PEAKS & PLAINS
Housing Trust

Data Protection Policy

Version number: V4

Effective Date:
September 2022

TABLE OF CONTENTS

1. INTRODUCTION

1.1. This Data Protection Policy (this "policy") sets out the obligations of Cheshire Peaks & Plains Housing Trust ("Trust", "we", "us", "our") regarding data protection and the rights of individuals whose Personal Data we collect, use and process in the course of our business activities.

1.2. This policy applies to all staff members of the Trust, Board and Committee members, workers and contractors ("staff", "you", "your").

1.3. Cheshire Peaks & Plains Housing Trust is registered as a Data Controller with the Information Commissioner's Office having registration number Z9530780.

2. SCOPE

2.1. This policy applies to all Personal Data processed by the Trust whether held in electronic form or in physical records, and regardless of the media on which that data is stored. It applies to Personal Data we process as a Data Controller.

2.2. All consultants, agencies and other parties working on our behalf and handling Personal Data must ensure that all of their employees who are involved in the processing of Personal Data are held to the same obligations as applicable to Trust staff arising out of this policy.

3. LEGAL & REGULATORY REQUIREMENTS

3.1. This policy has been prepared with due regard to the data protection laws applicable to the Trust and our Personal Data Processing activities. These Data Protection Laws include the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("DPA 2018"), (collectively referred to as the "Data Protection Law").

3.2. There is a broad regulatory requirement in the Regulator for Social Housing's Governance and Financial Viability Standard, for Registered Providers to comply with all relevant law. Complying with data protection law and regulations is covered by this requirement.

4. DEFINITIONS

4.1. The following definitions apply across all Trust data protection policies, procedures and supporting documents:

Term	Description:
Accountability	A duty to answer to the success or failure of strategies, decisions, practices and processes.
Criminal Information	Personal Data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings
Data Controller	A person, entity or organisation that determines the purposes and means of processing Personal Data.
DPA 2018	Data Protection Act 2018

Data Protection Officer	The Data Protection Officer is responsible for overseeing data protection strategy and implementation to ensure compliance with Data Protection Law.
Data Protection Law	UK GDPR and the Data Protection Act 2018 ("DPA 2018").
Data Processor	A person, entity or organisation that processes Personal Data on behalf of a Data Controller.
Data Subject	Any natural person (individual) whose Personal Data is being processed.
Data Protection Impact Assessment (DPIA)	A DPIA is designed to help an organisation assess the risks associated with data processing activities that could compromise the rights and freedoms of individuals. It can be used to identify and mitigate risk associated with a product, service, business process or other organisational change.
Legitimate Interest Assessment (LIA)	Determines if individual's Personal Data is being used in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
Personal Data	Any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Processing	Any operation or set of operations that is performed on Personal Data, such as collection, recording, organising, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, combination, restriction or erasure.
Information Commissioner's Office (ICO)	An independent public body established in the UK responsible for monitoring the application of the UK GDPR, Data Protection Act 2018 and the Privacy & Electronic Communications Regulations.
Sensitive Personal Data	Special Category Data and Personal Data relating to criminal convictions and offences.
Special Category Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data, biometric data (where used to identify a data subject), data concerning health and data concerning a natural person's sex life or sexual orientation.
UK GDPR	has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018

5. OUR POLICY

5.1. Overall Commitment

5.1.1. The Trust places high importance on respecting the privacy and protecting the Personal Data of individuals with whom we work including customers,staff and stakeholders. We are committed to the fair, lawful and transparent handling of Personal Data and to facilitating the rights of individuals. Our policy is to comply not only to the letter of the law, but also to the spirit of the law.

5.2. Data Protection Principles

The following data protection principles shall govern the collection, use, retention, transfer, disclosure and destruction of Personal Data by the Trust:

5.2.1. **Principle 1 - Fair, Lawful & Transparent**
Personal Data must be processed lawfully, fairly, and in a transparent manner in relation to the Data Subject.

5.2.2. **Principle 2 - Purpose Limitation**
Personal Data must only be collected and processed for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.

5.2.3. **Principle 3 - Data Minimisation**
Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

5.2.4. **Principle 4 - Accuracy:**
Personal Data must be accurate and kept up to date.

5.2.5. **Principle 5 - Storage Limitation:**
Personal Data which permits identification of Data Subjects (i.e. data which has not been anonymised) must be kept for no longer than is necessary for the purposes for which the Personal Data are processed.

5.2.6. **Principle 6 - Security:**
Personal Data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

5.2.7. The Trust will monitor the risks to Data Subjects associated with all existing and planned Personal Data processing activities and implement appropriate technical and organisational measures to safeguard Data Subjects and ensure the data protection principles set out in this policy are met. This risk led approach to data protection will be applied across all Trust business activities to ensure data protection by design and by default..

5.3. **Data Protection by Design and Default**

5.3.1. We will ensure that the risks to rights and freedoms of Data Subjects associated with processing are key considerations when:

a) Designing, implementing and during the life of business practices and processes that involve the processing of personal data ("processing activities"); and

b) Developing, designing, selecting, procuring, and using applications, services, products and other IT systems and technologies for collecting, holding, sharing, accessing, and otherwise processing personal data ("processing systems").

5.3.2. This risk led approach to processing activities and processing systems shall apply throughout the full lifecycle of the processing, from initial planning and setting of specifications, during use of processing systems, through to disposal of the personal data. It shall take into account both the likelihood and the severity of the potential harm to the rights and freedoms of Data Subjects.

5.3.3. Where the risks to rights and freedoms of Data Subjects associated with any existing or planned Personal Data processing to be carried out by the Trust are potentially high or where otherwise required by applicable law, the Trust will carry out a Data Protection Impact Assessment ("DPIA"). All DPIAs are to be undertaken as set out in the Trust's DPIA Procedure. A record of DPIAs shall be kept, to include details of the outcome, the names of the parties signing off the DPIA recommendations and the date of next review.

5.3.4. Safeguards and preventive measures shall be implemented into processing activities and processing systems from the outset and throughout the processing lifecycle, to mitigate the risks to data subjects and protect their rights. These safeguards and measures shall be proportionate to the risks and include organisational (e.g. policy, awareness, governance, and assurance) as well as technical measures (e.g. pseudonymisation). The objectives of such safeguards and measures shall include:

a) data minimisation
b) limiting the extent of the processing, storage, and access to what is strictly necessary
c) ensuring transparency for data subjects regarding the processing activities; and
d) ensuring the security of the personal data.

5.4. **Data Processing Obligations**

5.4.1. Data Subjects must be provided with information notifying them of the purposes for which the Trust will process their Personal Data (a "privacy notice"). When Personal Data is obtained directly, the privacy notice shall be provided to the Data Subject at the time of collection. The privacy notice must explain what processing will occur and must also include the information set out at Appendix 1.

5.4.2. Use of the Personal Data by the Trust must match the description given in the privacy notice and be limited to what is necessary for the specific purposes stated. Where our lawful basis for processing is based on our legitimate interests, we may only process the Personal Data if our legitimate interests are not outweighed by the interests, rights and freedoms of the Data Subjects in question. A legitimate interests assessment must be performed to confirm this.

5.4.3. We must not collect or process any more Personal Data than is strictly necessary for the purposes of the processing ("data minimisation"), as set out in our privacy notice, and must ensure that data minimisation continues to be applied throughout the lifetime of the processing activities.

5.4.4. Personal Data must be kept accurate and up to date. The accuracy of Personal Data must be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps are to be taken without delay to amend or erase that data, as appropriate. Personal Data must not be kept for any longer than is necessary for the purpose for which that data was originally collected and processed. When the data is no longer required, all reasonable steps must be taken to securely erase or dispose of it without delay, as set out at Section 12 of this policy.

5.4.5. Personal Data must be kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

5.5. **Record of Processing Activities (RoPA)**

5.5.1. The Trust will keep written internal records of processing activities in respect of all Personal Data collection, holding, and processing ("RoPA").

5.5.2. The Trust's RoPA will incorporate the following information:

- our name and contact details, our Data Protection Officer or point of contact for data related concerns and any joint controllers;
- the purposes for which we process Personal Data;
- details of the categories of Personal Data collected, held, and processed by us; and the categories of Data Subject to which that Personal Data relates;
- details (and categories) of any third parties that will receive Personal Data from us;
- details of any transfers of Personal Data to countries outside the UK including all mechanisms and security safeguards;
- the envisaged retention periods for the different categories of Personal Data; and
- descriptions of the technical and organisational measures we have implemented to ensure the security of Personal Data.

5.6. **Training and Awareness**

5.6.1. Only those staff and other interested parties that need access to, and use of, Personal Data to carry out their assigned duties correctly will be permitted access to Personal Data we hold. All staff and other interested parties handling Personal Data on behalf of the Trust must be:

- made fully aware of both their individual responsibilities and the Trust's responsibilities under this policy and applicable law, and be provided with a copy of this policy;
- appropriately trained to do so and suitably supervised, with training to be provided upon starting with the Trust and refresher training to be provided at least annually; and

- bound to handle the Personal Data in accordance with this policy and the law by contract.

5.6.2. When using a Data Processor (or, where permitted, a sub-Data Processor), a binding contract must be implemented between the Trust and the Data Processor setting out the subject matter and duration of the processing; the nature and purpose of the processing; the type of Personal Data and categories of Data Subject; and the obligations and rights of the controller. Processor contracts must also include the terms set out at Appendix 2.

5.7. **Data Subject Rights**

5.7.1. Data subjects have the following rights regarding Personal Data processing and the data that is collected and held about them:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure (also known as the 'right to be forgotten');
- the right to restrict processing;
- the right to data portability;
- the right to object;
- rights with respect to automated decision-making and profiling.

5.7.2. Requests by Data Subjects to exercise their rights must be facilitated as set out in the Trust's Data Subject Rights Procedure(s).

5.8. **Protection of Personal Data**

5.8.1. All staff and other interested parties must comply with the following when working with Personal Data:

- Personal Data must be handled with care at all times and must not be shared with any colleague, who does not have access to it, or with any third party without authorisation;
- physical records must not be left unattended or on view to unauthorised employees, agents, contractors or other parties at any time and must not be removed from the business premises without authorisation;
- if Personal Data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
- all physical copies of Personal Data, along with any electronic copies stored on physical, removable media should be stored securely in a locked filing cabinet, drawer, box or similar;
- all electronic copies of Personal Data are to be stored securely using passwords which are changed regularly, and which do not use words or phrases that can be easily guessed or otherwise compromised;
- Personal Data must not be transferred to any device personally belonging to an employee or transferred or uploaded to any personal file sharing, storage, communication or equivalent service (such as a personal cloud service);

- Personal Data may only be transferred to devices belonging to agents, contractors, or other parties working on our behalf where the party in question has agreed to comply fully with the letter and spirit of this policy and the Data Protection Law and all other applicable law (which may include demonstrating that all suitable technical and organisational measures have been taken and entering into a Data Processor contract with the Trust);
- all Personal Data stored electronically shall be backed-up regularly and securely;
- under no circumstances must any passwords be written down or shared between any employees, agents, contractors, or other parties working on our behalf, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method;
- all Staff and other interested parties involved in processing Personal Data are required to read and adhere to the Trust's Information Security Policy;
- No third-party data processors will be appointed who are unable to provide satisfactory assurances that they will handle personal data in a secure and confidential manner in accordance with data protection legislation and in line with our Information Security Policy;
- Third-party data processors will be required to notify us as soon as possible in the event of a data breach and no later than 24 hours after they become aware of the breach. This will allow for PPHT to evaluate and report on the issue to the Information Commissioners' Office (ICO) in-line with their guidance and;
- Commercially sensitive data will be protected through contractual confidentiality clauses and Non-Disclosure Agreements (NDAs) with third-party organisations

5.9. **Children's Data**

5.9.1. We will take special measures when processing personal data relating to children including the nature of privacy information provided and approach to information rights requests. In accordance with ICO guidance, and the UN Convention on the Rights of the Child, a child means anyone under the age of 18.

5.10. **Data Retention & Destruction**

5.10.1. We may only retain Personal Data for as long as is reasonably required and in any event, only for as long as set out in the Trust's Personal Data Retention Policy. Written authorisation from the Executive Management Team (EMT) is required to retain Personal Data for longer than as set out in the Personal Data Retention Policy.

5.10.2. Once Personal Data records have reached the end of their life, they must be securely destroyed in a manner that ensures that they can no longer be used.

5.11. **Data Sharing**

5.11.1. We will only share Personal Data with third parties where there is a legal basis for doing so and where the data sharing is necessary for the specified purposes. The sharing of Personal Data will only be permitted where either a data sharing agreement is in place, where we have the consent of the data subject or where it is otherwise fair and lawful to do so. It may also be shared in one of the exceptional circumstances listed below:

- where there is a suspicion that a criminal offence has been committed
- where there is clear evidence of fraud
- in connection with legal proceedings
- where it is essential to enable Peaks & Plains to carry out its duties
- where the health and safety of an individual would be at risk by not disclosing the information
- where the data is anonymised and to be used for statistical research

5.11.2. All data sharing agreements must be agreed by the relevant member of Senior Leadership Team (SLT) and the Data Protection Officer. Data sharing agreements will be recorded by the SLT in a central register and will be reviewed periodically to ensure that they are still necessary, accurate and are up to date.

5.11.3. Only secure methods of transferring personal data to other agencies will be used. The ICT team will provide information and advice on approved secure methods.

5.12. **International Data Transfers**

5.12.1. We do not transfer Personal Data outside the UK. However, if this changes in the future, will only transfer ('transfer' includes making available remotely) Personal Data from the UK to countries outside of the UK where:

- the transfer is to a country (or an international organisation) that the UK government has determined ensures an adequate level of protection ("Adequacy");
- an International Data Transfer Agreement ("IDTA") has been put in place between the entity in the UK and the entity located outside the UK;
- binding corporate rules have been implemented, where applicable; or where
- the transfer is otherwise permitted by the law.

5.12.2. Where a transfer is not based on Adequacy, we will undertake a transfer risk assessment ("TRA") using our TRA Template to ensure that Data Subjects (whose Personal Data is transferred) continue to have a level of protection essentially equivalent to that under the UK GDPR. If the TRA outcome is that the appropriate safeguard does not provide the required level of protection, we will implement supplementary measures.

5.13. **Data Breach Notifications**

5.13.1. All Personal Data breaches must be reported immediately to privacy@peaksplains.org. The Head of Business Improvement, Risk & Assurance will ensure these are added to the register of Personal Data breaches.

5.13.2. Unless a Personal Data breach occurs which is unlikely to result in a risk to the rights and freedoms of Data Subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Information Commissioner's Office must be notified of the breach without delay, and in any event, within 72 hours after having become aware of it, if this is feasible. If the notification is not

made within 72 hours, it should be made as soon as possible, together with reasons for the delay. The Information Commissioner's Office (ICO) is the supervisory authority in the UK. The Head of Business Improvement, Risk and Assurance has overall responsibility for ensuring the ICO is informed in a timely manner, in their absence a member of the Business Improvement, Risk and Assurance team has delegated authority.

5.13.3. In the event that a Personal Data breach is likely to result in a high risk (that is, a higher risk than that described immediately above) to the rights and freedoms of Data Subjects, all affected Data Subjects are to be informed of the breach directly and without undue delay.

5.13.4. All Trust data breach notifications must be handled strictly in accordance with the Trust's Personal Data Breach Procedure and be added to the Trust's Personal Data Breach Register.

6. EQUALITY, DIVERSITY & INCLUSION

An Equality Impact Assessment has been carried out on this policy to ensure that, as far as is foreseeable, it will not have a negative or adverse effect on diverse groups.

7. RESPONSIBILITIES

7.1. Key data protection responsibilities within the Trust are as follows:

7.1.1. The Peaks and Plains Housing Trust Board is accountable for ensuring we meet our data protection obligations;

7.1.2. The Governance Committee has delegated responsibility for ensuring that the Trust has appropriate arrangements in place for good Data Governance and for monitoring key performance indicators in relation to Data Protection.

7.1.3. The Senior Leadership Team is responsible for implementing and enforcing this policy;

7.1.4. Line Managers are responsible for ensuring that staff under their management are made aware of adhere and to this policy;

7.1.5. All staff and any other interested parties working with Personal Data over which they have decision making authority are responsible for ensuring it is kept securely, is accessible only to those who need to use it and it is not disclosed to any third party without the authorisation of the Executive Management Team (EMT)

7.1.6. All staff and any other interested parties are required to read, understand, and adhere to this policy when processing Personal Data on our behalf.

7.1.7. The methods of collecting, holding and processing Personal Data by staff, or other parties working on our behalf, are to be regularly evaluated and reviewed by Head of Business Improvement, Risk & Assurance.

7.1.8. Any questions or concerns relating to this Policy should be raised with the Head of Business Improvement, Risk and Assurance

8. MONITORING

8.1. Risks associated with this policy are monitored and maintained in the Data Protection Risk Register

8.2. The Trust reports Data breaches to Governance Committee, any further KPIs identified as part of monitoring this policy will be created and reported to the Performance Management Group.

9. REVIEW

9.1. This policy will be reviewed by Head of Business Improvement, Risk & Assurance in collaboration with the Trusts DPO annually and following any notifiable Personal Data breach.

9.2. If changes are identified as part of this annual review, a revised policy will be brought for approval as and when required, otherwise this Policy will be reviewed by the Governance Committee every three years.

10. ASSOCIATED DOCUMENTS

10.1. This policy should be read together with the following related documents:

- Peaks & Plains Personal Data Retention, Classification and Destruction Policy
- Peaks & Plains Information Security Policy
- Peaks & Plains Data Subject Rights Procedures
- Peaks & Plains Personal Data Breach Procedure
- Peaks & Plains DPIA Procedure
- Peaks & Plains Data Processing Agreement
- Peaks & Plains Mutual Non-Disclosure Agreement
- Peaks & Plains Data Sharing Agreement

POLICY INFORMATION

Policy Name:	Data Protection Policy
Status:	Approved
Approved by:	Governance Committee
Drafted By:	Head of Information and Insight
Date approved:	September 2022
Next Review Date:	September 2025

Appendix 1

Privacy Notices

Privacy notices for Data Subjects shall include:

- the identity and contact details of the Data Controller including, but not limited to, the identity of its Data Protection Officer, where applicable
- the purpose(s) for which the Personal Data is being collected and will be processed and the legal basis justifying that collection and processing;
- where applicable, the legitimate interests upon which is justifying its collection and processing of the Personal Data;
- where the Personal Data is not obtained directly from the Data Subject, the categories of Personal Data collected and processed and the source from which the personal data originated;
- where the Personal Data is to be transferred to one or more third parties, details of those parties;
- where the Personal Data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place;
- details of the length of time the Personal Data will be held (or, where there is no predetermined period, details of how that length of time will be determined);
- details of the Data Subject's rights;
- where applicable, details of the Data Subject's right to withdraw their consent to the processing of their Personal Data at any time;
- details of the Data Subject's right to complain to the Information Commissioner's Office;
- where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the Personal Data and details of any consequences of failing to provide it; and
- details of any automated decision-making that will take place using the Personal Data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

Appendix 2

Processor Contracts

Contracts with Data Processors who will process the Personal Data must set out the subject matter and duration of the processing; the nature and purpose of the processing; the type of Personal Data and categories of Data Subject; and the obligations and rights of the controller. They must also include terms requiring the Data Processor to:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-Data Processors with the prior consent of the Data Controller and under a written contract;
- assist the Data Controller in providing subject access and allowing Data Subjects to exercise their rights under the UK GDPR;
- assist the Data Controller in meeting its UK GDPR obligations (or obligations under other applicable laws) in relation to the security of processing, the notification of Personal Data breaches and data protection impact assessments;
- delete or return all Personal Data to the Data Controller as requested at the end of the contract; and
- submit to audits and inspections, provide the Data Controller with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Data Controller immediately if it is asked to do something infringing the Data Protection Law (or other applicable legislation).