Data Protection Policy - Draft

Old Etonian Housing Association Limited

1 Summary

1.1 As a landlord and employer, Old Etonian Housing Association ("**the Association**") holds personal information on a variety of people ("**Data Subjects**"), which includes prospective, current and former tenants and leaseholders, current and former loan-holders, current and former employees, job applicants, Board members, suppliers and contractors.

1.2 The Association needs to process information about various individuals in order for it to adequately carry out its day to day business in the provision of social housing accommodation and associated services, to provide an effective and efficient service, fulfil its responsibilities as an employer and to meet its legal and regulatory obligations. The responsibilities for ensuring compliance is delegated by the Management Committee to its managing agents Teachers' Housing Association.

1.3 The Association however acknowledges that all individuals have a right to privacy and that all Personal Data in its possession must be handled in a secure and lawful fashion.

1.4 The General Data Protection Regulations **("GDPR" or "the Regulations")** set legislative requirements for organisations processing personal information ("**Data Controllers**").

1.5 This Policy aims to protect and promote the rights of Data Subjects and the Association and should be read in conjunction with the managing agent's

- Data Protection Procedures,
- Document Retention Policy,
- Confidentiality Policy,
- Mobile Phone Policy,
- Information Security Policy,
- Email and Internet Use Policy, and
- Data Protection Statement.

1.6 The Association is registered with the Information Commissioner as a Data Controller (registration number ZA018115) and ensures that its handling of personal information is of a high standard and that it complies with the requirements of GDPR.

2 Purpose and Scope

2.1 The Association must process Personal Data fairly and lawfully and in accordance with individuals' rights.

2.2 **Processing** relates to collecting, editing and updating, retaining and storing, disclosing or sharing, deleting / erasing and destroying, viewing (including images and video footage), archiving, and listening to Personal Data.

2.3 **Personal Data** relates to any information relating to an identified or identifiable natural person. This includes any expression of opinion about the individual.

2.4 The information may be stored electronically, i.e. on a computer, including word processing documents, e-mails, computer records, CCTV images, microfilmed and

scanned documents, backed up files or databases, faxes and information stored on telephone logging systems, or, it may form part of the Association's manual records, where individuals can be identified and Personal Data can be easily accessed.

2.5 Personal Data may include personal details such as goods and services, supplier details, financial details, lifestyle and social circumstances, complaints, education and employment details, health, safety and security details and visual images, personal appearance and behaviour and online identifiers such as IP addresses.

2.6 Some Personal Data is classed as **Sensitive Personal Data**. This Personal Data is subject to further and more stringent regulations under GDPR which requires that it may be processed only in certain circumstances as set out later in this Policy.

2.7 Personal Data is regarded as Sensitive if it includes any of the following types of information about an identified or identifiable natural person:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic data,
- biometric data,
- data concerning health
- data concerning a natural person's sex life or sexual orientation

2.8 Personal Data relating to any proceedings for any offence committed or alleged to have been committed by the Data Subject, the disposal of such proceedings or the sentence of any court in such proceedings shall only be processed when such processing is authorised under EU or National Law. This includes Disclosure and Barring Service checks on prospective and existing employees.

3 Processing and collection

3.1 The Association has adopted and operates procedures in accordance with the six principles of GDPR ("**The Data Protection Principles**") when processing Personal Data.

3.2 The Data Protection Principles require that Personal Data held by the Association is: -

- Processed fairly, lawfully and in a transparent manner in relation to the Data Subject.
- Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed.
- Processed in a way that ensures appropriate security of the Personal Data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.3 Personal Data (including Sensitive Personal Data) will only be processed by the Association where there is a valid legal basis for doing so, as set out in the GDPR and our Data Protection procedures.

3.4 The processing of Sensitive Personal Data shall be proportionate to the aim being pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

3.5 Sensitive Personal Data relating to:

- ethnic origin or religion may be used to provide statistical information to organisations that regulate the Association provided this information is presented in a way that does not identify individuals.
- medical and/or health information may be used to assess applications for housing and adaptations, to assist residents in receiving appropriate care, support and assistance in an emergency, and to ensure that the Association makes reasonable adjustments for employees and Board Members in accordance with the Equality Act 2010.

4 Information Register

The Association will maintain an information register on the Personal Data that it processes, which will include the type, location, security arrangements, legal basis for collecting, who the data may be shared with and how long it will be retained.

5 Accuracy and Relevance

5.1 The Association will take steps to ensure that any Personal Data it processes is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained.

5.2 The Association will not process Personal Data obtained for one particular purpose for any other unconnected purposes unless the individual concerned has consented to this or would otherwise reasonably expect this.

6 Data Storage

6.1 The Association will take steps to ensure that Personal Data is kept secure from unauthorised users or unlawful loss or disclosure.

7 Disclosure

7.1 Where necessary, in order to carry out its objectives, the Association may need to share some of the Personal Data it processes with other organisations and individuals. This includes the following:

- Local government and authorities
- Central government including the Department of Work and Pensions
- Contractors and Suppliers
- Service providers, including resident's online accounts and SMS messaging
- Regulatory bodies such as the Regulator for Social Housing
- Family, associates and representatives of the Data Subject
- Professional bodies and advisors such as auditors, consultants and solicitors
- Health authorities, social welfare and social service organisations

- Enquirers and complainants
- Credit reference and debt collection agencies
- Courts and tribunals
- Other housing associations or trusts or landlords
- Educators and examining bodies
- Financial organisations
- Survey and research organisations
- Trade unions and associations
- Security organisations
- Probation services
- Charities and voluntary organisations
- Emergency services such as the Police and the Fire Brigade
- Employment and recruitment agencies and organisations who process applications for Disclosure and Barring Checks
- Current, past or prospective employers
- Insurers and providers of staff benefits
- Press, media and social media, provided Data Subject's identity is kept anonymous or explicit consent has been received.

7.2 Personal Data held by the Association will not be sold to any other organisation or individual.

7.3 Personal Data held by the Association will not be shared with organisations or individuals who have no particular right to know about the information or the internal business of the Association without the Data Subject's explicit written consent, other than in exceptional circumstances in compliance with the Regulations, as follows:

- Where there is clear evidence of fraud
- To comply with the law
- In connection with legal proceedings
- To protect the health and safety of the Data Subject, where they would be at risk if the information were not disclosed, or where there is a legal requirement to do so
- Anonymously for statistical purposes

7.4 If there is no clear legal basis for sharing Personal Data, consent or explicit consent will be obtained from the Data Subject where:

- Confidential or particularly sensitive information is going to be shared;
- The individual would be likely to object should the data be shared without his or her consent; or
- The sharing is likely to have a significant impact on an individual or group of individuals.

8 Retention

8.1 The Association will not retain Personal Data for longer than is required.

8.2 Personal Data that is no longer required will be disposed of in a way which protects the rights and privacy of Data Subjects.

8.3 Anonymous Personal Data may be kept for statistical use, for example, equality and diversity opportunities.

9 Data Subject Rights

9.1 Data Subjects are entitled to: -

- Know what information the Association holds and processes about them and why,
- Request access to it,
- Require the Association to rectify, block, erase or destroy inaccurate information
- Prevent processing likely to cause unwarranted damage or distress
- Prevent processing for the purposes of direct marketing

9.2 All requests should be made in writing using the Subject Access Request form and proof of identity should also be given.

9.3 Any reasonable request for Personal Data from a Data Subject will be processed in accordance with the Regulations.

9.4 Except as outlined in the clause below, a Data Subject shall receive access to their Personal Data within one calendar month of the request being made and this will be made free of charge.

9.5 The Association reserves the right to refuse a request, extend the period to provide the information being requested or charge a reasonable fee based on administrative costs, where the request is manifestly unfounded, excessive or a repeated request for copies of the same information. In such cases, the Data Subject will be notified accordingly within one calendar month of the request being made.

10 Data Breaches

10.1 A Personal Data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service.

10.2 Where such a breach occurs the Association will use its best endeavours to investigate the breach and draw up an appropriate action plan, including the taking of remedial steps and notification of the Information Commissioner and all affected Data Subjects as may be necessary.

11 Responsibility

11.1 Under the Data Protection Guardianship Code, whilst everyone who processes personal data is responsible for complying with the Association's policies and procedures and the regulations on Data Protection, overall responsibility for Personal Data rests with the Management Committee.

11.2 The Management Committee delegates responsibilities to the managing agent's who manage Old Etonian Housing Association, the Data Controller, who are responsible for the personal data, obtained, used and held.

11.3 The managing agent's Finance Director will act as the Data Protection Officer ("DPO") for the Association and together with the managing agent's Senior Management Team, is responsible for the effective implementation of this Policy.

11.4 The DPO will be responsible for:

- Understanding and communicating legal obligations
- Identifying potential problem areas or risks
- Keeping the Management Committee updated about data protection responsibilities, risks and issues
- Producing and reviewing all data protection procedures and policies on a regular basis
- Providing appropriate training and advice for all staff members
- Answering questions on data protection from staff, board members and other stakeholders
- Checking and approving contracts or agreements with third parties regarding data processing.
- Ensuring systems, services, software and equipment meet acceptable security standards

11.5 All employees who process Personal Data must:

- Ensure they understand and act in line with this Policy and Procedures and the Data Protection Principles.
- Inform their line manager, the Chief Executive or the Finance Director if they become or are aware of a breach of this Policy.
- Inform the Chief Executive or the Finance Director if they become or are aware of a data breach whether malicious or accidental.

11.6 A breach of the Regulations or failure to follow this Data Protection Policy is considered a serious offence and as such may result in disciplinary proceedings.

12 Training and Review

12.1 This Policy will be made available for viewing on the website and all current tenants and those applying for accommodation, together with current and prospective employees will be guided towards this Policy so that they may see how Personal Data collected may be used by the Association and who this data may be shared with.

12.2 All staff will receive training and refresher training on this policy and on the associated procedures, in particular when there has been a substantial change in the law or in the Association's policy and procedures.

12.3 New staff joiners will receive training as part of their induction process.

12.4 This Policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments in relevant legislature.