Shettleston Housing Association

PRIVACY POLICY

Contents

1.	Introduction	p1
2.	Legislation	p1
3.	Data	p2
4.	Processing of Personal Data	p3-5
5.	Data Sharing	p5-6
6.	Data Storage and Security	p6-7
7.	Breaches	p7-8
8.	Data Protection Officer	p8
9.	Data Subject Rights	p9-10
10.	Privacy Impact Assessments	p11
11.	Archiving, Retention and Destruction of Data	p11

1. Introduction

Shettleston 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.

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).

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.

Appendix 1 hereto details the Association's related policies.

2. Legislation

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

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

(a) the General Data Protection Regulation (EU) 2016/679 ("the GDPR");

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

(c) any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the 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 Fair Processing Notice at Appendix 2 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 Data” is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by the Association.

3.1.2 The Association also holds Personal data that is sensitive in nature (i.e. relates to or reveals a data subject’s racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is “Special Category Personal Data” or “Sensitive Personal Data”.

4. Processing of Personal Data

4.1 The Association is permitted to process Personal Data on behalf of data subjects provided it is doing so on one of the following grounds:

- Processing with the consent of the data subject (see 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; or
- Processing is necessary for the purposes of legitimate interests.

4.2 Fair Processing Notice

4.2.1 The Association has produced a Fair Processing Notice (FPN) which it is required to provide to all customers whose Personal data is held by the Association. That FPN must be provided to the customer from the outset of processing their Personal Data and they should be advised of the terms of the FPN when it is provided to them.

4.2.2 The Fair Processing 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

4.3 Employees

4.3.1 Employee Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by the Association.

Details of the data held and processing of that data is contained within the Employee Fair Processing Notice which is provided to Employees at the same time as their Contract of Employment.

4.3.2 A copy of any employee's Personal Data held by the Association is available upon written request by that employee from the Association's HR Manager.

4.4 Consent

Consent as a ground of processing will require to be used from time to time by the Association when processing Personal Data. It should be used by the Association where no other alternative ground for processing is available. In the event that the Association requires to obtain consent to process a data subject's Personal Data, it shall obtain that consent in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained by the Association must be for a specific and defined purpose (i.e. general consent cannot be sought).

4.5 Processing of Special Category Personal Data or Sensitive Personal Data

In the event that the Association processes Special Category Personal Data or Sensitive Personal Data, the Association must do so in accordance with one of the following grounds of processing:

- The data subject has given explicit consent to the processing of this data for a specified purpose;
- Processing is necessary for carrying out obligations or exercising rights related to employment or social security;
- Processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity; and
- Processing is necessary for reasons of substantial public interest.

5. Data Sharing

5.1 The Association shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with the Association's relevant policies and procedures.

5.2 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 in to an Agreement with the Association governing the processing of data, security measures to be implemented and responsibility for breaches.

5.3 Data Sharing

5.2.1 Personal data is from time to time shared amongst the Association and third parties who require to process personal data that the Association process as well. Both the Association and the third party will be processing that data in their individual capacities as data controllers.

5.2.2 Where the Association shares in the processing of personal data with a third party organisation (e.g. for processing of the employees' pension), it shall require the third party organisation to enter in to a Data Sharing Agreement with the Association in accordance with the terms of the model Data Sharing Agreement set out in Appendix 3 to this Policy.

5.4 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).

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

5.4.2 If a data processor wishes to sub-contact their processing, prior written consent of the Association must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

5.4.3 Where the Association contracts with a third party to process personal data held by the Association, it shall require the third party to enter in to a Data Protection Addendum with the Association in accordance with the terms of the model Data Protection Addendum set out in Appendix 4 to this Policy.

6. Data Storage and Security

All Personal Data held by the Association must be stored securely, whether electronically or in paper format.

6.1 Paper Storage

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.

6.2 Electronic Storage

Personal Data stored electronically must also be protected from unauthorised use and access. Personal data should be encrypted 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 data should be encrypted and the removable media if taken off site should be kept secure 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.

7. Breaches

7.1 A data breach can occur at any point when handling Personal Data and the Association has reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported externally in accordance with Clause 7.3 hereof.

7.2 Internal Reporting

The Association takes the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the 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 ICO 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

7.3 Reporting to the ICO

The DPO will require to report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the Information Commissioner's Office ("ICO") within 72 hours of the breach occurring. The DPO must also consider whether it is appropriate to notify those data subjects affected by the breach.

8. Data Protection Officer ("DPO")

8.1. A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by the Association with Data Protection laws. The Association has elected to appoint a Data Protection Officer whose details are noted on the Association's website and contained within the Fair Processing Notice at Appendix 3 hereto.

8.2 The DPO will be responsible for:

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

8.2.2 co-operating with and serving as the Association's contact for discussions with the ICO

8.2.3 reporting breaches or suspected breaches to the ICO and data subjects in accordance with Part 7 hereof.

9. Data Subject Rights

9.1 Certain rights are provided to data subjects under the GDPR. Data Subjects are entitled to view the personal data held about them by the Association, whether in written or electronic form.

9.2 Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to the Association's processing of their data. These rights are notified to the Association's tenants and other customers in the Association's Fair Processing Notice.

9.3 **Subject Access Requests**

Data Subjects are permitted to view their data held by the Association upon making a request to do so (a Subject Access Request). Upon receipt of a request by a data subject, the Association must respond to the Subject Access Request within one month of the date of receipt of the request.

The Association:

9.3.1 must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law.

9.3.2 where the personal data comprises data relating to other data subjects, must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the Subject Access Request, or

9.3.3 where the Association does not hold the personal data sought by the data subject, must confirm that it does not hold any personal data sought to the data subject as soon as practicably possible, and in any event, not later than one month from the date on which the request was made.

9.4 **The Right to be Forgotten**

9.4.1 A data subject can exercise their right to be forgotten by submitting a request in writing to the Association seeking that the Association erase the data subject's Personal Data in its entirety.

9.4.2 Each request received by the Association will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.4 and will respond in writing to the request.

9.5 **The Right to Restrict or Object to Processing**

9.5.1 A data subject may request that the Association restrict its processing of the data subject's Personal Data, or object to the processing of that data.

9.5.1.1 In the event that any direct marketing is undertaken from time to time by the Association, a data subject has an absolute right to object to processing of this nature by the Association, and if the Association receives a written request to cease processing for this purpose, then it must do so immediately.

9.5.2 Each request received by the Association will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.5 and will respond in writing to the request.

10. Privacy Impact Assessments ("PIAs")

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

10.2 The Association shall:

10.2.1 Carry out a PIA before undertaking a project or processing activity which poses a "high risk" to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing Personal Data; and

10.2.2 In carrying out a PIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data

10.3 The Association will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The Data Protection Officer ("DPO") will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the DPO within five (5) working days.

11. Archiving, Retention and Destruction of Data

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 5 hereto.

12 Policy Review/Access

The Association's Privacy Policy will be reviewed and amended as necessary due to changes in legislation or Regulation or every three years.

Access to the policy will be made available via the Association's website or a hard copy will be provided on request from the Association's office.

List of Appendices

1. Related Policies
2. Fair Processing Notice
3. Model Data Sharing Agreement
4. Model Data Processor Addendum
5. Table of Duration of Retention of certain Data

Related Policies/Documents

The following Association's policies should be referred to in relation to our approach to secure and process data held by the Association in relation to customers, staff and other individuals.

- ICT Acceptable Use Policy
- Recruitment & Selection Policy
- Maintenance Policy
- Allocations Policy
- Anti-social Behaviour Policy
- Rent Arrears Policy
- Code of Conduct for Governing Body Members

Appendix 1

#[insert RSL name]
GDPR Fair Processing Notice
(How we use your personal information)

Drafting Note:

- ***This document is intended to provide notice to individuals about the use of their personal data. It is important that individuals are informed in clear language of how their personal data will be used - this document must be provided to individuals before any use is made of their personal data.***

- ***Drafting notes have been included at the start of each section explaining the requirements of each section. These drafting notes should be deleted once the Fair Processing Notice ("FPN") is finalised, and prior to the distribution of the FPN to individuals. We have also provided indicative wording in most sections, however, each section should be reviewed and updated (in plain English) by the relevant data controller to ensure that individuals are appropriately notified. The wording in square brackets may in some cases also be relevant.***
- ***If any decisions or processes are based on automated decision-making (including profiling) then details of this should be included within this notice including the consequences of such processing for the individual.***

- ***This document will require to be adapted by the individual RSL members to suit their practices and procedures and work undertaken. It is designed as a model only with guidance/ drafting notes detailed throughout for ease of finalising the precise terms of the member's FPN. It is recommended that each member seek their own legal advice when finalising the terms of their Fair Processing Notice.***

This notice explains what information we collect, when we collect it and how we use this. 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?

#[**insert RSL name**], ###, a Scottish Charity (Scottish Charity Number ###), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number ### and having their Registered Office at ### ("**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 the 25th 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 #**[insert Data Controller number]** and we are the data controller of any personal data that you provide to us.

Our Data Protection Officer is #**[insert name and contact details]**.
Any questions relating to this notice and our privacy practices should be sent to #[**insert contact details**]. ***Drafting Note: Corporate Services/ Housing Team or DPO. RSL to determine***

How we collect information from you and what information we collect

Drafting Note: This section should set out details of: (i) how information is collected (e.g. via website, from third parties, from information provided by the individual etc.); (ii) the personal information collected from the individuals; and (iii) the reasons for collecting this information. This should specify whether this is collected by the data controller directly or received from third parties (where possible details of the third parties should be included).

We collect information about you:

- when you apply for housing with us, become a tenant, request services/ repairs, enter in to a factoring agreement with ourselves howsoever arising or otherwise provide us with your personal details

- when you apply to become a member;

- from your use of our online services, whether to report any tenancy/ factor related issues, make a complaint or otherwise; ***Drafting Note: Individual members must consider how their website is used by data subjects and whether any information is collected from website usage***

- from your 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;
- #[***insert further personal data you collect from the individual***]

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 as to the conduct or condition of your tenancy, including references from previous tenancies, and complaints of anti-social behaviour

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

Drafting Note: This section should set out the reasons for requiring the information and the legal basis for the processing (for example, if the processing is necessary to carry out a contract with the individual). It should also clearly detail how you will use the personal information. The current list is a suggestion based on some common uses of data and should be adjusted to reflect how the personal data is used in practice.

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 in order to send you details of any changes to our or supplies which may affect you;
- for all other purposes consistent with the proper performance of our operations and business; and
- to contact you for your views on our products and services.

Sharing of Your Information

Drafting Note: This section sets out details of when and how any personal data will be shared with third parties. It is important that data subjects are aware of the circumstances where their personal data may be shared and this section should be comprehensive.

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]* ***Drafting note: Members need to check that whether data is processed (particularly by IT support providers and other online facilities)- see section below***. 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 merged with another business entity, your information may be disclosed to our new business partners or owners;

- If we instruct repair or maintenance works, your information may 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 Local Authority);

- If we are investigating payments made or otherwise, your information may be disclosed to payment processors, 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

- **[insert details of any further data sharing arrangements/ third parties who process personal data on behalf of RSL member.] NOTE: I would be keen to discuss further with those in the working group.**

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

Drafting Note: If personal data will be transferred outside the EEA it is important that data subjects are aware of this. As the approach post Brexit is unclear, you may wish to include details of transfers outside the UK specifically. If personal data is stored in the cloud the location of the servers should be confirmed and if outside the UK/EEA this should be stated in this notice. This is something that individual member organisations will need to check.

#[Your information will only be stored within the UK and EEA]/ [We may transfer your information outside the UK and/or EEA] *(*delete as appropriate)*:

#[insert situations where personal data is transferred outside UK/EEA] *(*delete if not applicable)*

Where information is transferred outside the UK or EEA we ensure that there are adequate safeguards in place to protect your information in accordance with this notice, including the following:

#[Insert basis for transfer and relevant safeguards (e.g. decision by the Commission that the third country has adequate safeguards/ details of appropriate security provisions in place.)]

Security

Drafting Note: It is important that personal information is stored securely and appropriate technical measures are taken to protect this information. This section should set out details of the security measures in place.

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

#**[insert further details of security processes]** ***Drafting Note: the individual member organisation will require to confirm their own security measures that are in place and will require to update their FPN with these details. Alternatively, you could provide a link to the organisation's Data Protection/ Privacy Policy.***

How long we will keep your information

Drafting Note: It is important that personal data is not stored for any longer than it is reasonably required. Data subjects should be notified of how long personal data is stored for, or if this is not possible, then details of the criteria used to determine how long personal data will be kept for. The wording below provides some generic wording, however, this should be updated/specific for each type/use of personal data.

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 following minimum periods:

- **NOTE: TC Young will produce draft retention periods separately which can be adopted or altered. The individual member organisation must be able to demonstrate the requirement to retain the personal data for the specified period.**

  after which this will be destroyed if it is no longer required for the reasons it was obtained.

Our full retention schedule is available at #**[insert where data subject can source retention schedule (e.g. website or in our office)].**

Your Rights

Drafting Note: Data Subjects must be told of their rights in relation to the personal data you hold.

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 what personal data of your we hold; and
- object to receiving any marketing communications from us.

If you would like to exercise any of your rights above please contact us at **#[insert e-mail address]**

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 updated by informing us of any changes to your email address and other contact details.

Appendix 2

#[insert RSL name]

Fair Processing Notice
(How we use employee information)

Drafting Note:

- ***This document is intended to provide notice to employees about the use of their personal data. It is important that employees are informed in clear language of how their personal data will be used - this document must be provided to employees (or prospective employees) before any use is made of their personal data.***

- ***Drafting notes have been included at the start of each section explaining the requirements of each section. These drafting notes should be deleted once the FPN is finalised and prior to distribution to individual employees. We have also provided indicative wording in most sections, however, each section should be reviewed and updated (in plain English) by the relevant data controller to ensure that individuals are appropriately notified. The wording in square brackets may in some cases also be relevant.***
- ***If any decisions or processes are based on automated decision-making (including profiling) then details of this should be included within this notice including the consequences of such processing for the individual.***

- ***This document will require to be adapted by the individual RSL members to suit their practices and procedures and work undertaken. It is designed as a model only with guidance/ drafting notes detailed throughout for ease of finalising the precise terms of the member's Fair Processing Notice. It is recommended that each member seek their own legal advice when finalising the terms of their Fair Processing Notice.***

This notice explains what information we collect, when we collect it and how we use this. 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.

1. # [**insert name of RSL**] ("we" or "us") is committed to a policy of protecting the rights of individuals with respect to the processing of their personal data and adhere to guidelines published in the [Data Protection Act of 1998] and the General Data Protection Regulation (EU) 2016/679 which is applicable from the 25th May 2018, together with any domestic laws subsequently enacted. We collect and use personal data for a variety of reasons.

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

Our Data Protection Officer is #**[insert name and contact details]**. [*delete if not applicable]

Any questions relating to this notice and our privacy practices should be sent to #[**insert contact details**]. ***Drafting Note: Corporate Services/ Housing Team or DPO. RSL to determine***

Drafting Note: The following paragraph should set out details of: (i) how information is collected (e.g. from third parties, from information provided by the individual etc.); (ii) the personal information collected from the individuals; and (iii) the reasons for collecting this information. This should specify whether this is collected by the data controller directly or received from third parties (where possible details of the third parties should be included). Consider what sensitive Personal Data you hold about employees and on what basis you are processing this. If processing without consent, you must have an alternative basis and must disclose the sensitive personal data processing without consent in this Notice.

2. We collect the following information from you through a variety of resources (i) directly from you; or (ii) third parties (including Employment Agencies, pensions service):

   (a) Name

   (b) Date of Birth

   (c) Address

   (d) Telephone Number

   (e) E-mail address

   (f) NI number

   (g) Personal characteristics such as gender and ethnic group

   (h) Qualifications

   (i) Absence information

   (j) # [***Drafting Note: insert any further personal data collected from employees***]

   Drafting Note: The following paragraph should set out the reasons for requiring the information and the legal basis for the processing (for example, if the processing is necessary to carry out a contract with the individual). It should also clearly detail how you will use the personal information. The current list is a suggestion based on some common uses of data and should be adjusted to reflect how the personal data is used in practice.

We collect and use the above information and personal data for:

a. Administration of contracts of employment

b. Payment of salaries

c. Recruitment and selection

d. Pensions and associated benefits, appraisal, training and development

e. Membership of professional bodies

f. # [insert any further reasons for processing employee personal data]

Drafting Note: The following paragraph sets out details of when and how any personal data will be shared with third parties. It is important that data subjects are aware of the circumstances where their personal data may be shared and this section should be comprehensive.

3. We may disclose to and share information about you with third parties for the purposes set out in this notice, or for purposes approved by you, including the following:

- To process your # [***insert frequency, i.e. weekly/ fortnightly***] salary payments;

- To allow your pension provider to process pensions information and handle your pension; (delete if not applicable)

- To allow your electronic payslips to be produced and issued to you (delete if not applicable)

- If we enter into a joint venture with or is sold to or merged with another business entity, your information may be disclosed to our new business partners or owners.

Drafting Note: If personal data will be transferred outside the EEA it is important that data subjects are aware of this. As the approach post Brexit is unclear, you may wish to include details of transfers outside the UK specifically. If personal data is stored in the cloud the location of the servers should be confirmed and if outside the UK/EEA this should be stated in this notice. This is something that individual member organisations will need to check.

4. #[Your information will only be stored within the UK and EEA]/ [We may transfer your information outside the UK and/or EEA] *(*delete as appropriate)*:

#[insert situations where personal data is transferred outside UK/EEA] *(*delete if not applicable)*

Where information is transferred outside the UK or EEA we ensure that there are adequate safeguards in place to protect your information in accordance with this notice, including the following:

#[Insert basis for transfer and relevant safeguards (eg. decision by the Commission that the third country has adequate safeguards/ details of appropriate security provisions in place.)]

Drafting Note: It is important that personal information is stored securely and appropriate technical measures are taken to protect this information. This paragraph should set out details of the security measures in place.

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

   #**[insert further details of security processes]** ***Drafting Note: the individual member organisation will require to confirm their own security measures that are in place in relation to employee personal data and will require to update their FPN with these details. Alternatively, you could provide a link to the organisation's Data Protection/ Privacy Policy.***

   Drafting Note: It is important that personal data is not stored for any longer than it is reasonably required. Data subjects should be notified of how long personal data is stored for, or if this is not possible, then details of the criteria used to determine how long personal data will be kept for. The wording below provides some generic wording, however, this should be updated/specific for each type/use of personal data.

6. 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.

   Data retention guidelines on the information we hold is provided in our Privacy policy within the staff handbook.

   Drafting Note: Data Subjects must be told of their rights in relation to the personal data you hold.

7. You have the right at any time to:

   - Ask for a copy of the information about you held by us in our records; and

   - Require us to correct any inaccuracies in your information

8. If you would like to find out more about how we use your personal data or want to see a copy of information about you that we hold or wish to exercise any of your above rights, please contact: # [***insert contact details***].

   You have the right to complain to the Information Commissioner's Office in relation to our use of your information.

   The accuracy of your information is important to us – please help us keep our records updated by informing us of any changes to your personal and contact details.

Appendix 3

DATA SHARING AGREEMENT

between

#[insert name of RSL], a Scottish Charity (Scottish Charity Number #), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number # and having their Registered Office at # (the "Association");
and

#*[Insert organisation name, a # [e.g. Company]* registered in terms of the Companies Acts with registered number *[registered number]* and having its registered office/main office at #[*address]*] ("#**[Party 2]**")]") ***[Drafting note: amend from Party 2 to suitable defined term]***;

(each a "**Party**" and together the "**Parties**").

WHEREAS

Drafting Note: Further detail will require to be inserted here to confirm relationship between Parties to the Agreement. This will depend on the precise nature of relationship so will require to be adapted for every individual use of this model Agreement.

(a) The Association and [*Insert name of party*] ("[Party 2]")intend that this data sharing agreement will form the basis of the data sharing arrangements between the parties (the "Agreement"); and

(b) The intention of the Parties is that they shall each be independent Data Controllers in respect of the Data that they process under this Agreement.

(c) Nothing in this Agreement shall alter, supersede, or in any other way affect the terms of #[***insert details of relationship/ contract with Party 2***]

NOW THEREFORE IT IS AGREED AS FOLLOWS:

1 DEFINITIONS

1.1 In construing this Agreement, capitalised words and expressions shall have the meaning set out opposite:

"Agreement" means this Data Sharing Agreement, as amended from time to time in accordance with its terms, including the Schedule;

"Business Day" means any day which is not a Saturday, a Sunday or a bank or public holiday throughout Scotland;

"Data" means the information which contains Personal Data and Sensitive Personal Data (both of which have the definition ascribed to them in Data Protection Law) described in Part 1;

"Data Controller" has the meaning set out in Data Protection Law;

"Disclosing Party" means the Party (being either the Association or #[Party 2], as appropriate) disclosing Data (or on behalf of whom Data is disclosed to the Data Recipient);

"Data Protection Law" means Law relating to data protection, the processing of personal data and privacy from time to time, including:

(d) the Data Protection Act 1998;

(e) (with effect from 25 May 2018) the General Data Protection Regulation (EU) 2016/679;

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

(g) 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;

"Data Recipient" means the party (being either the Association or #[Party 2], as appropriate) to whom Data is disclosed;

"Data Subject" means any identifiable individual to whom any Data relates: and the categories of data subjects within the scope of this Agreement are listed in Part 1;

"Data Subject Request" means a written request of either party as Data Controller by or on behalf of a Data Subject to exercise any rights conferred by Data Protection Law in relation to the data or the activities of the parties contemplated by this Agreement;

"Disclosing Party" means the party (being either the Association or #[Party 2], as appropriate) disclosing Data to the Data Recipient;
"Information Commissioner" means the UK Information Commissioner and any successor;

"Law" means any statute, directive, other legislation, law or regulation in whatever form, delegated act (under any of the foregoing), rule, order of any court having valid jurisdiction or other binding restriction, decision or guidance in force from time to time;

"Legal Basis" means in relation to either Party, the legal basis for sharing the Data as described in Clause 2.3 and as set out in Part 2;

"Purpose" means the purpose referred to in Part 2;

"Representatives" means, as the context requires, the representative of the Association and/or the representative of #[Party 2] as detailed in Part 4 of the Schedule. The same may be changed from time to time on notice in writing by the relevant Party to the other Party;

"Schedule" means the Schedule in 6 Parts annexed to this Agreement and a reference to a "Part" is to a Part of the Schedule; and

"Security Measures" has the meaning given to that term in Clause 2.4.5.

1.2 In this Agreement unless the context otherwise requires:

1.2.1 words and expressions defined in Data Protection Law shall have the same meanings in this Agreement so that, in the case of Data Protection Law, words and expressions shall be interpreted in accordance with:

(a) the Data Protection Act 1998, in respect of processing undertaken on or before 24 May 2018;

(b) the General Data Protection Regulation (EU) 2016/679, in respect of processing undertaken on or after 25 May 2018; and

(c) in respect of processing undertaken on or after the date on which legislation comes into force that replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, that legislation;

1.2.2 more generally, references to statutory provisions include those statutory provisions as amended, replaced, re-enacted for the time being in force and shall include any bye-laws, statutory instruments, rules, regulations, orders, notices, codes of practice, directions, consents or permissions and guidelines (together with any conditions attached to the foregoing) made thereunder;

2 DATA SHARING

Purpose and Legal Basis

2.1 The Parties agree to share the Data for the Purpose in accordance with the provisions of Part 2 of the Schedule.

2.2 Save as provided for in this Agreement, the Parties agree not to use any Data disclosed in terms of this Agreement in a way that is incompatible with the Purpose.

2.3 Each Party shall ensure that it processes the Data fairly and lawfully in accordance with Data Protection Law and each Party as Disclosing Party warrants to the other Party in relation to any Data disclosed, that such disclosure is justified by a Legal Basis.

Parties Relationship

2.4 The Parties agree that the relationship between them is such that any processing of the Data shall be on a Data Controller to Data Controller basis. The Data Recipient agrees that:

2.4.1 it is a separate and independent Data Controller in respect of the Data that it processes under this Agreement, and that the Parties are not joint Data Controllers or Data Controllers in common;

2.4.2 it is responsible for complying with the obligations incumbent on it as a Data Controller under Data Protection Law (including responding to any Data Subject Request);

2.4.3 it shall comply with its obligations under Part 6 of the Schedule;

2.4.4 it shall not transfer any of the Data outside the United Kingdom except to the extent agreed by the Disclosing Party;

2.4.5 Provided that where the Data has been transferred outside the United Kingdom, the Disclosing Party may require that the Data is transferred back to within the United Kingdom:

(a) on giving not less than 3 months' notice in writing to that effect; or

(b) at any time in the event of a change in Law which makes it unlawful for the Data to be processed in the jurisdiction outside the United Kingdom where it is being processed; and

2.4.6 it shall implement appropriate technical and organisational measures including the security measures set out in Part 5 of the Schedule (the "**Security Measures**"), so as to ensure an appropriate level of security is adopted to mitigate the risks associated with its processing of the Data, including against unauthorised or unlawful processing, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or damage or access to such Data.

2.5 The Disclosing Party undertakes to notify in writing the other as soon as practicable if an error is discovered in Data which has been provided to the Data Recipient, to ensure that the Data Recipient is then able to correct its records. This will happen whether the error is discovered through existing Data quality initiatives or is flagged up through some other route (such as the existence of errors being directly notified to the Disclosing Party by the Data Subjects themselves).

Transferring Data

2.6 Subject to the Data Recipient's compliance with the terms of this Agreement, the Disclosing Party undertakes to endeavour to provide the Data to the Data Recipient on a non-exclusive basis in accordance with the transfer arrangements detailed in Part 3 of the Schedule.

3 BREACH NOTIFICATION

3.1 Each Party shall, promptly (and, in any event, no later than 12 hours after becoming aware of the breach or suspected breach) notify the other party in writing of any breach or suspected breach of any of that Party's obligations in terms of Clauses 1 and/or 2 and of any other unauthorised or unlawful processing of any of the Data and any other loss or destruction of or damage to any of the Data. Such notification shall specify (at a minimum):

3.1.1 the nature of the personal data breach or suspected breach;

3.1.2 the date and time of occurrence;

3.1.3 the extent of the Data and Data Subjects affected or potentially affected, the likely consequences of any breach (in the case of a suspected breach, should it have occurred) for Data Subjects affected by it and any measures taken or proposed to be taken by the that party to contain the breach or suspected breach; and

3.1.4 any other information that the other Party shall require in order to discharge its responsibilities under Data Protection Law in relation to such breach or suspected breach.

3.2 The Party who has suffered the breach or suspected breach shall thereafter promptly, at the other Party's expense (i) provide the other Party with all such information as the other Party reasonably requests in connection with such breach or suspected breach; (ii) take such steps as the other Party reasonably requires it to take to mitigate the detrimental effects of any such breach or suspected breach on any of the Data Subjects and/or on the other Party; and (iii) otherwise cooperate with the other Party in investigating and dealing with such breach or suspected breach and its consequences.

3.3 The rights conferred under this Clause 3 are without prejudice to any other rights and remedies for breach of this Agreement whether in contract or otherwise in law.

4 DURATION, REVIEW AND AMENDMENT

4.1 This Agreement shall come into force immediately on being executed by all the Parties and continue for #[***insert termination: this will be when Parties cease sharing data in terms of contractual relationship with each other***], unless terminated earlier by the Disclosing Party in accordance with Clause 4.5.

4.2 This Agreement will be reviewed one year after it comes into force and every two years thereafter until termination or expiry in accordance with its terms.

4.3 In addition to these scheduled reviews and without prejudice to Clause 4.5, the Parties will also review this Agreement and the operational arrangements which give effect to it, if any of the following events takes place:

4.3.1 the terms of this Agreement have been breached in any material aspect, including any security breach or data loss in respect of Data which is subject to this Agreement; or

4.3.2 the Information Commissioner or any of his or her authorised staff recommends that the Agreement be reviewed.

4.4 Any amendments to this Agreement will only be effective when contained within a formal amendment document which is formally executed in writing by both Parties.

4.5 In the event that the Disclosing Party has any reason to believe that the Data Recipient is in breach of any of its obligations under this Agreement, the Disclosing Party may at its sole discretion:

4.5.1 suspend the sharing of Data until such time as the Disclosing Party is reasonably satisfied that the breach will not re-occur; and/or

4.5.2 terminate this Agreement immediately by written notice to the Data Recipient if the Data Recipient commits a material breach of this Agreement which (in the case of a breach capable of a remedy) it does not remedy within five (5) Business Days of receiving written notice of the breach.

4.6 Where the Disclosing Party exercises its rights under Clause 4.5, it may request the return of the Data (in which case the Data Recipient shall, no later than fourteen (14) days after receipt of such a written request from the Disclosing Party, at the Disclosing Party's option, return or permanently erase/destroy all materials held by or under the control of the Data Recipient which contain or reflect the Data and shall not retain any copies, extracts or other reproductions of the Data either in whole or in part and shall confirm having done so to the other Party in writing), save that the Data Recipient will be permitted to retain one copy for the purpose of complying with, and for so long as required by, any law or judicial or administrative process or for its legitimate internal compliance and/or record keeping requirements.

5 LIABILITY

5.1 Nothing in this Agreement limits or excludes the liability of either Party for:

5.1.1 death or personal injury resulting from its negligence; or

5.1.2 any damage or liability incurred as a result of fraud by its personnel; or

5.1.3 any other matter to the extent that the exclusion or limitation of liability for that matter is not permitted by law.

5.2 The Data Recipient indemnifies the Disclosing Party against any losses, costs, damages, awards of compensation, any monetary penalty notices or administrative fines for breach of Data Protection Law and/or expenses (including legal fees and expenses) suffered, incurred by the Disclosing Party, or awarded, levied or imposed against the other party, as a result of any breach by the Data Recipient of its obligations under this Agreement. Any such liability arising from the terms of this Clause 5.2 is limited to £# (# STERLING) in the aggregate for the duration of this Agreement.

5.3 Subject to Clauses 5.1 and 5.2 above:

5.3.1 each Party excludes all liability for breach of any conditions implied by law (including any conditions of accuracy, security, completeness, satisfactory quality, fitness for purpose, freedom from viruses, worms, trojans or other hostile computer programs, non-infringement of proprietary rights and the use of reasonable care and skill) which but for this Agreement might have effect in relation to the Data;

5.3.2 neither Party shall in any circumstances be liable to the other party for any actions, claims, demands, liabilities, damages, losses, costs, charges and expenses that the other party may suffer or incur in connection with, or arising (directly or indirectly) from, any use of or reliance on the Data provided to them by the other Party; and

5.3.3 use of the Data by both Parties is entirely at their own risk and each party shall make its own decisions based on the Data, notwithstanding that this Clause shall not prevent one party from offering clarification and guidance to the other party as to appropriate interpretation of the Data.

6 DISPUTE RESOLUTION

6.1 The Parties hereby agree to act in good faith at all times to attempt to resolve any dispute or difference relating to the subject matter of, and arising under, this Agreement.

6.2 If the Representatives dealing with a dispute or difference are unable to resolve this themselves within twenty (20) Business Days of the issue arising, the matter shall be escalated to the following individuals in Part 4 of the Schedule identified as escalation points who will endeavour in good faith to resolve the issue.

6.3 In the event that the Parties are unable to resolve the dispute amicably within a period of twenty (20) Business Days from date on which the dispute or difference was escalated in terms of Clause 6.2, the matter may be referred to a mutually agreed mediator. If the identity of the mediator cannot be agreed, a mediator shall be chosen by the Dean of the Royal Faculty of Procurators in Glasgow.

6.4 If mediation fails to resolve the dispute or if the chosen mediator indicates that the dispute is not suitable for mediation, and the Parties remain unable to resolve any dispute or difference in accordance with Clauses 6.1 to 6.3, then either Party may, by notice in writing to the other Party, refer the dispute for determination by the courts in accordance with Clause 9.

6.5 The provisions of Clauses 6.1 to 6.4 do not prevent either Party from applying for an interim court order whilst the Parties attempt to resolve a dispute.

7 NOTICES

7.1 Any Notices to be provided in terms of this Agreement must be provided in writing and addressed to the relevant Party in accordance with the contact details noted in Part 4 of the Schedule, and will be deemed to have been received (i) if delivered personally, on the day of delivery; (ii) if sent by first class post or other next working day delivery, the second day after posting; (iii) if by courier, the date and time the courier's delivery receipt if signed; or (iv) if by fax, the date and time of the fax receipt.

8 GOVERNING LAW

8.1 This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) (a **"Dispute"**) shall, in all respects, be governed by and construed in accordance with the law of Scotland. Subject to Clause 6, the Parties agree that the Scottish Courts shall have exclusive jurisdiction in relation to any Dispute.

Appendix 4

DRAFT MODEL

Data Retention Periods

The table below sets out retention periods for Personal Data held and processed by the Association. It is intended to be used as a guide only. The Association recognises that not all Personal Data can be processed and retained for the same duration, and retention will depend on the individual circumstances relative to the Data Subject whose Personal Data is stored.

Type of record	Suggested 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, notification to the Secretary of State	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, e.g. 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
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	5 years 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