TAUNTON HERITAGE TRUST
Data Protection Policy and Procedure

Introduction:
The purpose of this policy is to enable Taunton Heritage Trust to comply with the law (The General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018, in respect of the data it holds about individuals.

The Trust will ensure that the information it holds about its Residents, Grant Applicants, Trustees, Staff and all other service providers is used in accordance with the law. The Trust will only collect and use personal data in compliance with this Policy and the procedures set out below.
The Trust will:

- follow good practice.
- protect Residents, Trustees, Grant Applicants, Staff, Volunteers, and other individuals by respecting their rights.
- demonstrate an open and honest approach to personal data and
- protect the Trust from the consequences of a breach of its responsibilities.

This policy applies to all sensitive and personal information that we control and process relating to identifiable, living individuals including contact details, test and exam results, bank details, photographs, audio, and digital recording.

The Trust will comply with GDPR 2018 as follows:

1. **Transparency:** The Trust will be open and transparent in the way personal data is used and shared. There may be limited circumstances where the Trust does not have to comply with the transparency requirement but in such instances the Trust will obtain further advice from the ICO. Individuals will be provided with information about how their personal data is collected and stored.
2. **Collecting and using Personal Data for lawful purpose only:** The Trust will only collect and use the minimum amount of personal data if relevant for the purpose of the charity and where the Trust can rely on a lawful basis (or bases) and where the purposes have been identified in a privacy notice provided to individuals, for example in the application form for potential residents. When collecting personal data from individuals the Trust will ensure that the individuals are aware of the purposes for which the personal data will be used.
   In addition, when collecting personal data, the Trust will only collect those details which are necessary for the purposes for which that personal data is being obtained. Any use of personal data will be for the identified purposes and any different or new purposes will have a lawful basis. Personal data that is not necessary for any legitimate business purpose will <u>not</u> be collected or accessed.
   The Trust has identified that it has a legitimate interest in keeping personal data about Residents, as Trustees must be satisfied that each Resident qualifies as a beneficiary of the Trust in accordance with the Constitution dated 02 October 2018.
   The Trust considers the processing and storing of such personal data is necessary to comply with the Constitution. All personal data, including details of Residents' next of kin, will be stored securely, data on computers will be password protected and paper copies of data will be kept in a locked filing cabinet. Only authorised members of Staff and Trustees will have access to personal data.
3. **Privacy Impact Assessments and Privacy by Design:** The Trustees consider that the use of personal data is unlikely to result in significant risks for the rights and freedoms of individuals and therefore a Privacy Impact assessment is not necessary. The Trust will ensure that systems, databases and tools that collect and use personal data are designed to promote privacy protection.

4. **Ensuring data quality:** Processing inaccurate information can be harmful to individuals and the Trust. The main way of ensuring that personal data is kept accurate and up to date is by ensuring that the sources the Trust uses to obtain personal data are reliable. Individuals will be actively encouraged to inform the Trust should their personal data change.
   To ensure that personal data is accurate, it will generally be collected directly from individuals. All Residents will be actively encouraged to update their contact details by notifying the Trust of any changes in their personal data and understanding that it is their responsibility to do so.
5. **Retaining and disposing of data:** Any personal data must only be kept where there is a business or legal need to do so. When the Trust disposes of personal data, this will be undertaken in a secure manner.
   Documents (including paper and electronic versions and email) containing personal data will not be kept indefinitely and will always be securely deleted and destroyed once they have become obsolete or when that personal data is no longer required. Paper based documents will be shredded on site or disposed of externally as confidential waste. Electronic data will be permanently deleted from all drives and electronic media. Computer equipment that is surplus to requirements will be disposed of securely by a specialist contractor.
   Personal data will not be retained simply on the basis that it might come in useful one day without any clear view of when or why.
   The Trust's data retention policy is:
   The Trust will not keep personal data for longer than is necessary. This means that:
   - a Resident's file will be destroyed after five years of the Resident leaving or passing away.
   - records of complaints/investigations concerning Residents will be destroyed five years after the Resident leaves or passes away.
   - application forms for unsuccessful housing applicants will be destroyed immediately after they have been notified that they have been unsuccessful.
   - Trustees will destroy and delete all sensitive Trust documents held within their own records twelve months after receipt, including all computer data and paper copies.
   - Trustees' personal files will be destroyed five years after ceasing to be a Trustee.
   - Staff personal files will be destroyed 6 Years after employment ceases. (Legal Requirements for Document retention in the UK (legalo.co.uk)
   - Grant application forms will be held for a maximum of 2 years on the Trust's electronic filing system which is password protected and then securely deleted *or* in secure storage in a locked filing cabinet and then will be securely shredded.
6. **Honouring Individuals' rights:** The Trust will reply to queries and complaints from individuals about how the Trust uses their personal data within 30 days.
   Individuals are entitled by law (by making a request) to be supplied with a copy of any personal data held about them (including both electronic and paper records). Individuals are also entitled to know the logic involved in decisions made about them.
   An individual also has the right to seek erasure of their data and to request portability of their data i.e. that the Trust provides their data to them in a structured, commonly used and machine-readable format.
   Where the Trust receives a request from an individual exercising their legal right to control their personal data, the Trust will respond promptly. If a valid request concerns a change in that individual's personal data, such information will be rectified or updated, if appropriate to do so.
7. **Taking appropriate security measures:** Personal data will be kept secure. Technical, organisational, physical and administrative security measures (both computer system and non-computer system related steps) are necessary to prevent the unauthorised or unlawful processing or disclosure of personal data, and the accidental loss, destruction of, or damage to personal data. The Trust will monitor the level of security applied to personal data and take into account current standards and practices. As a minimum the Trust will ensure that:
   - Personal files for Residents, Trustees, and Staff are kept in a locked filing cabinet at all times with access only by authorised Staff.

- Applications for accommodation are kept in a locked filing cabinet at all times with access only by authorised Staff.
- Trustee's personal details are kept in a locked filing cabinet with access only by the Chief Officer, and the Chair of Trustees on request.
- Electronic files containing personal data are password protected and passwords will be changed on a regular basis.
- Backed up electronic data is held securely on an alternative site or when off-site it is encrypted, password protected and will only be accessed by named Staff.
- If any personal data is taken from the office (e.g. to work at home) the personal data will be held securely at all times whilst in transit and at the location where held.

Any suspicion of any data security breach should be reported immediately to the Chief Officer. When the Trust becomes aware of a breach, protective measures will be taken to effectively mitigate the consequences of the breach.

8. **Using Subcontractors and Vendors:** Under EU data protection law, where a provider of a service has access to personal data the Trust will impose strict contractual obligations dealing with the purposes and ways personal data may be used and the data security of that information. These are third parties who act as processors (i.e. only holding the personal data according to the Trust's instructions). Housing Benefit and Government offices are not vendors.
   The Trust will carry out appropriate due diligence on any potential third party to which personal data is being provided and ensure that the third party's Data Privacy Policy is adequate.
   The Trust will always enter into a written contract with any Vendor that deals with personal data being provided by the Trust. The contract will meet the requirements under the GDPR Article 28.
9. **Disclosure to Third parties:** At times, the Trust may disclose personal data to vendors, contractors, service providers and other selected third parties.
   Prior to disclosing personal data to these parties, the Trust will take reasonable steps to ensure that: (i) the disclosure of personal data is appropriate; (ii) the recipient of such information is identified; and (iii) where appropriate or required by law, the third party is contractually committed to complying with this Policy and/ or the Trust's instructions concerning the use of personal data as well as implementing appropriate security measures to protect personal data, limiting further use of personal data, and complying with applicable laws.
   In certain circumstances, the Trust may be required to disclose personal data to third parties when required by law, when necessary to protect the Trust's legal rights, or in an emergency situation where the health or security of an individual is endangered. Prior to such disclosures, the Trust will take steps to confirm that the personal data is disclosed only to authorised parties and that the disclosure is in accordance with this Policy and applicable law.
10. **Safeguarding the use of special categories of data:** Special categories of data is information revealing an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, processing of genetic data or biometric data (for the purpose of uniquely identifying an individual), health and sex life or sexual orientation. Since this information is more intrusive, the Trust will only use it where absolutely necessary and often with the explicit consent of the individual affected.
    The Trust will only hold and make available special categories of data on an individual without their explicit consent if the Trust has another lawful basis under applicable law. This may be the case, for example, where the Trust holds information about an individual's health where this is necessary to exercise any obligation conferred by law on us in connection with the Trust.
    For Residents, the Trust may also collect and use their special category data where:
    - Our use of their personal data is to provide support for a particular disability or medical condition.
    - Our use of their personal data is necessary to enable the provision of confidential counselling, advice or support.
    - Our use of their personal data is necessary for protecting an individual from negligence or physical, mental or emotional harm.

- Our use of their personal data is necessary for the purpose of protecting the economic well-being of an individual at economic risk.

The Trust will always assess whether special categories of data are essential for the proposed use and will only collect special categories of data when it is absolutely necessary in the context of the organisation. Application (or other) forms used to collect special categories of data will include suitable and explicit wording expressing the individual's consent when the Trust is collecting explicit data.

Consent must be demonstrable. Therefore, if it is collected verbally it will be recorded in such a form as to prove that the requisite information was provided to the individual and their response was able to be verified.

Where consent is not relied upon, the Trust will take steps to ensure that there is another lawful basis under applicable law for the collection and use of such information. In certain circumstances, the Trust may be required to consult with the Information Commissioner's Office about the proposed use of such special categories of data.

Data Protection Procedure

Data Storage and processing:

Taunton Heritage Trust recognises that data is held about:

- Residents
- Trustees/Associates
- Staff
- Volunteers
- Grant applicants

This information is always stored securely, and access is restricted to those who have a legitimate need to know. We are committed to ensuring that those about whom we store data understand how and why we keep that data and who may have access to it. We do not transfer data to third parties without the express consent of the individual concerned. Archived records are stored securely, and the Trust has clear guidelines for the retention of information as set out in Point 5 above.

Rights of individuals

All individuals who come into contact with the Trust have the following rights under the DPA:

- a right of access to a copy of their personal data
- a right to object to processing that is likely to cause or is causing damage or distress.
- a right to prevent processing for direct marketing.
- a right to object to decisions being taken by automated means.
- a right, in certain circumstances, to have inaccurate personal data rectified, blocked, erased, or destroyed and
- a right to claim compensation for damages caused by a breach of the DPA.

Roles and Responsibilities:

The Trustees recognise their overall responsibility for ensuring that the Trust complies with its legal obligations. The Chief Officer in association with the Compliance Officer is responsible as follows:

- briefing Trustees on Data Protection responsibilities
- reviewing Data Protection and related policies
- advising other Staff on Data Protection issues
- ensuring that Data Protection induction and training takes place.
- notification
- handling subject access requests.

All Trustees, Staff and Volunteers are required to read, understand, and accept any policies and procedures that relate to the personal data they may handle in the course of their roles.
Significant breaches of these policies will be handled under disciplinary procedures.

Key risks to the safety of data control and process:
The Trustees have identified the following potential key risks:

- breach of confidentiality (information being given out inappropriately).
- individuals being insufficiently informed about the use of their data.
- misuse of personal information by Staff or Volunteers.
- failure to up-date records promptly.
- poor IT security and
- direct or indirect, inadvertent, or deliberate unauthorised access.

The Trustees will review the Trust's procedures regularly, ensuring that the Trust's records remain accurate and consistent and in particular:

- IT systems will be designed, where possible, to encourage and facilitate the entry of accurate data.
- data on any individual will be held in as few places as necessary and Trustees and Staff will be discouraged from establishing unnecessary additional data sets.
- effective procedures will be in place so that relevant systems are updated when information about an individual changes.

Subject Access Requests
Any individual who wants to exercise their right to receive a copy of their personal data can do so by making a Subject Access Request, ('SAR') to the Chief Officer. The request must be made in writing and the individual must satisfy the Chief Officer of their identity before receiving access to any information. A SAR must be answered within 30 calendar days of receipt by the Trust.

Collecting and using personal data
The Trust typically collects and uses personal data in connection with the provision of its Constitution. The Trust collects personal data mainly in the following way:

- by asking applicants for accommodation to complete paper forms.
- by asking residents to give staff information verbally and by completing forms.
- by asking grant referral agencies to complete paper forms on behalf of applicants and then emailing them securely to the office.
- by asking Board & Staff applicants to complete papers forms.

The Trust will:

- not use any of the personal data it collects in ways that have unjustified adverse effects on the individuals concerned.
- be transparent about how it intends to use the data and give individuals appropriate privacy notices when collecting their personal data.
- handle people's personal data only in ways they would reasonably expect.
- not do anything unlawful with the data.

Keeping Data Secure
The Trust will take all appropriate measures to prevent unauthorised or unlawful processing of personal data and to protect personal data against loss, damage, or destruction. This means that:

- *personal files for Residents, Trustees, and Staff and applications for accommodation will be always kept in a locked filing cabinet with access only by authorised Staff.*
- *grant application forms will be saved securely on the Trust's electronic filing system which is password protected.*
- *Trustees' personal details will be kept in a locked filing cabinet with access only by the Chief Officer, and the Chair of Trustees on request.*
- *electronic files containing personal data will be password protected and passwords will be changed on a regular basis.*

- *backed up electronic data will be held securely on an alternative site or when off-site it will be encrypted, password protected and only accessed by named Staff.*
- *if any data is taken from the office (e.g. to work at home) the data must be always held securely whilst in transit and at the location the data is held.*

More information:
Full information about the Data Protection Act, its principles and definitions can be found at www.ico.org.uk

POLICY APPROVED DATE: _____2024_____

NEXT REVIEW DATE: _____2027_____

This policy is reviewed every three years.

c:\users\jan peake\tht dropbox\policies & procedures\current policies and procedures\organisational\data protection policy.docx