Data Sharing & Protection

Policy & Procedure

Hollywell Housing Trust
Registered Charity No. 1160398

Policy Control

Policy Level	Operational
Version	Version 2 (effective from May 2018)
Approved by	Trustees Chief Executive Officer
Next Review Date	May 2019
Legal/Regulatory framework	General Data Protection Regulations 2018

Policy Statement

We are committed to providing housing support and advice for disadvantaged and vulnerable groups otherwise excluded from the private rented sector in line with our charitable objectives. We seek to do this in a fair, transparent and efficient way at all times. We are committed to ensuring a high standard of accommodation, advice and housing related support to all our service users

1. **Introduction**

This Policy sets out the obligations of Hollywell Housing Trust, a Charity registered with the Charities Commission (Registered Charity No. 1160398) whose registered office is at Unit 21, Basepoint Business Centre, Yeoford Way, Marsh Barton, Exeter, EX2 8LB ("the Charity") regarding data protection and the rights of individuals working with the Charity ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as 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.

This Policy sets the Charity's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Charity, its employees, agents, contractors, or other parties working on behalf of the Charity.

The Charity is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is 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 is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.
- 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.

3. Lawful, Fair, and Transparent Data Processing

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely

affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

The data subject has given consent to the processing of their personal data for one or more specific purposes;

- The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

- The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
- The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
- The processing relates to personal data which is clearly made public by the data subject;
- The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
- The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;
- The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and

safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim 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.

4. Specified, Explicit, and Legitimate Purposes

4.1 The Charity collects and processes the personal data set out in Part 21 of this Policy. This includes:

4.1.1 Personal data collected directly from data subjects; and
4.1.2 Personal data obtained from third parties.

4.2 The Charity only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the GDPR).

4.3 Data subjects are kept informed at all times of the purpose or purposes for which the Charity uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

5. Adequate, Relevant, and Limited Data Processing

5.1 The Charity will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

6. Accuracy of Data and Keeping Data Up-to-Date

6.1 The Charity shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.

6.2 The accuracy of personal data shall be checked when it is collected and at intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. Data Retention

7.1 The Charity shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

7.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

For full details of the Charity's approach to data retention, including retention periods for specific personal

data types held by the Charity, please refer to our Data Retention Policy.

8. Secure Processing

8.1 The Charity shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

9. Accountability and Record-Keeping

9.1 The Charity's Data Protection Officer is Katie Sherjan whose main place of work is at Unit 21, Basepoint Business Centre, Yeoford Way, Marsh Barton, Exeter, EX2 8LB.

9.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Charity's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

10. Data Subject Access

10.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Charity holds about them, what it is doing with that personal data, and why.

10.2 Data subjects wishing to make a SAR may do so in writing or other written communication. SARs should be addressed to the Charity's Data Protection Officer at the above address.

10.3 Responses to SARs shall normally be made within 14 days of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

10.4 All SARs received shall be handled by the Charity's Data Protection Officer.

10.5 The Charity does not charge a fee for the handling of normal SARs. The Charity reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

11. Rectification of Personal Data

11.1 Data subjects have the right to require the Charity to rectify any of their personal data that is inaccurate or incomplete.

11.2 The Charity shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Charity of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

11.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

12. Erasure of Personal Data

12.1 Data subjects have the right to request that the Charity erases the personal data it holds about them in the following circumstances:

12.1.1 It is no longer necessary for the Charity to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

12.1.2 The data subject wishes to withdraw their consent to the Charity holding and processing their personal data;

12.1.3 The data subject objects to the Charity holding and processing their personal data (and there is no overriding legitimate interest to allow the Charity to continue doing so)

12.1.4 The personal data has been processed unlawfully;

12.1.5 The personal data needs to be erased in order for the Charity to comply with a particular legal obligation

12.1.6 The personal data is being held and processed for the purpose of providing information society services to a child.

12.2 Unless the Charity has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

12.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

13. Restriction of Personal Data Processing

13.1 Data subjects may request that the Charity ceases processing the personal data it holds about them. If a data subject makes such a request, the Charity shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

13.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

14. Objections to Personal Data Processing

14.1 Data subjects have the right to object to the Charity processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

14.2 Where a data subject objects to the Charity processing their personal data based on its legitimate interests, the Charity shall cease such processing immediately, unless it can be demonstrated that the Charity's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

14.3 Where a data subject objects to the Charity processing their personal data for direct marketing purposes, the Charity shall cease such processing immediately.

14.4 Where a data subject objects to the Charity processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". The Charity is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

15. Data Security - Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

15.1 All emails containing written documentation of a personal nature must be encrypted

15.2 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

15.3 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

15.4 Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

15.5 All data taken and stored by staff working remotely must be securely stored at all time and at no time should any personal details be left visible to others.

16. Data Security - Storage

The Charity shall ensure that the following measures are taken with respect to the storage of personal data:

16.1 All electronic copies of personal data should be stored securely using passwords

16.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

16.3 All personal data stored electronically should be backed up with backups stored on a cloud based system.

16.4 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Charity or otherwise the Data Processor and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary

16.5 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Charity where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Charity that all suitable technical and organisational measures have been taken).

17. Data Security – Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Charity's Data Retention Policy.

18. Data Security - Use of Personal Data

The Charity shall ensure that the following measures are taken with respect to the use of personal data:

18.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Charity requires access to any personal data that they do not already have access to, such access should be formally requested from the CEO or Trustees

18.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Charity or not, without the authorisation of CEO or Trustees

18.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

18.4 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; and

19. Data Security - IT Security

The Charity shall ensure that the following measures are taken with respect to IT and information security:

19.1 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.

19.2 no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Charity, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

19.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date.

19.4 No software may be installed on any Charity-owned computer or device without the prior approval of the CEO or Trustees.

20. Organisational Measures

The Charity shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

20.1 All employees, agents, contractors, or other parties working on behalf of the Charity shall be made fully aware of both their individual responsibilities and the Charity's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

20.2 Only employees, agents, sub-contractors, or other parties working on behalf of the Charity that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Charity;

20.3 All employees, agents, contractors, or other parties working on behalf of the Charity handling personal data will be appropriately trained to do so;

20.4 All employees, agents, contractors, or other parties working on behalf of the Charity handling personal data will be appropriately supervised;

20.5 All employees, agents, contractors, or other parties working on behalf of the Charity handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

20.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

20.7 All personal data held by the Charity shall be reviewed periodically, as set out in the Charity's Data Retention Policy;

20.8 The performance of those employees, agents, contractors, or other parties working on behalf of the Charity handling personal data shall be regularly evaluated and reviewed;

20.9 All employees, agents, contractors, or other parties working on behalf of the Charity handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;

20.10 All agents, contractors, or other parties working on behalf of the Charity handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Charity arising out of this Policy and the GDPR; and

20.11 Where any agent, contractor or other party working on behalf of the Charity handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Charity against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

21. Data Breach Notification

21.1 All personal data breaches must be reported immediately to the Charity's Data Protection Officer.

21.2 If a personal data breach occurs and that breach is likely 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 Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

21.3 In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

21.4 Data breach notifications shall include the following information:

21.4.1 The categories and approximate number of data subjects concerned;

21.4.2 The categories and approximate number of personal data records concerned;

21.4.3 The name and contact details of the Charity's data protection officer (or other contact point where more information can be obtained);

21.4.4 The likely consequences of the breach;

21.4.5 Details of the measures taken, or proposed to be taken, by the Charity to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

22. Implementation of Policy

This Policy shall be deemed effective as of 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	Katie Sherjan
Position:	CEO
Date:	9th May 2018
Due for Review by:	9th May 2019
Signature: