DATA PROTECTION POLICY

Purpose:	To establish DPHA's policy on ensuring the secure and safe management of personal data held by the Association in relation to customers, staff, Management Committee and other customers.
Date Last Reviewed:	29 July 2022
Date Approved by Policy Review Working Group:	July 2022
Next Review Date:	July 2024
Guidance:	SFHA – GDPR Model Documentation and Guidance Notes – Oct 19
Regulatory Standards:	Standard 2 - The RSL is open and accountable for what it does. It understands and takes account of the need and priorities of it tenants, service users and stakeholders and its primary focus is the sustainable achievement of these priorities. Standard 5 - The RSL conducts its affairs with honesty and integrity.
Other Relevant Policies:	• Personal Data Breach Management Procedure • Data Subjects Rights Procedure • Privacy notices for staff, committee and public • equipment usage policies • Staff code of conduct
Approved by Management Committee:	July 2022

CONTENTS **PAGE NO.**

1. **INTRODUCTION**

Dalmuir Park Housing Association (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 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, committee 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 and sensitive personal data known as Special Categories of personal data under the General Data Protection Regulation (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 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 UK 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);
(c) The Data Protection Act 2018 ("the 2018 Act") 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). Data which can identify Data Subjects is known as personal data. The personal data held and processed by the Association is detailed within the Customer Privacy Notice.

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 must comply with the data protection principles ensuring that personal data is:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner 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.

In addition to these principles the law requires organisations to be responsible for, and be able to, demonstrate compliance with the above principles. This is often referred to as the 'accountability' principle.

4.2 The Association is permitted to process personal Data on behalf of data subjects provided it is doing so in accordance with one of the following legal bases:

1. Processing with the **consent** of the data subject (see section 4.4);
2. 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;

3. Processing is necessary for the Association's compliance with a **legal obligation;**
4. Processing is necessary to protect the **vital interests** of the data subject or another person;
5. 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
6. Processing is necessary for the purposes of **legitimate interests**.

4.3 Privacy Notice

4.2.1 The Association has produced a Customer Privacy Notice (CPN) which it is required to provide to all customers whose personal data is held by the Association. That CPN must be provided to the customer from the outset of processing their personal data and they should be advised of the terms of the CPN when it is provided to them.

4.2.2 The CPN sets out the personal data processed by the Association and the basis for that processing. This document is provided to all of the Association's customers at the outset of processing their data.

4.4 Employees

4.4.1 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 Privacy Notice which is provided to prospective Employees at application stage.

4.4.1.1 The Data Protection Clause of the Contract of Employment will be provided to all employees.

4.4.2 A copy of any employee's personal data held by the Association is available upon request by that employee from the Association's Corporate Services Officer.

4.5 Consent

Consent, as a legal basis of 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 legal basis 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). Where it is being relied on, Data Subjects are free to withhold their consent or withdraw it at any future time.

4.6 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 rely on an additional legal basis for processing in accordance with one of the ~~following~~ special category legal bases 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 or social security**; or social protection law;
- Processing is necessary for health of 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 legal bases 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

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 may require the third-party organisations to enter into an Agreement with the Association governing the processing of data, security measures to be implemented and responsibility for breaches. This will apply in situations where the third party is a joint controller.

5.2 Data Sharing

5.2.1 Personal Data is from time to time shared amongst the Association and third parties who require access to the same Personal Data as the Association. Whilst the Association and third parties may jointly determine the purpose and means of processing, 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 Processor Agreement with the Association.

5.3 Data Processors

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

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 into a Data Processor Agreement. The Data Processor Agreement may form part of a contract with the third party or be an addendum to the contract.

6. DATA STORAGE AND SECURITY

All personal data held by the Association 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 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 or encrypted

when being sent internally or externally to the Association's data processors or those with whom the Association has entered into 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

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 will be managed with in line with the Association's Information Security and Personal Data Breach Management procedure at Appendix 1. 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 section 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 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 Corporates Services Officer 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 Corporates Services Officer will inform the DPO who 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 guidance in Section 7;

- Notify 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 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")

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 has appointed a Data Protection Officer (DPO). The Association has engaged RGDP LLP (www.rgdp.co.uk) as our Data Protection Officer. The Association's DPO's details are noted on the Association's website and contained within all its Privacy Notices.

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

9. DATA SUBJECT RIGHTS

A. Certain rights are provided to Data Subjects under the GDPR. These rights are notified to the Association's tenants and other customers in the Association's Customer Privacy Notice. Such rights are subject to qualification and are not absolute.

The Association's Data Subject Rights procedure is set out at Appendix 2 to this policy and explains how the Association will comply with individuals':

- **Right to be Informed** – by ensuring individuals are informed of the reasons for processing their data in a clear, transparent and easily accessible form and informing them of all their rights.
- **Right to Access** – by ensuring that individuals are aware of their right to obtain confirmation that their data is being processed; access to copies of their personal data and other information such as a privacy notice and how to execute this right.
- **Right to Rectification** – by correcting personal data that is found to be inaccurate. We will advise data subjects on how to inform us that their data is inaccurate. Inaccuracies with be rectified without undue delay.
- **Right to Erasure** (also known as 'the right to be forgotten') - we will advise data subjects of their right to request the deletion or removal of personal data where processing is no longer required or justified.
- **Rights to Restrict Processing** - we will restrict processing when a valid request is received by a data subject and inform individuals of how to exercise this right.
- **Right to Data Portability** – by allowing, where possible, data to be transferred to similar organisation in a machine-readable format.

- **Right to Object** – by stopping processing personal data, unless we can demonstrate legitimate grounds for the processing, which override the interest, rights and freedoms of an individual, or the processing is for the establishment, exercise or defence of legal claims.

10. DATA PROTECTION BY DESIGN

The Association has an obligation to implement technical and organisational measures to demonstrate that we have considered and integrated data protection into our processing activities. When introducing any new type of processing, particularly using new technologies, we will take account of whether the processing is likely to result in a high risk to the rights and freedoms of individuals and carry out Data Protection Impact Assessment (DPIA). Advice will be provided by the DPO on conducting Data Protection Impact Assessments in line with the Association's Data Protection Impact Assessment Procedure which is at Appendix 3.

i.

11. ARCHIVING, RETENTION AND DESTRUCTION OF DATA

The Association must not 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 within its Data Retention procedure and schedule at Appendix 4.

12. TRAINING

Adequate and role specific training will be provided to everyone who has access to personal data, to ensure they understand their responsibilities when handling personal data. This will be conducted regularly, during induction for new staff and on an annual refresher basis.

List of Appendixes:

1. Personal Data Breach Management Procedure
2. Data Subject Rights Procedure
3. Data Protection Impact Assessment Procedure -TBC
4. Retention Procedure and Schedule – TBC
5. CCTV Procedure
6. Privacy Notice (Customers/Tenants)
7. Privacy Notice (Employees)
8. Privacy Notice (Governing Body/Committee)