Abertay Housing Association	**TITLE OF POLICY**	**NO.**
	Privacy and Data Protection	**VERSION 1**
		DATE May 18
		PAGES

Written By:	Marjorie Sloan
Department	
Guiding Standard	**Number(s)**

Approval Date by Committee	
Target Date for Revision	May 22
Date Reviewed	

Original	**May 18**
Date last Amended	

1. Introduction

Abertay Housing Association (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. This privacy and data protection policy sets out how the Association handles the data of its customers, suppliers, employees, workers and other third parties, and the procedures for the management of such data (the "**Policy**").

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 customers (tenants, factored owners etc.), employees, members 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 which includes Sensitive Personal Data / Special Categories of Personal Data and Pseudonymised Personal Data (all defined below) but excludes anonymous data or data that has the identity of the individual permanently removed.

2. Legislation

It is a legal requirement that the Association process data correctly; the Association must collect, handle and store Personal Data in accordance with the following legislation:

(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 from time to time 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 GDPR, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy (together "**Data Protection Law**").

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 can be defined as follows:

3.1.1 "**Personal Data**" is that from which a living individual can be identified (directly or indirectly) either by that data alone, or in conjunction with other data held or reasonably accessed by the Association. The Personal Data held and processed by the Association is detailed within the Association's Fair Processing

Notice and the Employee Fair Processing Notice which has been provided to all employees.

3.1.2 "**Special Category Personal Data**" or "**Sensitive Personal Data**" 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).

3.1.3 "**Pseudonymised Personal Data**" is data that directly or indirectly identifies an individual which has been replaced with one or more artificial identifiers or pseudonyms so that the individual cannot be identified without the use of additional data.

4. Processing of Personal Data

4.1 The Association is permitted to process Personal Data on behalf of data subjects provided the processing is:

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

4.2 Fair Processing Notice ("FPN")

4.2.1 The Association has produced a FPN which it is required to provide to all data subjects whose Personal Data is held by the Association. That FPN must be provided to the data subject 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 FPN sets out the Personal Data processed by the Association and the basis for that processing.

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 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 HR Manager.

4.4 Consent

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

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, in accordance with the Association's relevant policies and procedures, with third parties who assist with its day to day activities (e.g. processing its employees' pensions). In order that the Association can monitor compliance by these third parties with Data Protection Law, the Association will require the third party organisations to enter in to a data sharing agreement with the Association governing the processing of data, security measures to be implemented and responsibility for breaches in the form of the model Data Sharing Agreement.

5.2 Personal Data is from time to time shared amongst the Association and third parties who control the Personal Data also. Both the Association

and the third party will be processing that data in their individual capacities as data controllers.

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. payroll, maintenance and repair works).

5.3.1 A data processor must comply with Data Protection Law. The Association's data processors must ensure they: (i) have appropriate technical security measures in place; (ii) maintain records of processing activities; (iii) notify the Association immediately if a data breach is suffered, or a data subject request or complaint is received; and (iv) follow the Association's relevant policies and procedures.

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 its sub-contractors': (i) data protection breaches; and (ii) compliance with Data Protection Laws and the Association's relevant policies and procedures. The sub-contractor should be aware of the data processor's obligations under its data sharing agreement with the Association.

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 model Data Protection Addendum.

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 should be kept in a secure place where unauthorised personnel cannot access it. Employees should 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 securely 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 securely stored: (i) in a file and (ii) in accordance with the Association'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 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 to mobile devices or personal equipment and should be stored on the Association's 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.

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 or been discovered, the Data Protection Officer ("**DPO**") must be notified in writing of: (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
- The Association must seek to contain the breach by whatever means available;
- The DPO must consider whether the breach is one which requires to be: (i) reported to the Information Commissioner's Office ("**ICO**") and data subjects affected (in accordance with this clause 7); and (ii) notified to relevant third parties in accordance with the terms of any applicable data sharing agreements.

7.3 Reporting to the ICO

The DPO will require to report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the ICO within **72 hours** of the breach occurring or being discovered if later. The DPO must also consider whether it is appropriate to notify those data subjects affected by the breach. Failure to notify a breach to ICO when required to do so can result in a significant fine of up to 10 million euros or 2% of the Association's turnover.

8. Data Protection Officer ("DPO")

8.1. A DPO is an individual who has an over-arching responsibility and oversight over compliance by the Association with Data Protection Law. The Association has elected to appoint a Data Protection Officer whose details are noted on the Association's website and contained within the FPN.

8.2 The DPO will be responsible for:

8.2.1 monitoring the Association's compliance with Data Protection Law 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. In particular, data subjects have the right to:

- be informed of the Personal Data held about them by the Association;
- access their Personal Data, whether in written or electronic form;
- rectification of their Personal Data;
- erasure of their Personal Data;
- restrict processing of their Personal Data;
- Personal Data portability; and
- object to the Association's processing of their Personal data.

These rights are notified to the Association's tenants and other customers in the Association's FPN.

9.2 Subject Access Requests

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

9.2.1 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.

9.2.2 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.

9.2.3 where it 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.

9.3 The Right to be Forgotten

9.3.1 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.

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

9.4 The Right to Restrict or Object to Processing

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

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

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

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 should consult the ICO in the event that a PIA 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 PIA they should notify the DPO immediately.

11. Archiving, Retention and Destruction of Data

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 securely archived and destroyed in accordance with the periods specified within the Association's Data Retention Periods table.