Privacy Policy

Policy Ref: C08

Prepared By	Chief Executive
Date of Review	June 2021
Date of Next Review	June 2024
Reviewed By	PHA Board

1. Introduction

Partick 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, 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 UK General Data Protection Regulation ('UK 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 processes data correctly; the Association must collect, handle and store personal information in accordance with the relevant legislation. The legislation relevant to this policy includes, but is not limited to, the following:

- 'the UK GDPR;
- the Data Protection Act 2018;
- the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
- any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law including 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 having left 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 Notice at Appendix 1 hereto and the Data Protection Addendum of 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 will comply with its legal obligations and the **data protection principles** by ensuring that personal data is:

- **processed lawfully, fairly and in a transparent manner in relation to individuals**. Individuals will be advised on the reasons for processing via a Privacy Notice. Where data subjects' consent is required to process personal data, consent will be requested in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Data Subjects will be advised of their right to withdraw consent and the process for Data Subjects to withdraw consent will be simple.
- **collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**. Personal data will only be used for the original purpose it was collected for and these purposes will be made clear to the data subject. If the Association wishes to use personal data for a different purpose, the data subject will be notified prior to processing.

- **adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed**. The Association will only collect the minimum personal data required for the purpose. Any personal data deemed to be excessive or no longer required for the purposes collected for will be securely deleted. Any personal information that is optional for individuals to provide will be clearly marked as optional on any forms.
- **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**. The Association will take reasonable steps to keep personal data up to date, where relevant, to ensure accuracy. Any personal data found to be inaccurate will be updated promptly. Any inaccurate personal data that has been shared with third parties will also be updated.
- **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**. The Association will hold data for the minimum time necessary to fulfil its purpose. Timescales for retention of personal data will be stated in a Retention Schedule. Data will be disposed of in a responsible manner ensuring confidentiality and security.
- **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**. The Association will implement appropriate security measures to protect personal data. Personal data will only be accessible to those authorised to access personal data on a 'need to know' basis. Employees will keep data secure by taking sensible precautions and following the relevant the Association policies and procedures relating to data protection.

In addition, the Association will comply with the 'Accountability Principle' that states that organisations are to be responsible for, and be able to demonstrate, compliance with the above principles.

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

- Processing with the consent of the data subject (see clause 4.5 below);
- 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 the legitimate interests of the Association.

4.3 Fair Processing Notice

4.3.1 The Association has produced a Fair Processing Notice (FPN), which it is required to provide to all customers whose Personal data is held by the Association. That FPN must be provided to the customer 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.

4.3.2 The Fair Processing Notice at Appendix 1 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 Fair Processing Notice which is provided to Employees at the same time as their Contract of Employment.

4.4.2 A copy of any employee's Personal Data held by the Association is available upon written request by that employee from the Association's Corporate Services Manager.

4.5 Consent

Consent as a ground 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 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 seek to 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, where possible, 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) and the data subject should be advised of their right to withdraw their consent.

4.6 Processing of Special Category / 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 or otherwise in accordance with the law:

- 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 relates to personal data which are manifestly made public by the data subject;
- 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 and Processing

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 generally require the third-party organisations to enter in to an appropriate Agreement with the Association governing the processing of data, security measures to be implemented and responsibility for breaches.

5.2 Data Sharing

In certain circumstances the Association may share personal data with third parties. This may be part of a regular exchange of data, one-off disclosures or in unexpected or emergency situations. In all cases, appropriate security measures will be used when sharing any personal data.

Where data is shared regularly, a contract or data sharing agreement will be put in place to establish what data will be shared and the agreed purpose.

Prior to sharing personal data, the Association will consider any legal implications of doing so.

Data Subjects will be advised of data sharing via the relevant the Fair Processing Notice.

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 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 model Data Protection Addendum set out in Appendix 3 to this Policy.

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 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 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 into 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 Internal Reporting

Occasionally the Association may experience a data security incident or personal data breach; this could be if personal data is:

- Lost, e.g. misplacing documents or equipment that contain personal data through human error, via fire, flood or other damage to premises where data is stored.
- Stolen; theft or as a result of a targeted attack on the IT network (cyber-attack).
- Accidently disclosed to an unauthorised individual, e.g., email or letter sent to the wrong address.
- Inappropriately accessed or used.

All security incidents or personal data breaches must be reported to and managed by the Data Protection Lead (Corporate Services Manager) who will be advised and assisted by the DPO, including undertaking 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 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 reasonable means available;
- The DPO must consider whether the breach is one which requires to be reported to the ICO and / or data subjects affected and do so in accordance with this clause 7;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements.

7.2 Reporting to the ICO and / or Data Subjects

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') as soon as possible and in any event 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, and such data subjects should be informed without delay if the breach is likely to result in a high risk to the rights and freedoms of individuals.

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 elected to appoint a Data Protection Officer whose details are noted on the Association's website and contained within the Fair Processing Notice at Appendix 2 hereto.

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 Part 7 hereof.

9. Data Subject Rights

The Association will uphold the rights of data subjects to access and retain control over their personal data in accordance with its Data Subject Rights Procedure. 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 the Association will advise data subjects on how to inform us that their data is inaccurate. Inaccuracies with be rectified without undue delay.
- **Right to Erasure** (sometimes referred to as'the right to be forgotten') – the Association 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** – the Association 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 legitimate grounds can be demonstrated 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

10.1 The Association has an obligation to implement technical and organisational measures to demonstrate that data protection has been considered and integrated into its processing activities.

10.2 When introducing any new type of processing, particularly using new technologies, it will take account of whether the processing is likely to result in a high risk to the rights and freedoms of individuals and consider the need for a Data Protection Impact Assessment (DPIA).

10.3 All new policies including the processing of personal data will be reviewed by the Data Protection Lead to ensure compliance with the law and establish if a DPIA is required. Advice and assistance will be provided by the DPO and if it is confirmed that a DPIA is required, it will be carried out in accordance with the Association's DPIA Procedure.

11. Training

All staff will be made aware of good practice in data protection and where to find guidance and support for data protection issues. Adequate and role specific data protection training will be provided during induction and regularly thereafter to everyone who has access to personal data to ensure they understand their responsibilities.

12. Breach of Policy

Any breaches of this policy may be dealt with in accordance with the Association's disciplinary procedures.

13. Monitoring and Reporting

Regular monitoring and audits will be undertaken by the Data Protection Lead and/or DPO to check compliance with the law, this policy and associated procedures. Any concerns will be raised with the Corporate Services Manager.

14. 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 archived and destroyed in accordance with the periods specified in the Retention Policy and Schedule. .

15. Policy Review

This policy will be reviewed and revised every three years or more frequently if required to meet changes in legislation, address any weaknesses identified and/ or to implement new/good practices or lessons learned.

Appendices

Appendix 1 – Fair Processing Notice

Appendix 2 – Model Data Sharing Agreement

Appendix 3 – Model Data Processor Addendum