Community Counts
Milnbank
Housing Association
53 Ballindalloch Drive, Glasgow G31 3DQ

GENERAL DATA PROTECTION REGULATIONS POLICY

PH/NOVEMBER 2021/Ref:P14

0141 551 8131 0141 550 2060 admin@milnbank.org.uk www.milnbank.org.uk

1. INTRODUCTION

1.1 GENERAL DATA PROTECTION REGULATIONS (GDPR)

This policy, together with the appended documentation, has been prepared for use as model guidance by the Scottish Federation of Housing Association and the Glasgow West of Scotland Forum in relation to data protection matters for the implementation of the GDPR.

The GDPR came in to force on 25 May 2018. This is a regulation of the European Union and will take direct effect in the UK. The UK left the European Union on 31.01.20 and entered a Brexit transition period. During this period, which runs to end December 2020, the GDPR will continue to apply.

The GDPR overhauls many areas of current data protection laws, and the existing legislation is replaced by the Data Protection Act 2018.

Data Controller – Milnbank Housing Association (MHA), like all organisations processing personal data are required to comply with the terms of the GDPR.

Data Processor – As MHA have a contractual relationship with a number of third parties whom we ask to process personal data on our behalf for various reasons (e.g. external contractor), the GDPR defines those third party processors as "Data Processors". They are also required to comply with the GDPR.

1.2 DOCUMENTATION

The undernoted documents, which are appended to this policy, ensure that MHA is compliant with the terms of GDPR. These are:-

- Appendix 1 - Privacy Policy
- Appendix 2 - Data Retention Guidelines
- Appendix 3 - Fair Processing Notice
- Appendix 4 - Personal Data Map
- Appendix 5 – Employee Fair Processing Notice
- Appendix 6 – Contract of Employment (Data Protection Clause)
- Appendix 7 - Data Protection Addendum (Use MHA data processors)
- Appendix 8 - Data Sharing Agreement (Use other data controllers)

2. PRIVACY POLICY

The Model Privacy Policy at APPENDIX 1 sets out both the policy and procedure MHA implements of the GDPR.

2.1 PROCESSING OF PERSONAL DATA - CONSENT

Under GDPR, consent can no longer be given in a general sense and must be given freely, to a specific purpose of processing and by an affirmative action (i.e. seeking individuals to opt in rather than opt out). In view of this, MHA will review existing consents to ensure that we can process personal data someone has previously consented to us processing.

MHA will consider consent as a basis for processing in general and its use where other grounds for processing that personal data are unavailable. Reference should be made to point 2.2 below. (e.g. where MHA needs to consider consent in relation to the use of images like a photograph from a gala day in any publications or on our website). The resident would be requested to sign a consent form to confirm their agreement to the publication.

2.2 GROUNDS FOR PROCESSING PERSONAL DATA *WITHOUT* OBTAINING CONSENT

There are other grounds for processing personal data and when these are used, MHA does not require to obtain consent. This relates to the following:

- Necessary for performance of a contract between MHA and data subject or entering into a contract (e.g. name, date of birth, contact details);
- Necessary for compliance with a legal obligation (e.g. employment related requirements, such as the need to disclose salary details to HMRC);
- Necessary to protect the vital interests of the data subject or another person (e.g. ASB complaints);
- Necessary for the performance of a task carried out in the public interest or in exercise of an organisation's official authority (for Public Authorities only).

2.3 SECURITY

MHA takes its responsibility to ensure our practices in relation to security of personal data both in paper and electronic format are taken seriously. For full details of our IT security, please refer to MHA's IT & Acceptable Use Policy.

2.4 BREACHES

The GDPR imposes a timeframe for reporting breaches which pose a risk to the rights and freedoms of data subjects (individuals). In accordance with the terms, any breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours of the breach occurring, or from the point MHA becomes aware of that breach if later.

Not all breaches need to be reported to the ICO. This depends on the nature and severity of the breach.

2.5 DATA PROTECTION OFFICER

MHA's Data Protection Officer's role is to ensure data protection compliance by the Association. In terms of the GDPR a Data Protection Officer requires to be appointed by organisations who are deemed to be a public authority in terms of the Freedom of Information (Scotland) Act 2002, or whose core activities involve a large scale monitoring of individuals or the large scale processing of sensitive personal data. MHA was classed as a public authority from 11th November 2019 under the terms of the Freedom of Information (Scotland) Act 2004 (FOISA).

2.6 RIGHTS OF INDIVIDUALS

The GDPR gives enhanced rights to individuals. Clause 9 of the attached Appendix 1 Privacy Policy details those rights. This policy covers the timeframes for responding to subject access requests, as well as the new rights to be forgotten, and to restrict, or object to, processing.
Individuals have the right to view personal data held by MHA about them and this can be exercised under a Subject Access Request in which an individual will request copies/ to review data held about them in relation to specific matters (e.g. ASB complaints made about them).

2.7 DATA RETENTION

APPENDIX 2 of this policy provides Data Retention Guidelines. This information is available online and in hard copy from MHA offices.

3. NOTICE OF PROCESSING OF PERSONAL DATA

3.1 FAIR PROCESSING NOTICE (FPN)

Under the GDPR, MHA will provide documentation which notifies individuals what personal data of theirs is processed by us. This takes the form of a Fair Processing Notice (FPN) is forms APPENDIX 3 of this policy.

The FPN contains the following details:

- Identity and contact details of the Data Controller;
- Data processing purpose;
- Recipients of the data;
- Details of any transfer of the data out with the EU and the protections in place;
- How long the data will be held, or if unknown then how the data controller will determine how long it is to be held;
- Information on whether the data will be processed as part of an automated decision making process and the consequences of such processing;
- Information on the data subject's rights including the consequences of their failure to provide such data where required by statute or contract; and
- Any further information which is not already covered by the above.

MHA will provide a FPN to individuals whose personal data we collect. (e.g. a FPN is included within housing application packs). All new tenants and factored owners will also be provided with a copy of the FPN.

3.1.1 Personal Data

The personal data MHA processes will be clearly narrated within the FPN. The Personal Data Map at APPENDIX 4 is used as an internal audit of personal data we hold. This information is collated and completed on a departmental basis.

3.1.2 Special Categories of Personal Data (Sensitive Personal Data)

MHA will only process personal data that is required. Personal data will be securely stored and access will be restricted. All sensitive personal data will be processed under specific grounds and in accordance with the following:

- Explicit Consent for specific purpose;
- Necessary to comply with obligations re employment or social security;
- Necessary to protect vital interests of the data subject;
- Necessary for the establishment of, exercise or defence of legal claims;
- Necessary for reasons of substantial public interest.

3.2 MARKETING

MHA will seek the consent from individuals for marketing purposes. The consent form will explain the reason we are contacting you (e.g. when we are seeking views about MHA services) and clarification on how you would like MHA to contact you (e.g. by post, email, telephone, text message). Tenants, owners and other service users can change their mind about being contacted in the future by advising MHA.

4. PROCESSING OF EMPLOYEE PERSONAL DATA

Information on MHA employees is also processed in accordance with the terms of the GDPR. The details of which is outlined in MHA's Fair Processing Notice which is issued to all employees and prospective employees to detail what personal data of theirs is processed by the MHA. A copy of the Fair Processing Notice forms an appendix to the Association's contract of employment.

5. DATA SHARING

5.1 DATA SHARING – DATA PROCESSORS

The GDPR imposes a requirement on MHA, as the Data Controller, and Data Processors (e.g. a contractor from the Repairs Framework) to ensure that their contractual relationship with each other is in line with the terms of the GDPR.

MHA reviews the contracts with third party data processors to ensure that they are brought in line with the requirements of the GDPR. This is achieved through the use of an addendum, supplementary to the contract itself, to set out GDPR related matters.

Appendix 5 reflects the exact contractual relationship between MHA and each of our third party processors. The Addendum:

- ensures protection of data subject rights
- provides greater details re the processing itself
- states that personal data may only be processed under documented instruction from the data controller
- confirms the requirements of the processor to notify controller when required to process data due to a legal requirement
- confirms processor staff confidentiality obligations
- confirms arrangements for the processor's deletion or return personal data at the end of the service provision.

5.2 DATA SHARING – DATA CONTROLLERS

There will be situations in which both MHA and another organisation process personal data as Data Controllers, and require to share data for such purposes (e.g. a pension service provider who requires Personal Data to administer the pension service for MHA employees). The Data Sharing Agreement, APPENDIX 6, will be used for this purpose. This Agreement will be entered into with each Data Controller to ensure that each party is complying with the terms of the GDPR in processing personal data.

GDPR - APPENDIX 1

PRIVACY POLICY

1. INTRODUCTION

Milnbank Housing Association (MHA) is committed to ensuring the secure and safe management of data held by the Association in relation to customers, staff and other individuals. MHA'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 accompanying documentation.

MHA 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. MHA manages a significant amount of data, from a variety of sources. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the GDPR).

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

2. LEGISLATION

It is a legal requirement that MHA must collect, handle and store personal information in accordance with the relevant legislation, which is:

(a) the General Data Protection Regulation (EU) 2016/679 ("the GDPR");
(b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
(c) The Data Protection Act 2018 (the 2018 Act)
(d) any legislation that, in respect of the UK, replaces, or enacts into UK 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 UK leaving the European Union.

3. DATA

3.1 MHA 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 MHA is detailed within the Fair Processing Notice, the Data Protection Addendum and, for employees, the Terms of and Conditions of Employment.

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

3.1.2 MHA 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 MHA 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 3);
- Processing is necessary for the performance of a contract between MHA and the data subject or for entering into a contract with the data subject;
- Processing is necessary for MHA'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 MHA's official authority;

4.2 Fair Processing Notice

MHA 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 is provided to the customer from the outset of processing their Personal Data and they will be advised of the terms of the FPN when it is provided to them.

The FPN sets out the Personal Data processed by MHA and the basis for that Processing. This document is provided to all of MHA's customers at the outset of processing their data.

4.3 Employees

Employee Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by MHA. 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. A copy of any employee's Personal Data held by MHA is available upon request by that employee from the Association's Data Protection Officer.

4.4 Consent

Consent as a ground of processing will require to be used from time to time by MHA when processing Personal Data. It should be used by the Association where no other alternative ground for processing is available. In the event that MHA 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 MHA 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**

In the event that MHA 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.

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

MHA 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 MHA 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 MHA 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.

5.1 Data Sharing

a. Personal Data is from time to time shared amongst MHA 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 MHA and the third party will be processing that data in their individual capacities as data controllers.

b. Where MHA 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.

5.2 **Data Processors**

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

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

b. If a data processor wishes to sub-contact their processing, prior written consent of MHA 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.

c. Where MHA 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 MHA.

6. DATA STORAGE and SECURITY

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

6.1 Paper Storage

If Personal Data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. Employees should 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 MHA's storage provisions.

6.2 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 MHA's data processors or those with whom MHA 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

A data breach can occur at any point when handling Personal Data and MHA 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 7.2.

7.1 Internal Reporting

MHA 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);
- MHA 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

7.2 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")

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

The DPO will be responsible for:

- monitoring MHA's compliance with Data Protection laws and this Policy;
- co-operating with and serving as MHA'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 MHA, 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 MHA's processing of their data. These rights are notified to MHA'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**

Data Subjects are permitted to view their Personal Data held by MHA upon making a request to do so (a Subject Access Request). Upon receipt of a request by a Data Subject, MHA 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 MHA 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**

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

Each request received by MHA 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 has the responsibility for accepting or refusing the Data Subject's request in accordance with clause 9.3 and will respond in writing to the request.

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**

A data subject may request that MHA restrict its processing of the data subject's Personal Data, or object to the processing of that data. In the event that any direct marketing is undertaken from time to time by MHA, a data subject has an absolute right to object to processing of this nature by the Association, and if MHA receives a written request to cease processing for this purpose, then it must do so immediately.

Each request received by MHA will be considered on its own merits and legal advice will be obtained in relation to such requests from time to time. The DPO has the responsibility for accepting or refusing the data subject's request and will respond in writing to the request.

9.6 **The Right to Rectification**

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.

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")

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

- 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.

- 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.

- MHA will 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.

11. ARCHIVING, RETENTION AND DESTRUCTION OF DATA

MHA cannot store and retain Personal Data indefinitely. It must ensure that Personal Data is only retained for the period necessary. MHA shall ensure that all Personal Data is archived and destroyed in accordance with the periods specified within Appendix 2 of the GDPR Policy.

GDPR - APPENDIX 2

DATA RETENTION PERIODS GUIDELINES

Data Retention Periods

The table below sets out retention periods for Personal Data held and processed by MHA. This is intended to be used as a guide only. MHA 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	Retention time	Responsible Officer
Committee Members Documents	5 years after cessation of membership	Depute Director
Membership records	5 years after last contact	Corporate Services Manager
Committee Meetings Minutes	Indefinitely	Corporate Services Manager
Minute of factoring meetings	Duration of appointment as property managers	Property Manager
Minutes of residents meetings (eg. Agendas, notice of meetings etc)	2 years (this does not refer to minutes of meetings as these must be permanently retained)	Relevant lead officer
Third Party documents regarding care plans	Duration of Tenancy	Supported Accommodation. Manager
Tenancy files	Duration of Tenancy	Housing Services Manager
Former tenants' files (key info)	5 years	Housing Services Manager
Housing Benefits Notifications	Duration of Tenancy	Housing Services Manager
Anti-Social Behaviour case files	5 years/end of legal action	Housing Services Manager
Lease documents	5 years after lease termination	Housing Services Manager
Documents relation to successful tenders	5 years after end of contract	Asset Manager
Documents relating to unsuccessful form of tender	5 years after notification	Asset Manager
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 contractual claims	Corporate Services Manager

Application forms, interview notes	Minimum 6 months to a year from date of interviews. Successful applicant's documents will be transferred to personal file.	Corporate Services Manager
Documents proving the right to work in the UK	2 years after employment ceases.	Corporate Services Manager
Facts relating to redundancies	6 years if less than 20 redundancies. 12 years if 20 or more redundancies.	Corporate Services Manager
Parental Leave	18 years	Corporate Services Manager
Records relating to working time	2 years from the date they were made	Corporate Services Manager
Health records	During employment and 3 years thereafter if reason for termination of employment is connected to health	Corporate Services Manager
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of the redundancy	Payroll (Finance)
Payroll	3 years after the end of the tax year they relate to	Payroll (Finance)
Income tax, NI returns, correspondence with tax office	At least 3 years after the end of the tax year they relate to	Payroll (Finance)
Pensioners records	12 years after the benefit ceases	Payroll (Finance)
Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence	3 years after the end of the tax year to which they relate	Payroll (Finance)
Retirement benefits schemes – notifiable events, e.g. relating to incapacity	6 years from end of the scheme year in which the event took place	Payroll (Finance) Corporate Services Manager
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years	Payroll (Finance) Corporate Services Manager
Wages/salary records, expenses, bonuses	6 years	Payroll (Finance)

Accident books and records and reports of accidents	3 years after the date of the last entry	Asset Manager
Health and Safety assessments and records of consultations with safety representatives and committee	Permanently	Asset Manager
e-mail retention for current employees	5 years	Only accessible by Compliance Officer or M2

GDPR - APPENDIX 3

FAIR PROCESSING NOTICE

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

WHO ARE WE?

Milnbank Housing Association, a Scottish Charity (Scottish Charity Number SCO39891), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 1818 R(S) and having their Registered Office at 53 Ballindalloch Drive, Dennistoun, Glasgow, G31 3DQ. MHA 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), 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 Z627136X and we are the data controller of any personal data that you provide to us.

Our Data Protection Officer is Pauline Hamilton. Any questions relating to this notice and our privacy practices should be sent to p.hamilton@milnbank.org.uk or telephone 0141-551-8131

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 (ie. the tenancy agreement you are party to):

- when you apply for housing with MHA, become a tenant, request our services, repairs service, enter in to a factoring agreement
- when you apply to become a member;
- from your use of our online services, whether to report any tenancy or 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 under a requirement to provide us with the following information:

- name;
- address;
- telephone number;
- e-mail address;
- National Insurance Number;
- next of Kin;
- dependents details;
- financial information (e.g. bank details, income details)

- ethnic origin (this is classified as "Sensitive Personal Data")
- details re medical conditions/disabilities (this is classified as "Sensitive Personal Data")

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
- Medical information

WHY MHA 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 suppliers 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 YOUR INFORMATION

The information you provide to MHA 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 Local Authority);

- If we are investigating payments made or otherwise, your information may be disclosed to payment processors, Local Authority and the DWP;
- 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
- To the Scottish Housing Regulator with regards to statistical data.

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. For full details, please see our Privacy Policy.

HOW LONG MHA WILL KEEP YOUR INFORMATION
We review our data retention periods regularly and will only hold your personal data for as long as is necessary for the relevant activity, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you.
We will generally keep your information for the minimum periods outlined in Appendix 2 of this policy after which this will be destroyed if it is no longer required for the reasons it was obtained. Our full retention schedule is available at Appendix 2 of the GDPR Policy.

YOUR RIGHTS
You have the right at any time to:
- ask for a copy of the information about you held by MHA 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 yours we hold; and
- object to receiving any marketing communications from us.

If you would like to exercise any of your rights above please contact p.hamilton@milnbank.org.uk or 0141-551-8131. 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 Pauline Hamilton, DPO p.hamilton@milnbank.org.uk

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 MHA - please help us keep our records updated by informing us of any changes to your email address and other contact details.

GDPR - APPENDIX 4

PERSONAL DATA MAP

PERSONAL DATA MAP

Details of information collected or held	Location	Why is the data used?	Period retained for	Which 3rd Parties have access to data	What terms was the data acquired?
Employees personnel records	Individual files in computerised secure HR system Personnel computer records for PAYE, tax, NI contributions, SMP, pensions etc	Details of employment and next of kin etc to meet employment legislation requirements. See Fair Processing Notice for further details.	While in employment & thereafter for 5 years. 3 years for statutory payment items eg. SMP, PAYE and employee disciplinary and grievances. These records may be kept for up to 6years if required 6 years for redundancy records 12 years for pension information & Employee Liability Insurance	Details supplied for references, Inland Revenue, Pension Scheme, DWP, Dept of Employment, Auditors, SHR, Employment law & Counselling Service	Consent from individual employees.

			3 years for sickness records		
Employees Staff Appraisals and training and development records	Computerised secure HR system	To record employee personal learning and development	While in employment & thereafter for 5 years	Details supplied for reference, Management Committee and SHR	
Health & Safety Information	Files in locked cabinet & computerised system Reference Manuals in box file in policy store	To record health and safety incidents and keep staff informed	3 years (Accident Book, records & reports) 40 years for Asbestos and records relating to the Control of Substances Hazardous to Health Regulations Indefinite for other information	Details supplied for reference, Health & Safety Advisors or representatives	
Recruitment details for job vacancies (application forms and ethnic monitoring details)	Computerised secure HR files	To provide monitoring details for Equal Opportunities Policy. In case of recruitment enquiry.	Retained on secure HR computer system for a minimum 6 months to 1 year from date of interviews. Successful applicants documents will be transferred to personal file.	Used for monitoring for Management Committee, Auditors and SHR, Industrial Tribunals. Meet requirements of Equality Act 2010	
Tenancy files	Stored in data management system	Details of tenancy relationship with MHA (e.g.	Duration of tenancy and thereafter for 5 years	Details used for auditors, housing benefit claims	

		occupants of house, rent charge, family composition etc)			
Former residents personal files	Stored in data management system	Key details relating to tenancy and management arrangements	5 years	Details supplied for references, Auditors, SHR and Solicitors	Information is obtained from start and throughout tenancy
Anti-Social complaints records Anti-social case files	Recorded in data management system complaints module	To record reports of alleged anti-social behaviour and record action taken by Association	While resident remains within the system 5 years/end of legal action	Information used for SHR, Solicitors and Management Committee	Information is obtained as residents make complaints
Telephone contacts, addresses and e-mail addresses of suppliers, contractors and other contacts	Computerised system	To be able to contact people	5 years after end of contract	Relevant person who requests information	
Owners Factoring Details	Retained on Data Management System	To record factoring payment and arrears. To produce monthly reports	While resident and thereafter for 5 years.	Details used for SHR, Auditors, Solicitors and Management Committee	
Committee members names, addresses, date of birth and code of conduct details	Electronically file in a restricted access governance file	Regulatory requirement	Whilst a committee member and thereafter for 5 years.	Used for business planning, auditors and SHR	
Membership Details	Computer database with restricted access	Statutory obligation	Whilst a committee member and	Auditors, SHR, Management Committee and	

			thereafter for 5 years.	publicly available document	

Association Annual Accounts	Filed on PC with restricted access.	Statutory obligation	7 years	References, Auditors, SHR, borrowing facilities (lenders), recognised stakeholders, Big Lottery, GCC, OSCR, Pensions Trust, FCA	
Contractors Invoices	Stored in lever arch files in locked cabinets for 1 year then scanned	For auditing purposes	3 years	Auditors and SHR	
Debtors invoices	Stored in lever arch files in locked cabinets for 1 year then scanned	For auditing purposes	3 years	Auditors and SHR	
Suspended/cancelled housing list application forms	Scanned into MHA data management system	Details of applications applying to be rehoused by tenants	3 years review carried out on annual basis, but information of applicants who do not return forms are retained, at the moment indefinitely as a result of applications being scanned and held within the system. We may need to look at deleting	Auditors, SHR and Management Committee	Information is requested on housing application form

			them in the future if there is ever any 'data overload'		
Ethnic monitoring of housing list applications	Included within housing applications and noted on data management system	To provide statistics for Equal Opportunities Policy and ARC	3 years review carried out on annual basis, but information of applicants who do not return forms are retained, at the moment indefinitely as a result of applications being scanned and held within the system. We may need to look at deleting them in the future if there is ever any 'data overload'	Auditors and SHR	Information is requested on housing application form
Tenant rent details	In Data Management System on each individual tenant account.	To record rent payments, arrears and housing benefit arrangements. To produce monthly reports	For duration of tenancy and thereafter for 5 years	Details used for SHR, Auditors, housing benefit, Solicitors and Management Committee	Information is obtained on a monthly basis as rent charges and payments go through the individual accounts
Maintenance job repair lines	In data management system	Details of individual repairs carried out in properties. To produce monthly reports	3 years	Details used for Management Committee, SHR and Auditors	

Benefit to staff and committee members under Housing (Scotland) Act 2010	Payments and Benefits Register in locked cabinet with restricted access	Statutory requirements	Indefinitely	Publicly available record, Auditors and SHR	
Complaints to MHA, the Care Inspectorate or any other relevant agency in relation to all our services	Computerised Complaints Register with restricted access	Statutory obligation	Indefinitely	Ombudsman, Management Committee, SHR, Auditors and Staff. Social Work Services, Police, Court Officials, Nursery Child Protection Co-ordinator and Inspectors	
Owners and tenants direct debit mandates showing bank details	Retained on data management system	To record rent, factoring and recharge payments	While resident	Details used for SHR, Auditors, solicitors and Management Committee	
Potential new customer contact details	Secured computerised file with restricted access	To allow contact throughout the process of taking over as property managers	While potential customers and thereafter for the duration of MPS as property managers	Details used for Board Meetings	
S/A – Current Tenants files	Folders in locked cupboards	Access to their folders To give Care Inspectorate access to current tenant	Retained for duration of tenancy.	Archived and stored in locked filing cabinet and destroyed after 3 years	

		files when carrying out an inspection			
SA – ex-tenants files	Stored in sealed files in locked filing cabinet	Held to enable Care Inspectorate to have access to ex tenants files. Senior staff may require access to ex tenants files if asked to attend court etc	Retained for 3 years	Archived in locked filing cabinet and destroyed after 3 years using confidential document disposal company	

SA – referrals for support services	Stored in lever arch folder in locked cupboard	To enable senior staff to access to arrange information visits for prospective tenants	Retained for 6 months	If referral leads to placement at project referrals are transferred to tenant's individual file. If referral is cancelled it is transferred to cancelled and suspended referral folder.	
SA – Cancelled and suspended referrals to support services	Stored in lever arch folder in locked cupboard	To enable senior team to access folder for information or if a tenant is re-referred to look at previous referral to ascertain if there has been any significant issues since last referral was submitted	Retained for 6 months	After 6 months all cancelled and suspended referrals are destroyed using confidential document disposal company	

CFN – Child Protection chronologies and files	Child Protection Folder in locked filing cabinet in Manager's office	To ensure accurate records are maintained to monitor children and ensure that they are protected from harm	While child still attends service and for 3 years after they leave	Social Work Services, Police, Court Officials, Nursery Child Protection Co-ordinator and Inspectors	
CFN – Children's Files containing contact details, medical needs, address and family details	In Children's suspension files in locked cabinet in managers office	To ensure each child's neds are recorded and met. To ensure families can be contacted in emergency	While child attends Service and thereafter scanned to secure hard drive for 5 years after they leave	Staff at CFN, Inspectors	

GDPR - APPENDIX 5 EMPLOYEE FAIR PROCESSING NOTICE

EMPLOYEE FAIR PROCESSING NOTICE

(How we use employee information)

This notice explains what information MHA collect, when we collect it and how we use this. During the course of our activities MHA 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 MHA will handle your information.

1. MHA is committed to a policy of protecting the rights of individuals with respect to the processing of their personal data and adhere to guidelines published in the Data Protection Act of 2018 (The 2018 Act) and the General Data Protection Regulation (EU) 2016/679 (GDPR), together with any domestic laws subsequently enacted. MHA collect and use personal data for a variety of reasons.

   We are registered as a Data Controller with the Office of the Information Commissioner (ICO) under registration number Z627136X and we are the data controller of any personal data that you provide to MHA.

   MHA Data Protection is controlled by the Data Protection Officer, Pauline Hamilton. Any questions relating to this notice and our privacy practices should be sent to Pauline Hamilton at p.hamilton@milnbank.org.uk or 0141-551-8131.

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

   (a) Name
   (b) Date of Birth
   (c) Address
   (d) Telephone Number
   (e) E-mail address
   (f) NI number
   (g) Personal characteristics such as gender, disability, working pattern & ethnic group
   (h) Qualifications
   (i) Absence information
   (j) Personal identification (Driving licence, passport, birth certificate, proof of current address, eligibility for working in the UK)
   (k) Next of Kin for emergency contacts
   (l) GP medical requests
   (m) Bank account details

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

   a. Administration of contracts of employment
   b. Payment of salaries
   c. Recruitment and selection
   d. Pensions and associated benefits, appraisal, training and development
   e. Membership of professional bodies

f. PVG check & SSSC registration
g. SHR Annual Return

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

- To process your monthly salary payments;
- To allow your pension provider to process pensions information and handle your pension;
- For the external auditor as part of the annual audit;
- Employment law advice services;
- DWP, Office for National Statistics & employee support/assistance services in respect of employee queries;
- To allow your electronic payslips to be produced and issued to you;
- If we enter into a joint venture with or is sold to or merged with another business entity, your information may be disclosed to our new business partners or owners.

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

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

- There is only one personnel file per employee
- The personnel files are password protected
- Access is restricted to the HR function
- Your personal data will be shared with relevant person(s) only for the purposes of business related activity

6. MHA review our data retention periods regularly (no less than once per year) and will only hold your personal data for as long as is necessary for the relevant activity, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you.

   Data retention guidelines on the information we hold is provided in the Personal Data Map within the GDPR Policy.

7. 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 delete what personal data of yours we hold; and
- Object to receiving any marketing communications from us.

   These rights are qualified and are not absolute.

8. If you would like to find out more about how MHA use your personal data or want to see a copy of information about you that we hold or wish to exercise any of your above rights, please contact: Pauline Hamilton, Data Protection Officer.

   If you have any complaints about the way your data is processed or handled by us, please contact Pauline Hamilton, DPO
   p.hamilton@milnbank.org.uk

   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 MHA – please help us keep our records updated by informing us of any changes to your personal and contact details.

GDPR - APPENDIX 6

CONTRACT OF EMPLOYMENT (DATA PROTECTION CLAUSE)

EMPLOYMENT CONTRACT – DATA PROTECTION WORDING

We hold information about you on your personal file. You are entitled to access this file and to other information that we hold about you, subject to certain restrictions imposed by the GDPR and 2018 Act. The Fair Processing Notice annexed to this Contract (a duplicate copy of which we have provided to you) confirms what personal information we hold which we have obtained from you or third parties. Our Privacy Policy contains further details regarding Data Protection matters, and the handling of personal data. By signing this Contract you confirm that you have read and understood our Privacy Policy and will comply with the terms of that Policy.

We may also require to process sensitive personal data of yours. Any sensitive personal data we process to comply with our obligations as your employer and/or your vital interests is outlined within the Fair Processing Notice annexed hereto. We will seek to obtain your consent to process any additional sensitive personal data of yours that we wish to process if appropriate.

GDPR - APPENDIX 7

DATA PROTECTION ADDENDUM

DATA PROTECTION ADDENDUM

Between

Milnbank Housing Association, a Scottish Charity (SCO39891), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 1818 R(S) and having their Registered Office at 53 Ballindalloch Drive, Dennistoun, Glasgow, G31 3DQ

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

(a) MHA and the Processor have entered in to an agreement/contract to [insert detail] (hereinafter the "Principal Agreement"/"Principal Contract");

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

(c) 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 Subprocessor;

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 MHA pursuant to the Principal Agreement/ Contract;

1.1.10 "**Subprocessor**" 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 MHA 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 MHA Personal Data

2.1 The Processor shall:

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

2.1.2 not Process MHA 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 MHA 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 Subprocessor) to:

2.2.1.1 Process Association Personal Data; and

2.2.1.2 in particular, transfer MHA 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 MHA Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). MHA 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. <u>Processor and Personnel</u>

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 MHA Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or who access the relevant MHA 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. <u>Security</u>

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 MHA Personal Data implement appropriate technical and organisational 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. **<u>Subprocessing</u> [*Note: This clause should be adjusted depending on the arrangements between Parties*]**

5.1 MHA 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 MHA 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 MHA 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 MHA 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 MHA 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 MHA 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 MHA Personal Data; and

5.4.4 provide to MHA 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 MHA Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of the Processor.

6. Data Subject Rights

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

The Processor shall:

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

6.1.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of MHA 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 MHA of that legal requirement before the Contracted Processor responds to the request.

7. **Personal Data Breach**

The Processor shall notify MHA without undue delay upon the Processor or any Subprocessor becoming aware of a Personal Data Breach affecting MHA 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.

The Processor shall co-operate with MHA 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 MHA with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which MHA 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 MHA Personal Data

9.1.1 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 MHA Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

9.1.2 Subject to section 9.3, MHA 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 MHA Personal Data 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 MHA Personal Data Processed by any Contracted Processor. The Processor shall comply with any such written request within seven (7) days of the Cessation Date.

9.1.3 Each Contracted Processor may retain MHA 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.

9.1.4 Processor shall provide written certification to MHA 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 to MHA on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by MHA or an auditor mandated by the Association in relation to the Processing of MHA Personal Data by the Contracted Processors.

10.2 Information and audit rights of MHA 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, MHA 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.

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 MHA 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:

a) First name
b) Surname
c) Address
d) Postcode
e) Phone number

Part 2 – Nature and purpose of the processing

The parties are processing this data for the purposes of ..... (**e.g. to allow maintenance repairs to the property where the tenant has a tenancy with Milnbank Housing Association).**

It is necessary to process this data for the performance with the data subject.

Part 3 – Representative

Milnbank Housing Association has nominated contacts as narrated below, and those individuals should be contacted as appropriate in relation to any matter relating to this Addendum.

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

The Processers contact details are:

GDPR - APPENDIX 8

DATA SHARING AGREEMENT

DATA SHARING AGREEMENT

Between

Milnbank Housing Association, a Scottish Charity (SCO39891), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 1818 R(S) and having their Registered Office at 53 Ballindalloch Drive, Dennistoun, Glasgow, G31 3DQ

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 X** " each a "Party" together the "**Parties**")

WHEREAS
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) MHA 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

(e) 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.

(f) 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:

- the Data Protection Act 1998;
- the General Data Protection Regulation (EU) 2016/679;

- the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
- any legislation that, in respect of the UK replaces, or enacts into UK domestic law, the GDPR (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 UK leaving the European Union;

"Data Recipient" means the party (being either MHA 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 MHA on 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 GDPR (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 GDPR (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 UK except to the extent agreed by the Disclosing Party;

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

(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 UK 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 £x (STERLING) in the aggregate for the duration of this Agreement.

5.3 Subject to Clauses :

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

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

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

SCHEDULE PART 1 – DATA

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.

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].

[**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
- Telephone
- Paper?

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

- Emails are automatically secured by SSL

SCHEDULE PART 4 – REPRESENTATIVES

Contact Details

Association

Name:	Pauline Hamilton
Job Title:	Data Protection Officer
Address:	53 Ballindalloch Drive, Glasgow, G31 3DQ
E-mail:	p.hamilton@milnbank.org.uk
Tel. Number:	0141 551 8131

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 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

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

3 Disposal of Assets

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.