to
Retirement benefits schemes – notifiable events eg relating to incapacity	6 years from end of the scheme year in which the event took place
Pensioners records	12 years after the benefit ceases
Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence	3 years after the end of the tax year to which they relate
Parental Leave	18 years
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years
Wages/salary records, expenses, bonuses	6 years
Records relating to working time	2 years from the date they were made

Type of record	Retention time
Accident books and records and reports of accidents	3 years after the date of the last entry
Health and Safety assessments and records of consultations with safety representatives and committee	Permanently
Health records	During employment and 3 years thereafter if reason for termination of employment is connected to health
Board Members Documents	5 years after cessation of membership
Documents relation to successful tenders	5 years after end of contract
Documents relating to unsuccessful form of tender	12 months after notification
Applicants for accommodation	5 years
Housing Benefits Notifications	Duration of tenancy
Tenancy files	Duration of tenancy
Former tenants' files (key info)	5 years
Third Party documents re care plans	Duration of tenancy
Records re offenders. Ex-offenders (sex offender register)	Duration of tenancy
Lease documents	5 years after lease termination
ASB case files	5 years/end of legal action
Board meetings/residents' meetings	1 year
Minute of factoring meetings	Duration of appointment

The following schedule of data retention is not covered by the SFHA guidance:

Type of record	Retention time
General CCTV Footage	28 days
CCTV footage involving criminal activity or breaches of tenancy agreement	1 month after footage passed to the Police or incident resolved.
Emails contained in personal mailboxes	12 months

DATA RETENTION PERIODS FOR CONSTRUCTION PROJECTS

Type of record	Retention time	Storage method
Prime documents needed for financing: • Missives, title etc • Topographical surveys, site investigations, environmental reports • Planning consent and conditions • Section 75 agreement • Building warrants • Building warrant completion certificates • Road Construction Consent • Certificate of Practical Completion • Making Good of Defects certificate • HAG offer • Other miscellaneous consents, grant offers etc	Permanently	Electronic copy to be filed within PNB scheme files. No need to retain hard copy.
CDM health and safety files (including as-built drawings and operation and maintenance manuals).	Permanently	Hard copy to be saved in H&S file library at PoLHA offices. Electronic copy in H&S file section on shared drive.
As-built drawings (for projects predating CDM 1994).	Permanently	Hard copy to be saved in H&S file library at PoLHA offices.
Building contracts (new developments).	12 years from end of defects period.	Hard copy to be kept in contract library at PoLHA offices. Electronic copy to be filed within PNB scheme files.
Building contracts (refurbishment, maintenance and servicing contracts).	12 months from end of contract (or defects period where applicable).	Hard copy to be kept in in contract library at PoLHA offices. Electronic copy to be filed within PNB scheme files.

Type of record	Retention time	Storage method
Novation agreements and collateral warranties (new developments).	12 years from end of defects period.	Electronic copy to be filed within PNB scheme files. No need to retain hard copy.
Consultants appointment letters (new developments).	12 years from end of defects period	Electronic copy to be filed within PNB scheme files. No need to retain hard copy.
Consultants appointment letters (refurbishment, maintenance and servicing contracts).	12 months from end of contract (or defects period where applicable).	Electronic copy to be filed within PNB scheme files. No need to retain hard copy.
Clerk of works reports, snagging lists and end of defects period lists.	Until 12 months after issue of Making Good of Defects certificate and release of retention.	Electronic copy to be filed within PNB scheme files.
General project-related emails and documentation	Unless a prime document, until 12 months after issue of Making Good of Defects certificate and release of retention.	Emails to be saved within PNB shared mail boxes (not personal mail boxes). Other correspondence to be saved within PNB scheme files.
Email and other correspondence (with tenants).	Duration of tenancy.	To be saved onto QL only. No emails or correspondence to be retained in scheme files or shared or personal mail boxes.
General project-related emails and documentation relating to aborted projects.	5 years (or less if project is developed out by another party in the meantime).	In PNB scheme files and shared mail boxes (not personal mail boxes).