Melville Housing Association Ltd

PRIVACY POLICY

(DPR 001)

Issued May 2018

Contents

1. Introduction

The Melville Housing Association Ltd (hereinafter the "Association") is committed to ensuring the secure and safe management of data held by the Association in relation to customers, staff and other individuals.

The Association's staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures outlined.

We recognise that we have a responsibility to conduct our business in as open and accountable manner as possible.

At the same time, we recognise that we have a duty to ensure that personal and other sensitive information is kept confidential, and in particular that we comply with the Data Protection Act 1998 (as will be amended by the UK Data Protection Bill) and the General Data Protection Regulation (EU) 2016/679 which is applicable from 25 May 2018 (the GDPR) together with any domestic laws subsequently enacted. Our duty relates to our dealing with:

- Applicants, tenants, factored owners and other customers;
- Our staff, members, Board Members and other members of the public;
- All the local and national agencies and authorities which we currently deal with; and
- All commercial contacts.

This policy describes how we will seek to ensure openness and accountability in our activities, while maintaining the confidentiality of personal and sensitive details, including commercially confidential information.

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

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

The Appendices detail the Association's related data protection policies and key documents.

2. Legislation

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

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

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

(b) The Data Protection Act 1998 (as may be amended by the proposed UK Data Protection Bill);

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

(d) any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union

3. Data

3.1 The Association holds a variety of Data relating to individuals, including customers and employees (also referred to as data subjects) which is known as Personal Data. The Personal Data held and processed by the Association is detailed within the Fair Processing Notices at ***Appendix 2*** hereto and the Data Protection Addendum of the Terms and Conditions of Employment which has been provided to all employees.

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

3.1.2 The Association also holds Personal data that is sensitive in nature (i.e. relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, trade union membership,

genetics, biometrics (Used for ID purposes), relates to health or sex life of sexual orientation). This is "Special Category Personal Data" or "Sensitive Personal Data".

4. Processing of Personal Data

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

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

4.2 Fair Processing Notice

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

4.2.2 The Fair Processing Notices at ***Appendix 2*** sets out the Personal Data processed by the Association and the basis for that Processing. These documents are provided to all individuals for whom the Association processes Personal Data customers at the outset of processing their data.

4.3 Employees

4.3.1 Employee Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by the Association. Details of the data held and processing of that data is contained within the Employee Fair Processing Notice which is provided to all job applicants and to Employees at the same time as their Contract of Employment.

4.4 **Consent**

Consent as a lawful basis for processing will require to be used from time to time by the Association when processing Personal Data. It should be used by the Association where no other alternative lawful basis for processing is available, where it is not being requested as a precondition for accessing services and there is no imbalance of power between the Association and the individual. In the event that the Association requires consent to process a data subject's Personal Data, we shall obtain that consent in writing.

4.5 **Processing of Special Category Personal Data or Sensitive Personal Data**

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

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

5. Data Sharing

5.1 The Association shares its data with various third parties for numerous reasons in order that its day to day activities are carried out. In order that the Association can monitor compliance by these third parties with Data Protection laws, the Association will require the third party organisations to enter into a Data Sharing Agreement with the Association.

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

5.1.2 Where the Association shares in the processing of personal data with a third party organisation (e.g. for processing of the employees' pension), it shall require the third party organisation to enter in to a Data Sharing Agreement with the Association.

5.2 Data Processors

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

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

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

5.2.4 Where the Association contracts with a third party to process personal data held by the Association, it shall require the third party to enter in to a Data Protection Addendum with the Association.

6. Data Storage and Security

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

6.1 Paper Storage

If Personal Data is stored on paper it will be kept in a secure place where unauthorised personnel cannot access it. When the Personal Data is no longer required it must be disposed of according to our Retention and Disposal policy. If the Personal Data requires to be retained on a physical file then the Association will ensure it is appropriately secured.

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 the Association's data processors or those with whom the Association has entered in to a Data Sharing Agreement. If Personal Data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be stored securely at all times when not being used. Personal Data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

7. Breaches

7.1 In the unlikely event of a data breach, the Association has reporting duties. Breaches which pose a risk to the rights and freedoms of the individuals (who are the subject of the breach) will be reported externally in accordance with paragraph 7.3 below.

7.2 Internal Reporting

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

- As soon as the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the Data Protection Officer ("DPO", please see paragraph 8 below) must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
- The Association must seek to contain the breach by whatever means available;
- The DPO must consider whether the breach is one which requires to be reported to the ICO and data subjects affected and do so in accordance with paragraph 7.3 below;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements.

7.3 Reporting to the ICO and Data Subjects

The DPO will report any breaches which pose a risk to the rights and freedoms of the individual(s) who has been the 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 the individual(s) affected by the breach.

8. Data Protection Officer ("DPO")

8.1. A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by the Association with

Data Protection laws. The Association's DPO is Harper Macleod LLP, email DPO@Melville.org.uk.

8.2 The DPO will be responsible for:

8.2.1 Monitoring the Association's compliance with Data Protection laws and this Policy;
8.2.2 Co-operating with and serving as the Association's contact for discussions with the ICO; and
8.2.3 Reporting breaches or suspected breaches to the ICO and data subjects in accordance with paragraph 7 above.

9. Data Subject Rights

9.1 Certain rights are provided to data subjects under the GDPR. Individuals are entitled to view the Personal Data held about them by the Association, whether in written or electronic form. The Association has one month to respond to requests from data subjects exercising their rights.

9.2 Individuals have a right to request a restriction of processing their data, a right to be forgotten and a right to object to the Association's processing of their data. These rights are detailed within the Association's Fair Processing Notices.

9.3 **Subject Access Requests**

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

The Association:

9.3.1 Must provide the data subject with an electronic or hard copy of the Personal Data requested, unless any exemption to the provision of that data applies in law;

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

9.3.3 Where the Association does not hold the Personal Data sought by the data subject, must confirm that it does not hold any Personal Data sought to the data subject as soon as possible, and in any

event, not later than one month from the date on which the request was made.

9.4 **The Right to be Forgotten**

9.4.1 An individual can exercise their right to "be forgotten" by submitting a request in writing to the Association seeking that the Association delete all the individual's Personal Data.

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

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

9.5.1 An individual may request that the Association restrict its processing of Personal Data, or object to the processing of that data.

9.5.2 In the event that any direct marketing is undertaken from time to time by the Association, an individual has an absolute right to object to this marketing and if the Association receives a written request to cease direct marketing, then it must do so immediately.

9.5.3 Each request received by the Association will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests.

10. Data Protection Privacy Impact Assessments ("DPIAs")

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

10.2 The Association shall:

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

- In carrying out a DPIA, 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 we will take to reduce those risks, and details of any security measures that require to be taken to protect the Personal Data

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

11. Archiving, Retention and Destruction of Data

11.1 The Association cannot store and retain Personal Data indefinitely. It must ensure that Personal data is only retained for the period necessary. The Association shall ensure that all Personal Data is archived and destroyed in accordance with the periods specified in the table below.

11.2 **Retention of Data**

The Association reviews 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 (the Association may be legally required to hold some types of information), or as set out in any relevant contract we have with a data subject.

The Association will generally keep data for the following minimum periods set out in the table below, after which this will be destroyed if it is no longer required for the reasons it was obtained.

Type of record	Retention Time
Membership records	5 years after last contact
Personal files including training records and notes of disciplinary and grievance hearings	5 years to cover the time limit for bringing any civil legal action, including national minimum wage claims and contractual claims
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of the redundancy
Application forms, interview notes	Minimum 6 months to a year from date of interviews. Successful applicant's documents should be transferred to personal file.
Documents proving the right to	6 years after employment

work in the UK	ceases.
Facts relating to redundancies	6 years if less than 20 redundancies. 12 years if 20 or more redundancies.
Payroll	3 years after the end of the tax year they relate to
Income tax, NI returns, correspondence with tax office	At least 3 years after the end of the tax year they relate to
Retirement benefits schemes – notifiable events, e.g. relating to incapacity	6 years from end of the scheme year in which the event took place
Pensioners records	12 years after the benefit ceases
Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence	3 years after the end of the tax year to which they relate
Parental Leave	18 years
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years
Wages/salary records, expenses, bonuses	6 years
Records relating to working time	2 years from the date they were made
Accident books and records and reports of accidents	3 years after the date of the last entry
Health and Safety assessments and records of consultations with safety representatives and committee	Permanently
Health records	During employment and 3 years thereafter if reason for termination of employment is connected to health
Board Members Documents	5 years after cessation of membership
Documents relation to successful tenders	5 years after end of contract
Documents relating to unsuccessful form of tender	5 years after notification
Applicants for accommodation	5 years
Housing Benefits Notifications	Duration of Tenancy
Tenancy files	Duration of Tenancy
Former tenants' files (key info)	5 years
Third Party documents re care plans	Duration of Tenancy
Records re offenders. Ex-	Duration of Tenancy

offenders (sex offender register)	
Lease documents	5 years after lease termination
ASB case files	5 years/end of legal action
Board meetings/residents' meetings	1 year
Minute of factoring meetings	Duration of appointment

12. Training

12.1 All staff will receive the necessary training in the operation of Data Protection and the GDPR as it relates to their specific duties, and in the maintenance of the confidentiality and security of the manual and computer information that we hold.

12.2 The main training will be carried out as part of the induction process for all new staff. Refresher training will be given at regular intervals as required, as part of our staff training and development programme.

13. Implementation and Review

13.1 The Chief Executive is responsible for ensuring that this policy is implemented as required by the Board.

13.2 The Chief Executive will ensure that this policy is reviewed by the Board at least every three years.

14. Equality Act

14.1 We will ensure that by implementing this policy, we will continue to comply with equalities legislation.

List of Appendices

Related Policies – available in INVU

- Code of Conduct for Governing Body Members (GOV 003) –
- Code of Conduct for Staff (EMP 003)

Appendix 1 -

- Model Data Sharing Agreement
- Model Data Processor Addendum

Appendix 2 – Fair Processing Notices

- Customers
- Employees