# ST MATTHEWS H.A PRIVACY POLICY

## Contents

## 1. Introduction

St Matthews Housing Association (hereinafter the "Association" or "SMHA") is committed to ensuring the secure and safe management of data held by the Association in relation to tenants, staff and other individuals. The Association's staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures outlined in this policy and documentation referred to herein.

The Association needs to gather and use certain information about individuals. These can include 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.

## 2. Legislation

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

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

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

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

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

## 3. Data

3.1 The Association holds a variety of Data relating to individuals, including tenants 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 Association's Fair Processing Notice (Policy Ref: COR-06.2) hereto and the Association's Data Protection Addendum Policy (Policy Ref: COR-06.6) and the Terms of and Conditions of Employment which has been provided to all employees.

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

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

## 4. Processing of Personal Data

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

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

**4.2 Fair Processing Notice**

4.2.1 The Association has produced a Fair Processing Notice (FPN) – (Policy Ref: COR-06.2), which it is required to provide to all tenants whose Personal data is held by the Association. That FPN must be provided to the tenant from the outset of processing their Personal Data and they should be advised of the terms of the FPN when it is provided to them.

4.2.2 The Fair Processing Notice sets out the Personal Data processed by the Association and the basis for that Processing. This document will be provided to all of the Association's tenants 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 Association's Employee Fair Processing Notice (Policy Ref: COR-06.4), which is provided to Employees at the same time as their Contract of Employment.

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

### 4.4 Consent

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

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

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

- The data subject has given explicit consent to the processing of this data for a specified purpose;

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

## 5. Data Sharing

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

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

### 5.2 Data Sharing

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

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

accordance with the terms of the Data Sharing Agreement set out in SMHA Data Sharing Agreement (Policy Ref: COR-06.7).

### 5.3 Data Processors

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

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

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

5.3.3 Where the Association contracts with a third party to process personal data held by the Association, it shall require the third party to enter in to a Data Protection Addendum with the Association in accordance with the terms of the Association's Data Protection Addendum (Policy Ref: COR-06.6).

## 6. Data Storage and Security

All Personal Data held by the Association will 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. Employees must make sure that no Personal Data is left where unauthorised personnel can access it. When the Personal Data is no longer required it must be

disposed of by the employee so as to ensure its destruction. If the Personal Data requires to be retained on a physical file then the employee should ensure that it is affixed to the file which is then stored in accordance with the Association's storage provisions.

6.2 **Electronic Storage**

Personal Data stored electronically will also be protected from unauthorised use and access. Personal Data will 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 must be stored on designated drivers and servers.

## 7. Breaches

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

**7.2 Internal Reporting**

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

- As soon as the breach or any potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the Association's C.E.O 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 Association's C.E.O 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 clause 7;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

**7.3 Reporting to the ICO**

The Association's C.E.O is required 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 C.E.O must also consider whether it is appropriate to notify those data subjects affected by the breach.

## 8. Data Protection Officer ("DPO")

8.1. A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by the Association with Data Protection laws. The Association does not intend to directly appoint a Data Protection Officer and all responsibilities under GDPR are apportioned to the Association C.E.O, whose details are contained within the Association's Fair Processing Notice (Policy Ref: COR-06.2).

8.2 The Association's C.E.O will be responsible for:

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

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

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

## 9. Data Subject Rights

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

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

9.3 **Subject Access Requests**

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

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

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

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

9.4 **The Right to be Forgotten**

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

9.4.2 Each request received by the Association will require to be considered on its own merits and legal advice will be obtained in relation to such requests from time to time. The C.E.O will have responsibility for accepting or refusing the data subject's request and will directly respond in writing to any request made.

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

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

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

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

## 10. Privacy Impact Assessments ("PIAs")

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

10.2 The Association shall:

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

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

10.3 The Association is required to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The Association's C.E.O 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 ICO within five (5) working days.

## 11. Archiving, Retention and Destruction of Data

The Association cannot store and retain Personal Data indefinitely. It will ensure that Personal data is only retained for the period necessary. The Association shall ensure that all Personal data is archived and destroyed in accordance with the periods specified within the Association's Data Retention Periods (Appendix 1) hereto.

## Related Policies

- SMHA Data Protection and GDPR Policy (Policy ref: COR-06)
- SMHA Fair Processing Notice (Policy ref: COR-06.2)
- SMHA Personal Data Map (Policy ref: COR-06.3)
- SMHA Employee Fair Processing Notice (Policy ref: COR-06.4)
- SMHA Contract of Employment Data Protection Clause (Policy ref: COR-06.5)
- SMHA Data Protection Addendum (Policy ref: COR-06.6)
- SMHA Data Sharing Agreement (Policy ref: COR-06.7)

**Appendix 1**

| Information | Retention Period | Justification | Responsibility |
|---|---|---|---|
| **Finance** | | | |
| Bank Accounts and auditable financial data | 6 years end of accounting period or disposal of asset | Statutory/SMHA recommendation | Finance Officer/CEx |
| Payroll, Tax and Expenses | As above | As above | |
| Pension information | Permanent | | |
| **Capital Assets** | | | |
| Budget/Expenditure | 6 years | SMHA recommendation | Finance Officer/Maintenance Officer/CEx |
| Fixed Asset Register | Permanent | As above | |
| Asset Surveys | Permanent | As above | |
| RTB Purchases | 12 years after completion | As above | |
| Omniledger repairs information | Permanent | Good Practice | |
| Plans/Drawings | Permanent | | |
| Asbestos Surveys | Permanent | Good Practice | |
| Property maintenance programmes details | Permanent | Good Practice<br>Good Practice | |
| **Health & Safety** | | | |
| Gas Safety Certificate | Minimum 3 years | Gas Safety Regs. | Maintenance Officer/CEx |
| Electrical Work Certificates | 10 years | Legal | |
| Building Regulation Certs | Permanent | Legal | |
| Adaptation recommendations/reports | Permanent | Good Practice | |
| Fire Safety/Testing | 5 years | Legal | |
| Legionella Checks | | Legionnaire's COP | |
| **Governance** | | | |
| Board Papers/Minutes | Permanent | Legal | CEx |
| Board Directors records | 6 years | Legal | |
| Financial Statements | 6 years | Legal | |
| Board training records | 6 years | Good Practice | |
| Use of Seal/DoI Registers | Permanent | Legal | |
| Internal Audit Reports | Minimum 5 years | Good Practice<br>Good Practice | |
| | Minimum 5 | Good Practice | |

| | | | |
|---|---|---|---|
| External Audit Reports<br>Strategy Plans/Business Plans<br>Business Continuity Plan<br>Complaints<br>Surveys<br>Risk Plan/Register | years<br>Until superseded<br><br>Until superseded<br>Permanent<br>Until superseded<br>Until superseded | Good Practice<br>SMHA recommendation<br>SMHA recommendation<br>SMHA Recommendation | |
| **Insurance**<br><br>Claims Information<br>Policy Information<br>Employers Liability Insurance | 6 years<br>Permanent<br>40 years | SMHA recommendation<br>Legal<br>Legal | CEx |
| **Tenancy Records**<br><br>Application/Allocation files<br>Omnilgder tenant information<br>House File Information<br>Former tenant housefiles | 6 years<br>Permanent<br>Permanent<br>Permanent | SMHA recommendation<br>Good Practice<br>Good Practice<br>Good Practice | Housing Officer/CEx |
| **Rents/Arrears**<br><br>Omniledger rent account information<br>Arrears correspondence<br>Legal/court papers arrears<br>HB information | Permanent<br><br>Permanent<br>Permanent<br>Permanent | Good Practice<br><br>Good Practice<br>Good Practice<br>Good Practice | Finance Officer/Housing Officer/CEx |
| **ASB**<br><br>Case material<br>ASB Complaints log | Permanent<br>Permanent | Good Practice<br>Good Practice | Housing Officer/CEx |
| **Human Resources**<br><br>Employees Records<br>Recruitment and Selection records<br>Staff Training Plan/records | Minimum 6 years<br>Minimum 6 years | SMHA recommendation<br>SMHA recommendation | CEx |

| | | | |
|---|---|---|---|
| Disciplinary Information<br>Grievance Information<br>All Leave Records<br>Redundancy Records<br>Appraisal Records<br>Trade Union Dealings | Minimum 6 years<br>Minimum 6 years Minimum 6 years<br>Minimum 6 years Minimum 6 years<br>Minimum 6 years<br>10 years | SMHA recommendation<br>SMHA recommendation<br>SMHA recommendation<br>SMHA recommendation<br>SMHA recommendation<br>SMHA recommendation<br>Good Practice | |