Data Protection/Management of Information Policy

Management Committee submission:	27 August 2019
Last Approved:	26 February 2018
Approved:	27 August 2019
Review date:	June 2020

CHA Objectives:

- To manage the houses provided, in a professional and cost effective manner, for the benefit of our local community and the environment.
- To provide a first class maintenance service which offers value for money and ensures the comfort and safety of our residents while achieving high levels of satisfaction
- To ensure that our resources are adequate to deliver our objectives by investing in our people, demonstrating value for money and through robust procurement practices.
- To promote social inclusion by applying principles of equality and diversity to everything we do.

Regulatory Standards:

- The governing body leads and directs the RSL to achieve good outcomes for its tenants and other service users.
- The RSL is open about and accountable for what it does. It understands and takes account of the needs and priorities of its tenants, service users and stakeholders. And its primary focus is the sustainable achievement of these priorities.
- The RSL manages its resources to ensure its financial well-being, while maintaining rents at a level that tenants can afford to pay.
- The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation's purpose.

This policy can be made available on request in a variety of different formats, such as on CD, in large print and translated into other languages.

Contents

Glossary of Key Terms

The following is a glossary of key terms, which Committee members and staff should be familiar with to execute this policy, they include:

a) Information Commissionerôs Office (ICO) ï Responsible for enforcing legislation. The Association requires submitting an annual notification to the ICO detailing the systems containing data and how the data is used. We are also required to notify the ICO of any changes to the register within 28 days.

b) Data Controller - The organisation that determines the purposes for which and manner in which personal data is used, in our case, the Association.

c) Data Subject ï a living individual who is the subject of personal data e.g. tenant, employee, committee member, suppliers, applicant, complainant, etc.

d) Personal data is defined as, data relating to a living individual who can be identified from:

- That data;
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

e) Relevant Filing System - Any set of information relating to individuals and structured, either by reference to the individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily available.

f) Processing ï obtaining, recording or holding data or carrying out any operation on data, including disclosure and destruction.

g) Data breach - A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

1. Introduction

Clydebank Housing Association (hereinafter the ñAssociationò) is committed to ensuring the secure and safe management of data held by the Association in relation to customers, staff and other individuals. The Associationôs staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individualsô 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 General Data Protection Regulations - GDPR).

This Policy sets out the Associationôs 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 Associationôs 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 (ñthe GDPRò);

(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

(d) The Freedom of Information (Scotland) Act 2002 (Designation of Persons as Scottish Public Authorities) Order 2019 ï applicable from 11 November 2019

(e) Environmental Information Regulations

3. Freedom of Information (FOI) and Environmental Information

The Freedom of Information Act gives everyone the right to can ask to see recorded information from the Association including paper, computer files, and video with exception of personal information that is covered by GDPR. It also excludes commercially sensitive information and information that might prejudice the safety or security of Clydebank Housing Association.
The Association recognises its 3 mandatory duties under FOI as follows: -

- Duty to publish information
- Duty to respond to requests
- Duty to advise and assist

In order to meet its duties, the Association will publish its Guide to Information via its website and will adhere to the provisions as detailed in its Model Publication Framework (SFHA/GWSF Open All Hours Guide).

4. 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 ñPersonal Dataò 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 subjectôs racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is ñSpecial Category Personal Dataò or ñSensitive Personal Dataò

5. Processing of Personal Data

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

- Processing with the consent of the data subject (see clause 4.4 hereof);

- Processing is necessary for the performance of a contract between the Association and the data subject or for entering into a contract with the data subject;
- Processing is necessary for the Associationôs 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 Associationôs 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 Associationôs 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 employeeôs Personal Data held by the Association is available upon written request by that employee from the Associationôs Chief Executive.

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 obtaining consent to process a data subjectôs 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.

6. Data Sharing

6.1 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 Associationôs relevant policies and procedures. In order that the Association can monitor compliance by these third parties with Data Protection laws, the Association will require the third party organisations to enter in to an Agreement with the Association governing the processing of data, security measures to be implemented and responsibility for breaches.

6.2 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 employeesô 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 Association's Data Sharing Agreement set out in Appendix 3 to this Policy.

6.3 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. Maintenance and repair works, IT support, etc.).

6.3.1 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.

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

6.3.3 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.

7. Data Storage and Security

All Personal Data held by the Association must be stored securely, whether electronically or in paper format in accordance with the Association's Information Security Policy.

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.

6.2 Electronic Storage

Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should only be sent internally or externally to the Association's data processors or those with whom the Association has entered in to a Data Sharing Agreement. If Personal data is stored on removable media (CD, DVD,

USB memory stick) then that removable media must be stored securely at all times when not being used. Personal Data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

8. Breaches

The GDPR introduces a duty on the Association to report certain types of personal data breach to the relevant supervisory authority. This must be done within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individualsô rights and freedoms, we must also inform those individuals without undue delay. Recital 85 of the GDPR explains that: ñA personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.ò

Failing to notify a breach when required to do so, can result in a significant fine of up to 10 million euros or 2 per cent of our turnover. The fine can be combined with the ICOôs other corrective powers under Article 58. We will therefore ensure we have robust breach detection, investigation and internal reporting procedures in place to facilitate decision-making about whether or not we need to notify the relevant supervisory authority and the affected individuals.

We will also keep a record of any personal data breaches, regardless of whether we are required to notify.

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. A data security breach can happen for a number of reasons including e.g. theft or loss of computer hardware and paper files, inappropriate access controls allowing unauthorised use, human error, malicious attacks, contractor computer compromised, etc.

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 Data Processing Officer 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 Information Commissioners Office (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
- Update the Breach Register with details of any breach/suspected breach

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 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.

9. 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 Associationôs 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 Associationôs compliance with Data Protection laws and this Policy;

8.2.2 Co-operating with and serving as the Associationôs 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.

10. 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 Associationôs processing of their data. These rights are notified to the Associationôs tenants and other customers in the Associationôs 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 subjectôs 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 subjectôs 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 subjectôs 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 subjectôs request in accordance with clause 9.5 and will respond in writing to the request.

11. Privacy Impact Assessments (ñPIAsò)

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

11.2 The Association shall:

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

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

12. Archiving, Retention and Destruction of Data

The Association cannot store and retain Personal Data indefinitely. It must ensure that Personal data is only retained for the period necessary. The Association shall ensure that all Personal data is archived and destroyed in accordance with the periods specified within the table at Appendix 5 hereto. Destruction will take place via deletion from computer network (including archived files), internal shredding and the use of an external shredding company holding appropriate data security guarantees. Shredding and destruction of data will take place under the express guidance, supervision and authority of appropriate departmental managers as set out in Appendix 5. Deletion of computer data is regularly monitored through CPTRAX software on a weekly basis.

List of Appendices

1. Information Security Policy

2. Fair Processing Notice

3. Model Data Sharing Agreement

4. Model Data Processor Addendum

5. Table of Duration of Retention/Destruction of certain Data ï (NHF document)

6. Specific Consent Form

APPENDIX 1

clydebank housing association

Information Security Policy

Management Committee submission:	26 March 2019
Previous Approval:	27 February 2018
Approved:	26 March 2019
Review date:	February 2022

CHA Objectives:

- To manage the houses provided, in a professional and cost effective manner, for the benefit of our local community and the environment.
- To provide a first class maintenance service which offers value for money and ensures the comfort and safety of our residents while achieving high levels of satisfaction
- To ensure that our resources are adequate to deliver our objectives by investing in our people, demonstrating value for money and through robust procurement practices.
- To promote social inclusion by applying principles of equality and diversity to everything we do.

Regulatory Standards:

- The governing body leads and directs the RSL to achieve good outcomes for its tenants and other service users.
- The RSL is open about and accountable for what it does. It understands and takes account of the needs and priorities of its tenants, service users and stakeholders. And its primary focus is the sustainable achievement of these priorities.
- The RSL manages its resources to ensure its financial well-being, while maintaining rents at a level that tenants can afford to pay.
- The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation's purpose.

This policy can be made available on request in a variety of different formats, such as on tape, in large print and translated into other languages.

Clydebank Housing Association Ltd
Information Security Policy Statement

Section 1 - Purpose

The purpose of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Association by:

1.1 Ensuring that relevant members of staff are aware of and fully comply with the relevant legislation as described in this and other related policies.

1.2 Describing the principals of security and explaining how they shall be implemented in the Association.

1.3 Introducing a consistent approach to security, ensuring that all relevant members of staff and third parties fully understand their own responsibilities.

1.4 Creating and maintaining within the Association a level of awareness of the need for Information Security as an integral part of the day to day business.

1.5 Protecting information assets under the control of the Association.

Section 2 - Responsibilities

2.1 Ultimate responsibility for information security rests with the Association's Board/Committee, but on a day-to-day basis the Chief Executive shall be responsible for managing and implementing this Information Security Policy and related procedures.

2.2 The Information Security Policy shall be maintained, reviewed and updated by the Chief Executive, the Head of Housing Services and Finance & IT Assistant. This review shall take place annually.

2.3 All staff are responsible for reading and formally accepting the terms and conditions of this policy.

Section 3 - Legislation

3.1 The Association is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the Association, who may be held personally accountable for any breaches of information security for which they may be held responsible. The Association shall comply with the following legislation and other legislation as appropriate:

- General Data Protection Regulations 2018
- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)

- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000

Section 4 – Policy Framework

A clear audit trail will be in place for all security management processes detailed in this policy framework.

4.1 Information Security Awareness Training

4.1.2 Information security awareness training shall be included in the staff induction process.

4.1.3 An ongoing awareness/training programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

4.1.4 The Associationôs IT support provider, the Head of Housing Services and the Finance and IT Assistant will ensure their knowledge is kept relevant and fit for purpose through the regular review of security bulletins and training materials.

4.1.5 All responsible staff will sign up to the ICO Monthly Newsletter/Bulletin

4.1.6 The Association will ensure the IT support providerôs/relevant staff membersôskills and knowledge are fit for purpose through an annual review of their Continuous Professional Development (CPD) programme.

4.2 Change Management

4.2.1 Change management will be a key part of ensuring effective management and control of systems. The Association and IT support providers will ensure that proposed changes to hardware, software or network configurations are reviewed, approved and tested before being applied to the production environment. There should be formal procedures for testing and approval. There should be documentation regarding the process for change management to ensure consistency in managing incidents and changes. This could result in incidents not being managed effectively and/or changes not being implemented successfully.

4.2.2 Data Protection impact assessments (DPIAôs) help organisations identify, assess and mitigate or minimise privacy risks during data processing activities. They are particularly relevant when new data processing, systems or technology is being introduced. A DPIA will be conducted where data processing or a change in processing is likely to result in a high risk to the rights and freedoms of natural persons e.g. the introduction of a new Housing IT system.

4.3 Access Control

4.3.1 Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset per the Associationôs IT Policy and Information Security Risk Assessment.

4.3.2 Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

4.3.3 Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

4.3.4 Access to data, system utilities and programme source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a license from the supplier.

4.3.5 Third Party Service Providers that routinely receive, send, transmit, store, control, or process Association information that is non-Public in nature or that provide technology and/or non-technology related services that require or include handling such information, shall be controlled and restricted to those users who have been authorised by the named custodian who is responsible for the information of that asset. All relationships with Third Parties and all obligations incurred in either direction with Third Parties must be documented and maintained to facilitate the management of the risk associated with the relationship. The Association must have in place a service agreement with any Third Party before the Third Party begins performing any tasks or providing any services, including development or pilot projects. Formal acceptance of the Associationôs Acceptable Use Policy and any other Association related policies will be included as a requirement of any service level agreement. Once the agreement is terminated, all access will be disabled and passwords must be changed where applicable.

4.3.6 No employee of the Association will have elevated access privileges such as administrative access to Association owned IT devices such as desktop PCôs, smart devices, laptops etc.

4.3.7 The Associationôs IT Policy sets out access permissions matrix and the Associationôs Financial Procedures set out the inventory of assets

4.3.8 Authorisation must be sought from the Chief Executive, or in their absence, the Head of Housing Services to enable remote access from approved devices. Weekly CPTRAX software reports monitor access to the Associationôs systems.

4.4 Secure Data Transfer

The transmission of Personal or Confidential information will be transferred in a secure manner to prevent unauthorised access.

This section lists the main methods and sets out any restrictions and the requirements for secure transfer of Personal or Confidential information. For all transfers of Personal or Confidential information it is essential that the identity and authorisation of the recipient has been appropriately authenticated by the sender.

4.4.1 Email

- Information sent via email must be enclosed in an attachment and encrypted using a product approved by the Association. Minimum standard for encryption is AES (256 bit).
- Any password must be in line with the requirements of section 4.14.2 of this policy.
- Any password to open the attached file must be transferred to the recipient using a different method than e-mail, e.g. a telephone call to an agreed telephone number, closed letter.
- E-mail message must contain clear instructions on the recipients responsibilities and instructions on what to do if they are not the correct recipients.
- An accompanying message and the filename must not reveal the contents of the encrypted file.
- Check with the recipient that their e-mail system will not filter out or quarantine the transferred file.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to their line manager.

4.4.2 Electronic Memory (CD, DVD, USB drive, Memory Card)

Information must be enclosed in a file and encrypted using a product approved by the Association set at an appropriate strength. Or an approved encrypted hardware device such as encrypted USB drive.

The requirements of Section 4.4.1 regarding Email transmission apply to this section also.

4.4.3 Fax Transmission

FAX is inherently insecure and is not recommended for transfer of sensitive information. However, it is acknowledged that certain circumstances demand it.

- Sender must check that the Fax number is correct and that

the receiver is awaiting transmission.

- For high sensitivity information the number must be double-checked by a colleague before transmission, and telephone contact should be maintained throughout transmission.
- Both sender and receiver must have an agreed process to avoid their copy being left on the Fax machine, and a clear requirement to securely destroy the message when no longer required.
- The message should contain clear instructions on the recipients responsibilities and instructions on what to do if they are not the correct recipients.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to their line manager.

4.4.4 **Delivery by Post or by Hand**

It is essential that the file, whether electronic or paper is kept secure in transit, tracked during transit, and delivered to the correct individual.

- An appropriate delivery mechanism must be used.
- Package must be securely and appropriately packed, clearly labelled and have a seal, which must be broken to open the package.
- Package must have a return address and contact details.
- The label must not indicate the nature or value of the contents.
- Package must be received and signed for by addressee.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to their line manager.

4.4.5 **Telephone/Mobile Phone**

As phone calls may be monitored, overheard or intercepted either deliberately or accidentally, care must be taken as follows.

- Transferred information must be kept to a minimum.
- Personal or Confidential information must not be transferred over the telephone unless the identity and authorisation of the receiver has been appropriately confirmed.
- CHA emails should only be received onto Association mobile phones and the Association can monitor which devices exchange user accounts are synchronised to.

4.4.6 **Internet Based Collaborative Sites**

Sites such as iCloud, OneDrive, GoogleDrive, Dropbox etc. can be used but only with express authorisation from a line manager. These sites should not be used for Personal or Confidential information.

4.4.7 **Text Messaging (SMS). Instant Messaging**
SMS must not be used for Personal or Confidential information.

4.4.8 **Office Paperwork/Files**

4.4.9 The Association will operate a clear desk policy and all personal and sensitive paperwork in relation to customers, staff, Management Committee members, etc. will be held securely in a locked cabinet/filing room when employee(s) have left the/their office.

4.5 Equipment Security

4.5.1 In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from security threats and environmental hazards. Physical and environmental protection measures must be developed, maintained, operated, and supported within parameters and according to standards established by the Association policies, and applicable laws and regulations.

4.5.2 The Association will provide secure server isolation facilities with protected power arrangements and climate controlled environments for the provision of central computing and network facilities.

4.5.3 Any computer equipment in general office environments should be secured behind locked doors and protected by automatic user log-out (after 15 minutes) and or password protected screensavers whenever it is left unattended; and outside of general office hours.

4.5.4 All IT assets must be recorded and labelled with an asset tag/bar code to allow each asset to be easily identified.

4.5.5 Physical media that contains or formerly contained information belonging to the Association must be handled, stored, and destroyed as needed or required in accordance with business objectives, Association policies, and applicable laws and regulations. Only appropriately authorised personnel or Users must use, handle, store, or destroy physical media that contains or formerly contained information belonging to the Association.

4.5.6 Physical media that contains or formerly contained information belonging to the Association which requires destruction must be destroyed beyond recovery.

4.6 Information Risk Assessment

4.6.1 The core principle of risk assessment and management thereof requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

4.6.2 Once identified, information security risks shall be managed on a formal basis. They shall be recorded within the Association's risk

register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of the Association's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

4.7 Information security events and weaknesses

4.7.1 All information security events and suspected weaknesses are to be recorded. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

4.8 Protection from Malicious Software

The Association shall use software countermeasures and management procedures to protect itself against the treat of malicious software. Minimum requirements are:

4.8.1 All devices should have centrally managed anti-virus software installed onto them which is regularly reviewed, maintained and updated with the latest definitions.

4.8.2 Laptops will all have firewalls installed onto them.

4.8.3 Internet access is protected by a firewall hosted and managed by the Association.

4.8.4 Internet access is directed through web filtering software managed by Association to provide security against malicious websites and content.

4.8.5 Email security filtering is in place to protect filter malicious email content and attachments.

4.9 Vulnerability Management

4.9.1 Historical, existing, and emerging vulnerabilities within or external to the Association networks, systems, and other information assets must be managed and/or monitored to ensure the on-going safety, security, and integrity of the systems and the information they contain and transmit.

4.10 External Access to the Network

The Association will use secure data transfer methods and mobile device management procedures to protect itself against unauthorised access the network. The Association will:

4.10.1 Provide remote access via a secure method of data transfer which will be hosted and managed by the Association.

4.10.2 Provide webmail services, which are controlled over HTTPS, which ensures that the data is encrypted; normal HTTP traffic is not encrypted.

4.10.3 Clydebank HA Smart phones and devices will be controlled by mobile device management solutions to enforce a passcode and remote wiping capabilities to protect against theft or loss. This access will be controlled by the Associationôs Access Control procedure.

4.11 Wireless Communication

The Association provides wireless network access for guest use and Internet access for staff that require access via remote devices owned by the Association. The Association will:

4.11.1 Ensure the wireless network is configured in such a way that users on the wireless network are unable to access the corporate local area network (LAN)

4.11.2 Ensure access to the network is authenticated using the WPA-PSK (AES) security protocol.

4.11.3 The password requirements to access the wireless network will be in line with section 4.14.2 of this policy. This knowledge of this password will be given to authorised personnel only and will be changed on a monthly basis to prevent guest users from impinging on the network. Authorised personnel will be listed in Appendix A of this policy.

4.11.4 Ensure Internet access on the wireless network is directed through web filtering software managed by Association to provide security against malicious websites and content.

4.12 Uncontrolled Storage Devices

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of Chief Executive before they may be used on Associationôs systems. Such media must also be fully virus checked before being used on the Associationôs equipment. Personal Data should not be copied to unprotected and uncontrolled media such as removable media or cloud storage solutions such as Dropbox, OneDrive etc.)

4.13 Authorised Computer Equipment and Storage Media

Only Association owned or leased computer equipment or storage media, or that which is owned by third parties under contractual agreement with Association, must be used to store, process or transmit Personal or Confidential information.

4.14 User Account Control

User access authorisation protocols, processes, and procedures must be crafted to prevent unauthorised access to Association information assets and to facilitate security incident detection and response.

4.14.1 User Creation and Deletion

4.14.1.1 The Associationôs IT Support Providers/Finance and IT Provider will only set up a new staff user on the Association network when authorised by the Chief Executive or in their absence, the Head of Housing Services, advising of the start date and network access requirements.

4.14.1.2 The IT Support Provider/Finance and IT Assistant will set a start date and expiry date (where applicable) in Active Directory.

4.14.1.3 The Chief Executive will notify the Head of Housing Services/Finance and IT Assistant BEFORE the employment end date of any employee, to allow the department to disable the user account after employment has been terminated. In the event of the user account being required to be left enabled, this must be authorised by the Chief Executive or in their absence, the Head of Housing Services and the password MUST be changed on the account. This request should be followed up regularly to ensure it is still valid.

4.14.1.4 The Chief Executive or in their absence, the Head of Housing Services will ensure any loaned IT equipment is collected from the user before employment is terminated.

4.14.1.5 Password Configuration Requirements

- All system-level passwords (e.g., root, enable, server admin, application administration accounts, etc.) must be changed on at least a 6 monthly basis.
- Password length must be at a minimum 8 characters long.
- All user level password age must be a maximum of 90 days.
- Password history must be enforced to at least 6 passwords.
- Password complexity rules must be forced.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic or physical communication.

4.14.1.6 Account Lockout Requirement

- Account Lockout duration must be set to at least 15 minutes
- Account Lockout attempts must be set to at least 5 attempts

4.15 Disaster Recovery Management

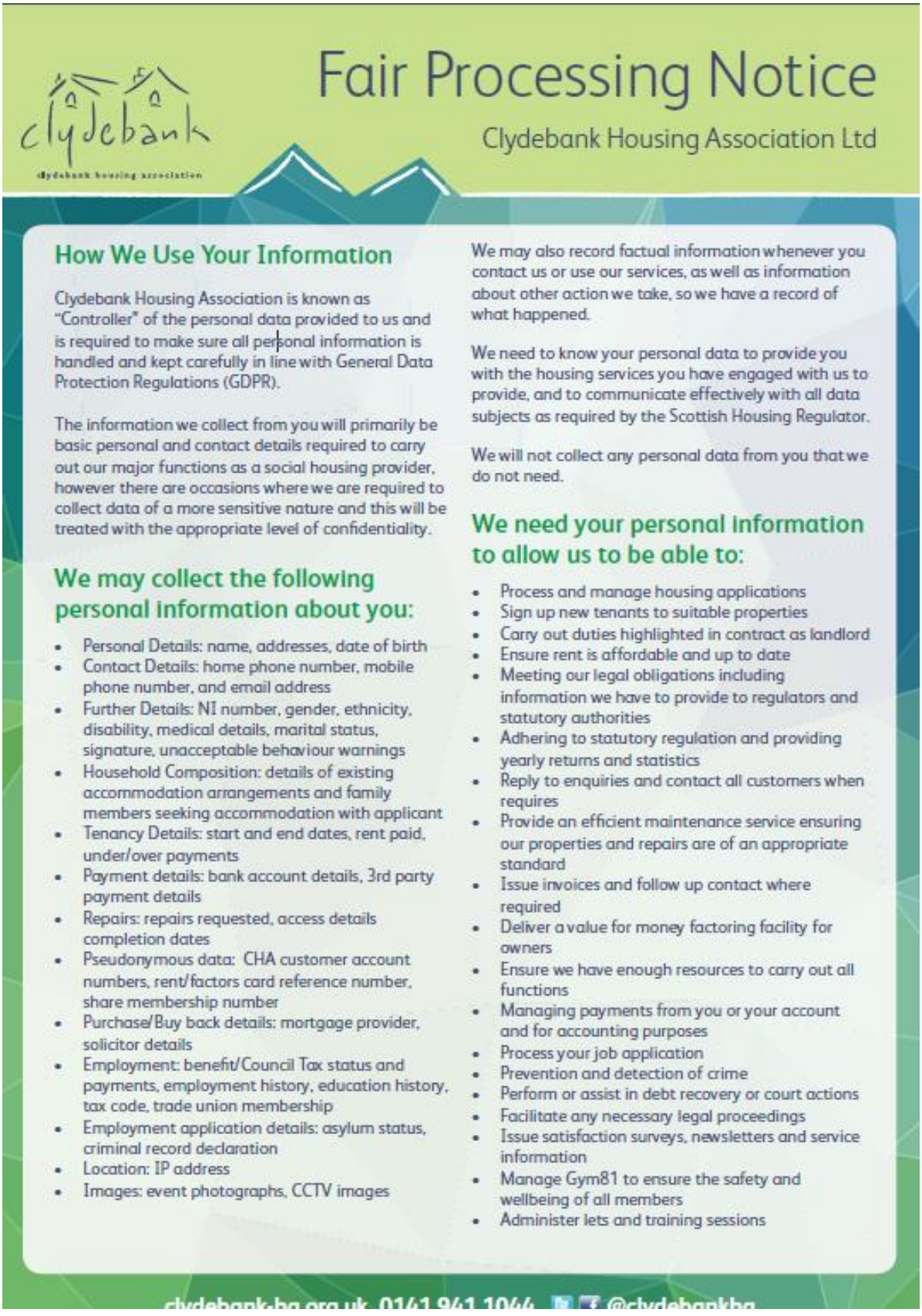
Network and application systems that are critical to the business must be planned for continuity of operations despite possible disruptive events to ensure that business operations are not adversely affected. The cost effectiveness and fitness of counter measures to be implemented and maintained must be considered and continually reviewed as part of the normal management responsibilities.

Please refer to The Associations Business Continuity and Disaster Recovery Policy for approved arrangements.

For Office Use Only – Required Actions

Customer Consultation Required/Arranged	No
Intranet Update	Yes
F Drive Update	Yes
Website Update	No
Leaflet change required?	No
Newsletter Promotion?	No
Other information updated, e.g. posters, automatic email responses, post cards, answering machine messages, etc.	No
Equality Impact Assessment completed	Yes 20.03.19

APPENDIX 2



Fair Processing Notice

Clydebank Housing Association Ltd

How We Use Your Information

Clydebank Housing Association is known as "Controller" of the personal data provided to us and is required to make sure all personal information is handled and kept carefully in line with General Data Protection Regulations (GDPR).

The information we collect from you will primarily be basic personal and contact details required to carry out our major functions as a social housing provider, however there are occasions where we are required to collect data of a more sensitive nature and this will be treated with the appropriate level of confidentiality.

We may collect the following personal information about you:

- Personal Details: name, addresses, date of birth
- Contact Details: home phone number, mobile phone number, and email address
- Further Details: NI number, gender, ethnicity, disability, medical details, marital status, signature, unacceptable behaviour warnings
- Household Composition: details of existing accommodation arrangements and family members seeking accommodation with applicant
- Tenancy Details: start and end dates, rent paid, under/over payments
- Payment details: bank account details, 3rd party payment details
- Repairs: repairs requested, access details completion dates
- Pseudonymous data: CHA customer account numbers, rent/factors card reference number, share membership number
- Purchase/Buy back details: mortgage provider, solicitor details
- Employment: benefit/Council Tax status and payments, employment history, education history, tax code, trade union membership
- Employment application details: asylum status, criminal record declaration
- Location: IP address
- Images: event photographs, CCTV images

We may also record factual information whenever you contact us or use our services, as well as information about other action we take, so we have a record of what happened.

We need to know your personal data to provide you with the housing services you have engaged with us to provide, and to communicate effectively with all data subjects as required by the Scottish Housing Regulator.

We will not collect any personal data from you that we do not need.

We need your personal information to allow us to be able to:

- Process and manage housing applications
- Sign up new tenants to suitable properties
- Carry out duties highlighted in contract as landlord
- Ensure rent is affordable and up to date
- Meeting our legal obligations including information we have to provide to regulators and statutory authorities
- Adhering to statutory regulation and providing yearly returns and statistics
- Reply to enquiries and contact all customers when requires
- Provide an efficient maintenance service ensuring our properties and repairs are of an appropriate standard
- Issue invoices and follow up contact where required
- Deliver a value for money factoring facility for owners
- Ensure we have enough resources to carry out all functions
- Managing payments from you or your account and for accounting purposes
- Process your job application
- Prevention and detection of crime
- Perform or assist in debt recovery or court actions
- Facilitate any necessary legal proceedings
- Issue satisfaction surveys, newsletters and service information
- Manage Gym81 to ensure the safety and wellbeing of all members
- Administer lets and training sessions

Sharing your Information

All personal data we process is processed by our staff in the UK. We sometimes need to share personal information with other organisations, however where this is necessary, we are required to comply with all aspects of the GDPR. Even when this is required, we only share data within the European Union (EU). We do not give anyone else access to your information in return for payment, for their marketing or commercial purposes.

Clydebank Housing Association may enter into partnerships with other organisations such as local authorities and the police. For example, we may join a partnership to help prevent and control anti-social behaviour. We will enter into a formal data sharing agreement to govern the process and ensure it is lawful. That agreement will be approved by our Data Protection Officer before it is implemented. The types of organisations we may share with in these instances are the following:

- West Dunbartonshire Council
- Other landlords
- Solicitors
- Trustees
- Sherriff Officers

We are also required to share information with statutory bodies governing finance and housing industries, for auditing and inspection purposes. However this will be restricted to the actual information required from the association and will mainly be viewed within the association, with strict permission set on our electronic file system to ensure use is controlled. We will also encrypt and limit the content of any files that do have to be sent either electronically or otherwise.

We will share specific and relevant information with law enforcement, government or public bodies and statutory agencies where we are legally required to do so in order to aid:

- The prevention or detection of crime and fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax or duty owed to customs and excise
- Sharing in relation to the physical or mental health of an individual, where disclosure is required to protect them or others from serious harm
- Sharing in connection with legal proceedings
- Research and statistical purposes

Clydebank Housing Association remains responsible for the fair and lawful processing of all personal data shared with suppliers. Unless we have requested your specific consent, we only share information with other external organisations or agencies that we have a signed agreement to do so with ensuring as data processor, all data they manage remains compliant to GDPR.

Contractors and Suppliers

We may share your personal information with our suppliers who provide a service to you, or who provide services on our behalf. The data shared is the specific information the supplier requires to carry out their task, as well as any information that ensures we fulfil our health and safety obligations to the people carrying out the task. We may share this information with the following organisations:

- Maintenance contractors and suppliers
- Printing and mail distribution
- Customer surveys
- Insurers
- Banks
- Payment card, direct debit and billing solutions
- Document storage and archive scanning

In order to ensure all tenants have the required utilities available when they sign up to a tenancy with Clydebank Housing Association, we may also provide names addresses, forwarding addresses, contact details and tenancy dates to utility providers.

Special Category Data

There are certain occasions where it will be necessary to perform our functions as a social housing landlord for us to share information containing special categories of data. Currently we would only ever share the following type of this more sensitive information:

- Racial or ethnic origin: Shared with statutory bodies and reported on as a statistical breakdown of housing or job applicants only, not including any actual personal data

Third Party Access

Any third party who Clydebank Housing Association gives access to our electronic files is therefore called a Data Processor because they are processing data on behalf of the Association. Although the Data Controller and Data Processor are two separate entities, we are required to ensure all third party access is given in compliance with all GDPR principles, and to this affect will have a third party access agreement in place.

The following organisations may be given controlled access to our electronic network for reasons of security, maintenance, or any specific purposes outlined in their third party agreement:

- IT maintenance/support contractors
- Specialist housing software providers
- User and file system auditing software provider

Power of Attorney

If you wish anyone to deal with your affairs on your behalf please find specific consent form for this on our website or request this from the office. This allows you to request a named person to discuss specific or all of your personal data with the Association as required.

We will not share your personal information with anyone who claims to represent you unless we are satisfied that you have appointed them or they act in some recognised official capacity. There may be a delay to us dealing with requests whilst we confirm the caller's identity, or check that we have your approval to deal with them.

Violent or Abusive Behaviour

If you are violent or abusive to Clydebank Housing Association staff, customers or other residents, we may decide to place a "warning marker" on your customer record in order to protect Clydebank Housing Association colleagues.

If we do this, we will write and tell you why and you will have the right to appeal against our decision as per our Unacceptable Behaviour Policy. We will share this information with our partners, for example our contractors or the Fire Service in order to protect their colleagues too.

How we store your personal information

We are committed to holding your personal information securely. This means only those of our colleagues and contractors that need to see it have access.

Unless you pay our bills using direct debit we will not usually retain your payment details. Whoever pays your bills will have to give us the payment card details each time they make a payment.

If we store your personal information and can do so solely on computers we will, however there will be cases where we have paper copies instead, or in addition to this. All computers are kept in secure location and are password protected, with unusual and unauthorised access monitored by specialist auditing software and our electronic files kept on shared network accessed by our computers are controlled by strict access permissions so data is only available to those who need to use it. Paper files containing personal or sensitive information will be kept in locked drawers, cabinets or rooms.

Our computer systems are located in our offices in Clydebank but we occasionally may use computers (including laptops and tablets) offsite, however they will at all times remain secure and under our control.

We will keep your personal details for no longer than necessary. Once the information is no longer required for the lawful purpose for which it was obtained it will be destroyed. More information on the document retention schedule adopted by the association can be found in the Nation Housing Federation's most recent guide to document retention available online at

www.housing.org.uk/resource-library/browse/document-retention-for-housing-associations

See over the page for information on Your Rights

Your Rights

If at any point you believe the information we hold is incorrect you may request to see it, have it corrected or deleted. You are entitled to request a copy of any personal data we hold of yours.

You have the right to ask us not to process all or part of the personal information we have received, however we may be unable to provide our service to you if we are unable to record and process certain details.

If you wish to complain about how we have handled your data you can contact our Data Protection Officer who will investigate the matter on your behalf. If you are not satisfied with our response you may submit a formal complaint to the Information Commissioners Office.

Our Data Protection officer can be contacted at dataprotection@clydebank-ha.org.uk

A full Fair Processing Notice including details of how we retrieve, use, share and manage data from all client groups can be found online at http://clydebank-ha.org.uk/data-protection/ or by request from our office.

If you or someone you know would like this notice in any other format, please contact us.

Clydebank Housing Association Ltd
77-83 Kilbowie Road
Clydebank
G81 1BL
Tel 0141 941 1044 info@clydebank-ha.org.uk twitter: @clydebankha
Fax 0141 941 3448 www.clydebank-ha.org.uk facebook: @clydebankha

Please recycle this notice when you are finished with it

clydebank housing association

APPENDIX 3

MODEL DATA SHARING AGREEMENT - RSLS

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]**")]ð ***[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 being adapted for every individual use of this model Agreement.

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

(f) the Data Protection Act 1998;

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

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

(i) 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 **Error! Reference source not found.** 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 **Error! Reference source not found.**.

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 monthsônotice 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 **Error! Reference source not found.**, 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 **Error! Reference source not found.** and **Error! Reference source not found.** 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 **Error! Reference source not found.**, 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 **Error! Reference source not found.**.

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 courierôs 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.

IN WITNESS WHEREOF these presents consisting of this and the preceding 6 pages together with the Schedule in 6 parts hereto are executed by the Parties hereto as follows:

On behalf of the Association
at

on

by

Print Full Name	Director/Secretary/Authorised Signatory

before this witness

Print Full Name	Witness

Address

On behalf of #[Party 2]
at

on
by

Print Full Name

Director/Secretary/Authorised Signatory

before this witness

Print Full Name

Witness

Address

This is the Schedule referred to in the foregoing Data Sharing Agreement between the ASSOCIATION and #[Party 2]

APPENDIX 4

MODEL DATA PROTECTION ADDENDUM

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]*] (the "Processor")

(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.]

(d) The Association and the Processor have entered in to an agreement/ contract to #[insert detail] (hereinafter the "Principal Agreement"/"Principal Contract");

(e) This Data Protection Addendum forms part of the Principal Agreement/Principal Contract (*delete as appropriate); and

(f) In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalised terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement/Contract shall remain in full force and effect. In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 **"Applicable Laws"** means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Association Personal Data in

respect of which any Company Group Member is subject to any other Data Protection Laws;

1.1.2 "**Association Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of the Association pursuant to or in connection with the Principal Agreement/Contract;

1.1.3 "**Contracted Processor**" means Processor or a Sub processor;

1.1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.8 "**Restricted Transfer**" means:

1.1.8.1 a transfer of Association Personal Data from the Association to a Contracted Processor; or

1.1.8.2 an onward transfer of Association Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of the Processor for the Association pursuant to the Principal Agreement/ Contract;

1.1.10 "**Sub processor**" means any person (including any third party and any , but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of Processor which is engaged in the Processing of Personal Data on behalf of the Association in connection with the Principal Agreement/Contract; and

1.2 The terms, "**Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their related terms shall be construed accordingly.

1.3 The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly**.**

2. Processing of Association Personal Data

2.1 The Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Association Personal Data; and

2.1.2 not Process Association Personal Data other than on the Association's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform the Association of that legal requirement before the relevant Processing of that Personal Data.

2.2 The Association

2.2.1 Instructs the Processor (and authorises Processor to instruct each Sub processor) to:

2.2.1.1 Process Association Personal Data; and

2.2.1.2 in particular, transfer Association Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement/Contract; and

2.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 2.2.1.

2.3 The Schedule to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Association Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). The Association may make reasonable amendments to the Schedule by written notice to Processor from time to time as the Association reasonably considers necessary to meet those requirements. Nothing in the Schedule (including as amended pursuant to this section 2.3) confers any right or imposes any obligation on any party to this Addendum.

3. Processor and Personnel

The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Association Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Association Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall in relation to the Association Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. **Sub processing [*Drafting Note: This clause should be adjusted depending on the arrangements between Parties*]**

5.1 The Association authorises the Processor to appoint (and permit each Sub processor appointed in accordance with this section 5 to appoint) Sub processors in accordance with this section 5 and any restrictions in the Principal Agreement.

5.2 The Processor may continue to use those Sub processors already engaged by the Processor as at the date of this Addendum, subject to the Processor in each case as soon as practicable meeting the obligations set out in section 5.4.

5.3 The Processor shall give the Association prior written notice of its intention to appoint a Sub processor, including full details of the Processing to be undertaken by the Sub processor. The Processor shall not appoint (nor disclose any Association Personal Data to) the proposed Sub processor except with the prior written consent of the Association.

5.4 With respect to each Sub processor, the Processor or the relevant shall:

5.4.1 before the Sub processor first Processes Association Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due

diligence to ensure that the Sub processor is capable of providing the level of protection for Association Personal Data required by the Principal Agreement;

5.4.2 ensure that the arrangement between on the one hand (a) the Processor, or (b) the relevant intermediate Sub processor; and on the other hand the Sub processor, is governed by a written contract including terms which offer at least the same level of protection for Association Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

5.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) the Processor or (b) the relevant intermediate Sub processor; and on the other hand the Sub processor, or before the Sub processor first Processes Association Personal Data; and

[***Drafting Note: Each member organisation will require checking arrangements with its Data Processors to ascertain where the Processing is taking place – i.e. within UK/EEA or outwith. If outwith, where. The Standard Contractual Clauses are not appended to this initial draft for discussion as it is not anticipated that member organisations will be contracting with Data Processors who are Processing Personal Data out with the UK/EEA***]

5.4.4 Provide to the Association for review such copies of the Contracted Processors' agreements with Sub processors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as the Association may request from time to time.

5.5 The Processor shall ensure that each Sub processor performs the obligations under sections 2.1, 3, 4, 6.1, 7.2, 8 and 10.1, as they apply to Processing of Association Personal Data carried out by that Sub processor, as if it were party to this Addendum in place of the Processor.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, the Processor shall assist the Association by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Association's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 The Processor shall:

6.2.1 promptly notify the Association if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Association Personal Data; and

6.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of the Association or as required by Applicable Laws to which the Contracted Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform the Association of that legal requirement before the Contracted Processor responds to the request.

7. **Personal Data Breach**

7.1 The Processor shall notify the Association without undue delay upon the Processor or any Sub processor becoming aware of a Personal Data Breach affecting the Association Personal Data, providing the Association with sufficient information to allow it to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 The Processor shall co-operate with the Association and at its own expense take such reasonable commercial steps as are directed by the Association to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

The Processor shall provide reasonable assistance to the Association with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Association reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Association Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Association Personal Data

9.1 Subject to sections 9.2 and 9.3, the Processor shall promptly and in any event within seven (7) days of the date of cessation of any Services involving the Processing of Association Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

9.2 Subject to section 9.3, the Association may in its absolute discretion by written notice to the Processor within seven (7) days of the Cessation Date require the Processor

to (a) return a complete copy of all Association Personal Data to the Association by secure file transfer in such format as is reasonably notified by the Association to the Processor; and (b) delete and procure the deletion of all other copies of Association Personal Data Processed by any Contracted Processor. The Processor shall comply with any such written request within seven (7) days of the Cessation Date.

9.3 Each Contracted Processor may retain Association Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that the Processor shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

9.4 Processor shall provide written certification to the Association that it has fully complied with this section 9 within fourteen (14) days of the Cessation Date.

10. Audit rights

10.1 Subject to sections 10.2 and 10.3, the Processor shall make available the Association on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by the Association or an auditor mandated by the Association in relation to the Processing of the Association Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Association only arise under section 10.1 to the extent that the Principal Agreement/Contract does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

10.3 Where carrying out an audit of Personal Data, the Association shall give the Processor reasonable notice of any audit or inspection to be conducted under section 10.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

10.3.1 to any individual unless they produce reasonable evidence of identity and authority; or

10.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the

Association undertaking an audit has given notice to the Processor that this is the case before attendance outside those hours begins

11. General Terms

Governing law and jurisdiction

11.1 The Parties hereby submit to the choice of jurisdiction stipulated in the Principal Agreement/Contract with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

11.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement/Contract.

Order of precedence

11.3 Nothing in this Addendum reduces the Processor's obligations under the Principal Agreement/Contract in relation to the protection of Personal Data or permits the Processor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement/Contract.

11.4 Subject to section 11.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement/Contract and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

[Drafting Note: see comments above re Restricted Transfers etc and the applicability of standard contractual clauses]

Changes in Data Protection Laws, etc.

11.5 The Association may:

11.5.1 by giving at least twenty eight (28) daysôwritten notice to the Processor, from time to time make any variations to the terms of the Addendum which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

11.5.2 propose any other variations to this Addendum which the Association reasonably considers to be necessary to address the requirements of any Data Protection Law.

Severance

11.6 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the partiesô intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

On behalf of the Association

at

on

by

Print Full Name	Director/Secretary/Authorised Signatory

before this witness

Print Full Name	Witness

Address

On behalf of the Processor

at

on

by

Print Full Name

Director/Secretary/Authorised Signatory

before this witness

Print Full Name

Witness

Address

APPENDIX 5 – to follow – Refer to NHF Retention document

Data Retention Periods

The table below sets out retention periods for Personal Data held and processed by the Association in accordance with National Housing Federation recommended figures. 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 ï 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,	3 years after the end of the tax year to which they relate

calculations, certificates (MAT 1Bs) or other medical evidence	
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 tenantsôfiles (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/residentsô meetings	1 year
Minute of factoring meetings	Duration of appointment

APPENDIX 6

Specific Consent Form

I ....., confirm I am over the age of 16 and consent to the following personal or sensitive data being processed for the specified purpose shown below:

What data .....

For what specific purpose .....

.....

.....

I consent to this data being processed from the date given below until .....

If consent is needed for a further purpose or timeframe, we are required to gain additional specific consent to do so.

Please note: If you wish to remove this consent please contact the Association for a withdrawal form, in order for any processing to be stopped immediately.

Name:	
Address:	
Signature:	**Date:**

Clydebank Housing Association Ltd
77-83 Kilbowie Road
Clydebank
G81 1BL
Tel 0141 941 1044 info@clydebank-ha.org.uk twitter: @clydebankha
Fax 0141 941 3448 www.clydebank-ha.org.uk facebook: @clydebankha