PRIVACY POLICY

Approved: 4 March 2020
Review date: March 2023

Contents

1. Introduction

1.1 Govanhill Housing Association and its subsidiary Govanhill Community Development Trust (hereinafter the "Association") is committed to ensuring the secure and safe management of data held by the Association in relation to customers, staff and other individuals. The Association's staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures outlined in this policy and documentation referred to herein.

1.2 The Association needs to gather and use certain information about individuals. These can include customers (tenants, factored owners etc.), employees and other individuals that the Association has a relationship with. The Association manages a significant amount of data, from a variety of sources. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the GDPR).

1.3 This Policy sets out the Association's duties in processing that data, and the purpose of this Policy is to set out the procedures for the management of such data.

1.4 Appendix 1 hereto details the Association's related policies.

2. Legislation

2.1 It is a legal requirement that 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:

- the General Data Protection Regulation (EU) 2016/679 ("the GDPR");
- the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications);
- the Data Protection Act 2018 ("the 2018 Act") and
- any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union

3. Data

3.1 The Association holds a variety of Data relating to individuals, including customers and employees (also referred to as Data Subjects). Data which can identify Data Subjects 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.

3.2 "Personal Data" is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by the Association.

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

4 Processing of Personal Data

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

- Processing with the consent of the data subject (see clause 4.4 hereof);
- Processing is necessary for the performance of a contract between the Association and the data subject or for entering into a contract with the data subject;
- Processing is necessary for the Association's compliance with a legal obligation;
- Processing is necessary to protect the vital interests of the data subject or another person; or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the Association's official authority.

4.2 Fair Processing Notice

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

4.2.2 The Fair Processing Notice at Appendix 2 sets out the Personal Data processed by the Association and the basis for that Processing. This document is provided to all of the Association's customers at the outset of processing their data

4.3 Employees

4.3.1 Employee Personal Data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by the Association. Details of the data held and processing of that data is contained within the Employee Fair Processing Notice which is provided to prospective Employees at application stage.

4.3.2 A copy of any employee's Personal Data held by the Association is available upon request by that employee from the Association's Data Protection Officer (see part 8).

4.4 Consent

4.4.1 Consent as a ground of processing will require to be used from time to time by the Association when processing Personal Data. It should be used by the Association where no other alternative ground for processing is available. In the event that the Association requires to obtain consent to process a Data Subject's Personal Data, it shall obtain that consent in writing. The consent provided by the Data Subject must be freely given and the Data Subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained by the Association must be for a specific and defined purpose (i.e. general consent cannot be sought). Where consent is being relied on, Data Subjects are free to withhold their consent or withdraw it at any future time.

4.5 Processing of Special Category Personal Data or Sensitive Personal Data

4.5.1 In the event that the Association processes Special Category Personal Data or Sensitive Personal Data, the Association must rely on an additional ground for processing in accordance with one of the special category grounds. These include, but are not restricted to, the following

- 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, social security, or social protection law;
- Processing is necessary for health or social care
- 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 under law

4.5.2 All the grounds for processing sensitive personal data are set out in Article 9(2) of the GDPR and expanded on in the Data Protection Act 2018.

5. Data Sharing

5.1 The Association shares its data with various third parties for numerous reasons in order that its day-to-day activities are carried out in accordance with the Association's relevant policies and procedures. In order that the Association can monitor compliance by these third parties with Data Protection laws, the Association may 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. This will only apply in situations where the third party is a joint controller.

5.2 Personal Data is from time-to-time shared amongst the Association and third parties who require to process the same Personal Data as the Association. Whilst the Association and third parties may jointly determine the purposes and means of processing, both the Association and the third party will be processing that data in their individual capacities as data controllers.

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

5.4 Data Processors

5.4.1 A data processor is a third-party entity that processes Personal Data on behalf of the Association and are frequently engaged if certain of the Association's work is outsourced (e.g. payroll, maintenance and repair works).

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

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

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

6. Data Storage and Security

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

6.2 **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 ensure that no Personal Data is left in a place 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 secure destruction. If the Personal Data requires to be retained on a physical file then the employee should ensure that it is affixed to the file which is then stored in accordance with the Association's storage provisions.

6.3 **Electronic Storage**
Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should be password protected when being sent internally or externally to the Association's data processors or those with whom the Association has entered in to a Data Sharing Agreement. If Personal Data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be encrypted and 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.

7. Breaches

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

7.2 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 it becomes known the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the Association's DPO must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
- The Association must seek to contain the breach by whichever means available;
- The DPO must consider whether the breach is one which requires to be reported to the ICO and to the Data Subjects affected and, if appropriate, will do so in accordance with this clause 7;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

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

8. Data Protection Officer ("DPO")

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

8.2 The DPO will be responsible for:

- monitoring the Association's compliance with Data Protection laws and this Policy;
- co-operating with and serving as the Association's contact for discussions with the ICO
- reporting breaches or suspected breaches to the ICO and data subjects in accordance with Part 7 hereof.

9. Data Subject Rights

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

9.2 Data Subjects have a right to request a restriction of processing their data, a right to request erasure of their Personal Data, and a right to object to the Association's processing of their data. These rights are notified to the Association's tenants and other customers in the Association's Fair Processing Notice. Such rights are subject to qualification and are not absolute.

9.3 **Subject Access Requests**

9.3.1 Data Subjects are permitted to view their Personal 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 from the day after the date of receipt of the request. The Association:

- must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law.
- 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
- where the Association does not hold the Personal Data sought by the Data Subject, must confirm that it does not hold any or that Personal Data sought to the Data Subject as soon as practicably possible, and in any event, not later than one month from the day after the date on which the request was made.

9.4 **The Right to Erasure**

9.4.1 A Data Subject can exercise their right to erasure (otherwise known as the right to be forgotten) by submitting a request to the Association seeking that the Association erase the Data Subject's Personal Data in its entirety.

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

9.4.3 Requests for Erasure will be considered and responded to by the Association by one month from the day after the date we receive the request.

9.5 The Right to Restrict or Object to Processing

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

9.5.2 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.

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

9.6 The Right to Rectification

9.6.1 A Data Subject may request the Association to have inaccurate Personal Data rectified. If appropriate, a Data Subject may also request the Association to have incomplete Personal Data completed.

9.6.2 Each request received by the Association will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the Data Subject's request in accordance with clause 9.6 and will respond in writing to the request.

10. Privacy Impact Assessments ("PIAs")

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

10.2 The Association shall:

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

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

10.3 The Association will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced or mitigated. 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.

10.4 Archiving, Retention and Destruction of Data

10.4.1 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.

Appendix 1: Related Policies & Procedures

Guidance: Dealing with personal or/and sensitive information

1. Introduction

1.1 Govanhill Housing Association will manage personal and sensitive data in accordance with the requirements of the General Data Protection Regulations.

1.2 We hold such data about applicants, tenants, owners, staff and committee members.

1.3 We have a Privacy Policy in place which outlines our duties in more detail and have issued fair processing notices to each of the groups noted above. This procedure provides more detail on how we should obtain, use, store and share personal and sensitive data.

2. Definition of personal and sensitive information

2.1 Personal data means any information relating to an identifiable person who can be directly or indirectly identified.

2.2 This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

2.3 Special category or sensitive personal data is defined in the GDPR as the type of data which could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. This could include but is not limited to information about an individual's :

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

3. Obtaining personal or sensitive data

3.1 Our fair processing notices set out in what circumstances we will obtain and keep personal or sensitive information. If we receive such information in any other way then it is likely that we will have to seek explicit consent of its use and storage. Please speak to the Information officer for further guidance.

3.2 Please be aware when adding notes to the Capita system that the tenant/owner's name should not be used within the text as this is not searchable and therefore cannot be traced and deleted as required by GDPR timescales.

4. Using general information, personal or sensitive data

4.1 Our fair processing notices set out in what circumstances we will use personal or sensitive information. If we require to use such information in any other way then it is likely that we will have to seek explicit consent for this. Please speak to the Information Officer for further guidance.

4.2 Information about customers

General guidance on use of customer information:

- Committee reports and minutes must not contain information identifying individual customers (e.g. names, addresses, household composition etc.).
- Committee members must not have access to customers' personal information records.
- Staff may share information with colleagues within the Association, when working as part of a team to provide services.
- All data records (paper and digital) must be kept securely and confidentially.

4.3 The Association will investigate any alleged breaches of confidentiality. Serious or deliberate breaches will be dealt with under the Association's codes of conduct and may result in disciplinary action for a member of staff, or a vote to remove a member of the Management Committee.

5. Sharing personal or sensitive data

5.1 We require to have stringent levels of control in terms of sharing personal or sensitive data and those we share this data with are noted in the fair processing notices.

5.2 We should however maintain the highest standards of confidentiality with all information we hold. This procedure sets out in detail what we expect of staff in this regard.

5.3 Except for those organisations noted in the fair processing notices, we should only share information with the data subject unless we have a mandate from them authorising someone to act on their behalf.

6. Sharing data in person

6.1 In a face to face interview it is appropriate to share information with the data subject and anyone else they choose to bring with them. Be aware that any information shared should be only about them and should not identify any other party.

6.2 If interviewing the data subject in our office, the interview should be conducted in the privacy of the interview room and not in the public area where the conversation could be overheard.

6.3 If using the computer as part of the interview, it must be logged off at the conclusion of the interview to safeguard the records of the data subject concerned and the security of our computer network.

7. Sharing data by telephone

7.1 Always confirm who you are speaking to before releasing information. Ask the caller to provide proof of identity or/and call them back on a number which should match that which we have on record for them.

7.2 If someone is unable to provide proof of their identity, advise them you will send the requested information to the address we have on record for them by 1st class post including their reference number which ensures that next time you will be able to share the information.

7.3 Leaving messages on answerphones:
Confidentiality can be breached from messages left on answer phones, resulting in embarrassing or harmful situations arising.. Before leaving a message consider the urgency of getting the information to the individual. If you feel you have to leave a message, think about what you say, and leave the minimum amount of information – for example, 'Please call (full name) on(number) to talk about your appointment' Leaving your name and direct dial number will ensure the individual can call you back and not need to share information with other staff or be passed around trying to find the right staff member.

7.4 When the phone is answered by someone else:
Always ask to speak to the individual, but don't say where you are calling from initially.
If they ask who is calling, you should respond with a minimum amount of information. Stating the organisation name may then be sufficient.

If the individual is not present, then unless there is a degree of urgency do not leave a message, but ask when is a good time to call back.

If the individual is present but unable to speak (either due to language or physical difficulties), ask to speak to the next of kin. Before giving information to them, try to ascertain whether they are aware of why you may be calling (it may be necessary to reveal basic information to do this)

8. Sharing data by post

8.1. External Mail: use a robust envelope (not an Internal Mail envelope), double envelope where size or weight dictates; mark "Private & Confidential", for personal or sensitive data send either "Recorded Signed For" or "Special Delivery" or private courier, clearly print name and full address of recipient (and sender on reverse) and request acknowledgement of safe receipt.

8.2 Removable devices and DVDs sent by post: must be encrypted and sent by courier.

8.3 Opening incoming post: Where confidential mail is received (eg marked Personal, Private & Confidential, In Confidence, etc) this should only be opened by the addressee unless authority has been delegated. If a letter comes in addressed to an individual but is not otherwise marked you should open it. Local arrangements must be made to deal with post received in the absence of addressees.

9. Sharing data by email

9.1 Whatever route the email takes, the subject line of the email must never contain personal confidential information.

9.2 Please check the accuracy of the email address you are sending information to and use appropriate encryption if the information is personal or sensitive. Please check with IT for further guidance.

9.3 Emails which contain personal or sensitive information should be deleted from your sent box as soon as you have sent them.

9.4 If you receive an incorrectly addressed email you must inform the sender so that they can correct their records, you must then delete the email from your inbox.

10. Use of portable equipment

10.1 A number of staff use mobile phones or/and tablets for work purposes. These must be treated with care as they allow a thief access to our systems if they are not properly secured.

10.2 Mobile phones and tablets must be password protected and an appropriate time lapse set for auto lock.

10.3 When using such a device outside the office, it must be kept on your person at all times and never left within a vehicle.

10.4 If you lose the device or have it stolen, you must report this immediately to your line manager as we can then track and wipe the device.

11. Monitoring & review

11.1 We expect all staff to adhere to the above processes and may instigate disciplinary action if this guidance is not followed.

11.2 If you are unsure about any aspect of this guidance please discuss with your line manager

Data Breach procedure

1. Introduction

1.1 Govanhill Housing Association and its subsidiary Govanhill Community Development Trust collects, holds, processes, and shares personal data. We need to treat this information confidentially and in a secure manner.

1.2 Every care is taken to protect personal data from incidents (either accidental or deliberate) to avoid a data protection breach that could compromise security.

1.3 Compromise of information, confidentiality, integrity or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial and reputational costs.

2. Purpose and Scope

2.1 We are obliged under Data Protection legislation1 to have in place a framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

2.2 This procedure should be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the organisation.

2.3 This policy relates to all personal and special categories (sensitive) of data held by the organisation regardless of format.

2.4 This policy applies to all staff. This includes temporary, casual or agency staff and also contractors, consultants, suppliers and data processors working for, or on behalf of the organisation.

2.5 By using this procedure we aim to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

3. Definitions / Types of breach

3.1 For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

3.2 An incident in the context of this procedure is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to our information assets and / or reputation.

3.3 An incident includes but is not restricted to, the following:

3.3.1 loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record) whether or not it has been encrypted;
3.3.2 equipment theft or failure;
3.3.3 system failure;
3.3.4 unauthorised use of, access to or modification of data or information systems;
3.3.5 attempts (failed or successful) to gain unauthorised access to information or IT system(s);

3.3.6 unauthorised disclosure of sensitive / confidential data;
3.3.7 website defacement;
3.3.8 hacking attack;
3.3.9 unforeseen circumstances such as a fire or flood;
3.3.10 human error;
3.3.11 'blagging' offences where information is obtained by deceiving the organisation who holds it.

4. Reporting an incident

4.1 Any individual who accesses, uses or manages our information is responsible for reporting data breach and information security incidents immediately to the head of Corporate Services & HR or in her absence to another member of the Management Team.

4.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

4.3 The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process (refer to Appendix 1).

4.4 All staff should be aware that any breach of Data Protection legislation may result in our Disciplinary Procedures being instigated.

5. Containment and recovery

5.1 The Head of Corporate Services & HR will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

5.2 An initial assessment will be made to establish the severity of the breach and who will take the lead investigating the breach, as the Lead Investigation Officer (LIO) (this will depend on the nature of the breach; in some cases it could be the Head of Corporate Services & HR or more likely the line manager in charge of the department/section in which the breach occurred).

5.3 The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

5.4 The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

5.5 Advice from experts such as legal advisors or our insurance company may be sought in resolving the incident promptly.

5.6 The Head of Corporate Services & HR and LIO will determine the suitable course of action to be taken to ensure a resolution to the incident.

6. Investigation and risk assessment

6.1 An investigation will be undertaken by the LIO immediately and wherever possible, within 24 hours of the breach being discovered / reported.

6.2 The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

6.3 The investigation will need to take into account the following:
6.3.1 the type of data involved;
6.3.2 its sensitivity;
6.3.3 the protections are in place (e.g. encryptions);
6.3.4 what has happened to the data (e.g. has it been lost or stolen);
6.4.5 whether the data could be put to any illegal or inappropriate use;
6.4.6 data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);
6.4.7 whether there are wider consequences to the breach.

7. Notification

7.1 The Head of Corporate Services & HR & Information Officer will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, the Information Officer acting as Data Protection Officer for the Association, notify them within 72 hours of becoming aware of the breach, where feasible.

7.2 Every incident will be assessed on a case by case basis; however, the following will need to be considered:
7.2.1 whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation 2;
7.2.2 whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);
7.2.3 whether notification would help prevent the unauthorised or unlawful use of personal data;
7.2.4 whether there are any legal / contractual notification requirements;
7.2.5 the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

7.3 Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. The Head of Corporate Services & HR will decide whether notification is required. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact us for further information or to ask questions on what has occurred.

7.4 The Head of Corporate Services & HR must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

7.5 The Head of Corporate Services & HR will decide with the Director or/and Chair a press release should be prepared and/or issued.

8. Evaluation and response

8.1 Once the initial incident is contained, the Head of Corporate Services & HR will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

8.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

8.3 The review will consider:

8.3.1 where and how personal data is held and where and how it is stored;
8.3.2 where the biggest risks lie including identifying potential weak points within existing security measures;
8.3.3 whether methods of transmission are secure; sharing minimum amount of data necessary;
8.3.4 staff awareness;
8.3.5 implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

8.4 A record will be kept of any personal data breach, regardless of whether notification was required. This will be reported quarterly to the management Committee.

DATA BREACH REPORT FORM

To be completed by person reporting incident

Please act promptly to report any data breaches. If you discover a data breach, please notify a member of the Management Team immediately, complete Section 1 of this form and email it to her immediately you have the necessary information Section 1: Notification of Data Security Breach
Date incident was discovered:
Date(s) of incident:
Place of incident:
Name of person reporting incident:
Contact details of person reporting incident (email address, telephone number):
Brief description of incident or details of the information lost:
Number of Data Subjects affected, if known:
Has any personal data been placed at risk? If, so please provide details:
Brief description of any action taken at the time of discovery:
For use by the Head of service
Received by:
On (date):
Forwarded for action to:
On (date):

Appendix 2: Fair processing notice

GDPR Fair Processing Notice

(How we use your personal information)

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

Who are we?

Govanhill Housing Association, is a Scottish Charity (Scottish Charity Number SCO10307) and having their Registered Office at 79 Coplaw Street, Glasgow G42 7JG. We take the issue of security and data protection very seriously and strictly adhere to guidelines published in the Data Protection Act of 2018 (the 2018 Act) and the General Data Protection Regulation (EU) 2016/679 (GDPR) which is applicable from the 25th May 2018, together with any domestic laws subsequently enacted.

We are registered as a Data Controller with the Office of the Information Commissioner (ICO) under registration number Z9769493 and we are the data controller of any personal data that you provide to us.

Our Data Protection Officer is Chris Mochan, gdprinfo@govanhillha.org, 0141 433 2157.

Any questions relating to this notice and our privacy practices should be sent to Chris Mochan, gdprinfo@govanhillha.org, 0141 433 2157.

How we collect information from you and what information we collect

We collect information about you to enable us to perform our contractual obligations. You, in turn, are under a contractual obligation to provide the data requested from you to enable performance of the contract (i.e. the tenancy agreement you are party to):

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

Under the terms of the tenancy agreement, you are required to provide us with the following information:

- name (including any alias you may use)
- address
- gender
- date of birth
- ethnicity
- nationality
- details of any disability
- housing benefit reference number
- telephone number
- e-mail address;
- National Insurance number;
- next of kin/emergency key holder;

We receive the following information from third parties:

- Benefits information, including awards of Housing Benefit/ Universal Credit
- Payments made by you to us;
- Complaints or other communications regarding behaviour or other alleged breaches of the terms of your contract with us, including information obtained from Police Scotland;
- Reports as to the conduct or condition of your tenancy, including references from previous tenancies, and complaints of anti-social behaviour
- Information supplied by the relevant authority regarding any housing application

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

We need your information and will use your information to undertake and perform our obligations and duties to you in accordance with the terms of our contract with you. This includes:

to enable us to supply you with the services and information which you have requested;

to enable us to respond to your repair request, housing application and complaints made;

to analyse the information we collect so that we can administer, support and improve and develop our business and the services we offer;

to contact you in order to send you details of any changes to our or supplies which may affect you;

for all other purposes consistent with the proper performance of our operations and business; and

to contact you for your views on our products and services.

Sharing of Your Information

The information you provide to us will be treated by us as confidential and will be processed only by our employees within the UK/EEA

We may disclose your information to other third parties who act for us for the purposes set out in this notice or for purposes approved by you, including the following:

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

- If we are investigating a complaint, information may be disclosed to Police Scotland, Local Authority departments, Scottish Fire & Rescue Service and others involved in any complaint, whether investigating the complaint or otherwise;
- If we are updating tenancy details, your information may be disclosed to third parties (such as utility companies and the Local Authority);
- If we are investigating payments made or otherwise, your information may be disclosed to payment processors, Local Authority and the Department for Work & Pensions;
- If we are conducting a survey of our products and/ or service, your information may be disclosed to third parties assisting in the compilation and analysis of the survey results
- With our solicitors and auditors

Unless we have a lawful basis for disclosure, we will not otherwise share, sell or distribute any of the information you provide to us without your consent.

Transfers outside the UK and Europe

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

Security

When you give us information we take steps to make sure that your personal information is kept secure and safe. We password protect our systems and all electronic data is stored securely. All paper files are kept in locked cabinets.

How long we will keep your information

We review our data retention periods regularly and will only hold your personal data for as long as is necessary for the relevant activity, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you. Please see our retention schedule for more detailed information on this. http://www.govanhillha.org/wp-content/uploads/2019/10/Retention-schedule-Oct-2019.pdf

Your Rights

You have the right at any time to:

ask for a copy of the information about you held by us in our records;

ask us to correct any inaccuracies of fact in your information;

request that we restrict your data processing

data portability

Rights related to automated decision making including profiling

make a request to us to delete what personal data of your we hold; and

object to receiving any marketing communications from us.

If you would like to exercise any of your rights above please contact Chris Mochan, 0141 433 2157 gdprinfo@govanhillha.org

You should note that your rights under the GDPR and 2018 Act are not absolute and are subject to qualification.

If you have any complaints about the way your data is processed or handled by us, please contact Chris Mochan, 0141 433 2157 gdprinfo@govanhillha.org

If you remain unsatisfied after your complaint has been processed by us, you also have the right to complain to the Information Commissioner's Office in relation to our use of your information. The Information Commissioner's contact details are noted below:

The Information Commissioner's Office – Scotland

45 Melville Street, Edinburgh, EH3 7HL

Telephone: 0303 123 1115

Email: Scotland@ico.org.uk

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

Appendix 3: Model Data sharing agreement

DATA SHARING AGREEMENT

between

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

and

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

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

WHEREAS

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

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

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

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

NOW THEREFORE IT IS AGREED AS FOLLOWS:

1 DEFINITIONS

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

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

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

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

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

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

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

(a) the Data Protection Act 2018;

(b) the General Data Protection Regulation (EU) 2016/679;

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

(d) 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 separately and individually responsible for compliance with Data Protection Law;

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

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

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

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

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

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

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

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

Transferring Data

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

3 BREACH NOTIFICATION

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

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

3.1.2 the date and time of occurrence;

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

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

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

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

4 DURATION, REVIEW AND AMENDMENT

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

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

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

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

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

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

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

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

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

4.6 Where the Disclosing Party exercises its rights under Clause **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 8.

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.

6.6

7 NOTICES

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

8 GOVERNING LAW

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

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]

SCHEDULE PART 1 – DATA

Drafting Note: This Part should contain details of the Personal Data to be shared between Parties and will need to be populated on a case by case basis when utilising this Agreement.

DATA SUBJECTS

For the purposes of this Agreement, Data Subjects are all living persons about whom information is transferred between the Parties.

SCHEDULE PART 2: PURPOSE AND LEGAL BASIS FOR PROCESSING

Purpose

The Parties are exchanging Data to allow #[insert details].

Legal Basis

#[**insert details - this will require specific requirements to be drafted in to the model Agreement depending on the relationship between the Association and Party 2**]

SCHEDULE PART 3 - DATA TRANSFER RULES

Information exchange can only work properly in practice if it is provided in a format which the Data Recipient it can utilise. It is also important that the Data is disclosed in a manner which ensures that no unauthorised reading, copying, altering or deleting of personal data occurs during electronic transmission or transportation of the Data. The Parties therefore agree that to the extent that data is physically transported, the following media are used:

- Face to face
- Secure email
- Courier
- Encrypted removable media
- #[**insert further methods of transport of Data (and delete above if desired)**]

The data is encrypted, with the following procedure(s):

- #[**insert details**]

SCHEDULE PART 4 – REPRESENTATIVES

Contact Details

Association

Name:	#
Job Title:	#
Address:	#
E-mail:	#
Telephone Number:	#

#[Party 2]

Name:	#
Job Title:	#
Address:	#
E-mail:	#
Telephone Number:	#

SCHEDULE PART 5 – SECURITY MEASURES

1 The Parties shall each implement an organisational information security policy.

2 Physical Security

2.1 Any use of data processing systems by unauthorised persons must be prevented by means of appropriate technical (keyword / password protection) and organisational (user master record) access controls regarding user identification and authentication. Any hacking into the systems by unauthorised persons must be prevented. Specifically, the following technical and organisational measures are in place:

The unauthorised use of IT systems is prevented by:

- User ID
- Password assignment
- Lock screen with password activation
- Each authorised user has a private password known only to themselves
- Regular prompts for password amendments [**Delete/amend as appropriate]**

The following additional measures are taken to ensure the security of any Data:

- Network Username
- Network Password
- Application Username
- Application Password
- Application Permissions and access restricted to those who require it ***(Drafting Note: though this is no longer recommended so individual members may wish to delete)***
  [Delete/ amend as appropriate]

3 Disposal of Assets

3.1 Where information supplied by a Party no longer requires to be retained, any devices containing Personal Data should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

4 Malicious software and viruses

Each Party must ensure that:

4.1.1 PCs used in supporting the service are supplied with anti-virus software and anti-virus and security updates are promptly applied.

4.1.2 All files received by one Party from the other are scanned to ensure that no viruses are passed.

4.1.3 The Parties must notify each other of any virus infections that could affect their systems on Data transfer.

SCHEDULE PART 6 – DATA GOVERNANCE

Data accuracy

The Disclosing Party shall make reasonable efforts to ensure that Data provided to the Data Recipient is accurate, up-to-date and relevant.

In the event that any information, in excess of information reasonably required in order to allow both organisations to comply with their obligations, is shared, the Data Recipient will notify the other party immediately and arrange the secure return of the information and secure destruction of any copies of that information.

Data retention and deletion rules

The Parties shall independently determine what is appropriate in terms of their own requirements for data retention.

Both Parties acknowledge that Data that is no longer required by either organisation will be securely removed from its systems and any printed copies securely destroyed.

Appendix 4: Model Data sharing addendum

[Drafting Note: It is anticipated that specific standard clauses will require to be included within finalised DP Addendums depending on the third party processor and nature of the member's relationship with them, in which case this draft will require to be updated to reflect that]

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 "**Subprocessor**" means any person (including any third party 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 ["of" insert Association staff member details here if appropriate]** 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. **Subprocessing [*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 Subprocessor appointed in accordance with this section 5 to appoint) Subprocessors in accordance with this section 5 and any restrictions in the Principal Agreement.

5.2 The Processor may continue to use those Subprocessors 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 Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. The Processor shall not appoint (nor disclose any Association Personal Data to) the proposed Subprocessor except with the prior written consent of the Association.

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

5.4.1 before the Subprocessor first Processes Association Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor 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 Subprocessor; and on the other hand the Subprocessor, 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 Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Association Personal Data; and

[***Drafting Note: Each member organisation will require to check 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 outwith the UK/EEA***]

5.4.4 provide to the Association for review such copies of the Contracted Processors' agreements with Subprocessors (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 Subprocessor 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 Subprocessor, 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 Subprocessor 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) days' written 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 parties' 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

SCHEDULE

This is the Schedule referred to in the foregoing Data Protection Addendum between the Association and the Processor

Part 1 – Data and Categories of Data Subject
For the purposes of this Data Protection Addendum, the categories of personal or special categories of data being processed are:

Name, Address, Contact Details, Household makeup, language spoken, vulnerabilities or risk factors (including deafness, mental health, physical disability), criminal record, associates **[#amend as necessary]**

The data subjects will be tenants of the Association and members of the tenant's household.

Part 2 – Nature and purpose of the processing
The Processor will processes Association Personal Data when performing housing management and void management tasks in accordance with the Management Agreement. **[#amend as necessary]**

Parties are processing this data for the following reasons:

> the processing is necessary for the performance of the contracts between the Association and its tenants.
> **[#add additional grounds as necessary]**

Part 3 – Duration and subject-matter
The subject matter of this Agreement is the execution and performance of the services specified within the Management Agreement, performed by the Processor as Data Processor. **[#amend as necessary]**

The Agreement will remain in place until terminated or until the **[#insert principal contract details]** is terminated, whichever is earlier. **[#amend as necessary]**

Part 4 – Representatives
The Association has an appointed DPO for data protection matters. This contact must be contacted should the Processor;

(a) receive a Data Subject Access request
(b) identify or become aware of a Personal Data Breach.

The Processor requires to provide contact details below of their Data Protection Officer (if applicable) or appropriate contact person in relation to this addendum.

Contact Details

Association Contact 1 (#**insert DPO details**)

Name: :
Job Title:
Address:
Email:
Telephone:

Association Contact 2
Name: :
Job Title:
Address:
Email:
Telephone:

Processor Contact 1
Name:
Job Title:
Address:
Email:
Telephone:

Processor Contact 1
Name:
Job Title:
Address:
Email:
Telephone:

Appendix 5: Retention schedule

http://www.govanhillha.org/wp-content/uploads/2019/10/Retention-schedule-Oct-2019.pdf