Perth and Kinross HERITAGE TRUST

Data Protection Policy

Adopted: May 2018

The Lodge
4 York Place
Perth
PH2 8EP
Scottish Charity No. SC003139

1 Introduction

Data protection legislation has existed in the UK for many years. In May 2018, a new piece of data protection legislation comes into force in the UK (replacing the Data Protection Act [1998]): the General Data Protection Regulation (GDPR). The new legislation extensively amends the provisions of the 1998 Act to better suit the 'internet-age'; there are stricter penalties for failure to comply. The GDPR applies to all data relating to, and descriptive of, living individuals defined in the GDPR as 'personal data'. Individuals are referred to as 'data subjects'. A summary of definitions is provided in section 4: for full definitions of terms used and the rights of data subjects please see the relevant sections of the Information Commissioner's Office (ICO) website (www.ico.org.uk).

2 Aim of this policy

This policy sets out the responsibilities of Perth and Kinross Heritage Trust (hereby referred to as 'the Trust'), its staff and its Trustees to ensure full compliance with the data protection legislation. It is for the information of staff, Trustees and Trust supporters and clients. This policy also incorporates the Trust's register of data processing which details the data collection, processing & retention plans.

3 Associated Policies

The following associated policies should be consulted in conjunction with the Data Protection Policy as appropriate.

- Volunteer and Outreach Policy
- Child Protection Policy

4 Definitions

Data Protection principles
The Trust will adhere to the six principles of data protection as stipulated in the GDPR, which means that information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The six principles are:

a) Personal data shall be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').
b) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes. Further processing for archiving, scientific or historical research or statistical purposes is permissible ('purpose limitation')
c) Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed ('data minimisation').
d) Personal data shall be accurate and where necessary kept up to date ('accuracy').
e) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose ('storage limitation').
f) Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Personal Data
Personal data is information about a living individual, who is identifiable from that information or who could be identified from that information when combined with other data which the Trust either holds or is likely to obtain. GDPR also refers separately to 'special categories' of personal data which includes particularly sensitive personal information such as health details, racial or ethnic origin or religious beliefs.

Data Subject Rights
The GDPR provides the following rights for individuals: The right to be informed • the right of access • the right to rectification • the right to erasure • the right to restrict processing • the right to data portability • the right to object • rights in relation to automated decision making and profiling.

Processing Data
The definition of 'processing data' includes obtaining/collecting, recording, holding, storing, organising, adapting, aligning, copying, transferring, combining, blocking, erasing and destroying the information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure.

5 General Policy Statement

To deliver the Trust's core functions, the Trust must create, collect, process and store personal data from a variety of data subjects including: Trustees & staff (both potential, current and former); clients; and supporters. The Trust currently processes personal data in accordance with the Data Protection Act (1998) and this will continue to be the case with the GDPR and any future amendments to Data Protection legislation.

The Trust holds personal data (on paper, computer or other media) in three data subject categories: **Supporters** of the Trust (e.g. prospective, active and past project volunteers); **Clients** (e.g. grant applicants and holders, meeting and conference delegates, customers and services suppliers); and **Staff & Trustees**. This data includes contact details, preferences, specific health information, age, name, address, telephone number and email address. We ensure this personal information is stored and processed in accordance with legal requirements and best practice. Other personal data may be captured when using the 'contact us' or other forms on our website and is governed by appropriate privacy notices published online.

Our use of personal data includes, but is not limited to: financial transactions with commercial customers; provision of advice to clients; maintaining a database of supporters' participating in Trust projects; claiming Gift Aid; fundraising; providing for the election of new Trustees; and facilitating communication between staff and data subjects. As the Trust processes 'personal data', it is defined as a Data Controller for the purposes of the GDPR. It is exempt from registration with the ICO on account of being established for not-for-profit making purposes and because it only processes information that is necessary to establish and maintain support and to provide or administer activities for people who are supporters of the organisation or have regular contact with it. The Trust also only shares processed data with people and organisations (third parties) that are strictly necessary for carrying out the organisation's activities and only keeps this information while the individual is a supporter or for as long as is necessary for supporter administration.

6. Data Security

All Trust staff are responsible for ensuring that the personal data they hold and use is maintained securely utilising file encryption/password protection. Staff will ensure that personal data is not disclosed to any unauthorised third party in any form either accidentally or otherwise. This will involve making use of anonymity options for electronic communications and evaluative reporting.

7. Data Retention, Consent and Privacy Notices

The GDPR places obligations on the Trust and the way it handles personal data. This means that personal data will only be processed if there is a valid (defined by GDPR as lawful) condition of processing (e.g. consent obtained from the data subject, or a contract with them) and we have provided information to the individuals concerned about how and why we are processing their information (i.e. a privacy notice).

DATA SUBJECT CATEGORY	LAWFUL BASIS FOR PROCESSING
Supporters	Legitimate interest / consent
Clients	Contract / Legitimate interest
Staff & Trustees	Legal Obligation (to comply with HMRC & OSCR requirements)

Personal data will only be retained for the length of time necessary to perform processing (e.g. duration of a project), while the individual remains a supporter of the Trust, or for as long as is necessary for Trust operations and governance. Once information is no longer needed it will be disposed of securely. Paper records will be shredded or disposed of in confidential waste and electronic records will be permanently deleted. The duration of personal data retention will vary depending on the purpose of its collection (3 years on average). In all cases, the data subject will be informed of the conditions of retention within a privacy notice issued at the point of collection and given the opportunity to offer or withhold their consent to its collection, use and/or retention. If data is fully anonymised then there is no time limit on storage from a data protection point of view.

8 Register of Data Processing

8.1 SUPPORTERS

Explanation of Lawful Basis: Supporter personal data is collected, processed and retained through consent and for legitimate interests. The legitimate interests are namely to share information of direct relevance and interest with the Trust's supporters, to maintain support and provide or administer activities for individuals who are supporters of the organisation or have regular contact with it. With consent, necessary donors' personal information will be shared with a third party (HMRC) to facilitate gift aid reclamation. All data will be held securely and only for as long as is strictly necessary for the Trust to fulfil core and project operational and administrative activities/ administration (e.g. project duration). Supporters will be contacted at the end of the project they have been involved in and offered the opportunity to have their data removed or to have it retained and be contacted about future Trust activities that may be of direct interest to them. Supporters will be contacted on a 3 yearly basis and invited to update their preferences; they are also free to have their personal data removed from record at any intermediate time.

PROCESSING PURPOSE	CATEGORY OF INDIVIDUAL	CATEGORY OF PERSONAL INFORMATION
Report distribution	Stakeholders	Contact details;

Project administration & evaluation	Vulnerable Individuals	Contact details; Carer details; Condition details; Emergency details
	Active Volunteers	Contact details; Emergency contact details; Relevant health conditions; age; Relevant vaccination details
	Potential Volunteers	Contact details; Demographic data
	Past Volunteers *(where specific consent has been granted to be notified of future activities)*	Contact details; Emergency contact details; Relevant health conditions; age; Relevant vaccination details
Claiming Gift Aid	Donors	Contact details

8.1.1 SUPPORTERS' SPECIAL CATEGORY DATA

When supporters register as project volunteers they will be asked to disclose more sensitive, special category data relating to their age and health conditions (mental or physical) that they feel may affect their ability to participate in project activities (e.g. manually exertive tasks such as archaeological excavation). This data is collected, strictly controlled, held securely and processed for the purpose of ensuring the health and safety of all activity participants and project staff. It will be used to provide additional information and offer support to the data subject as well as for risk assessing and implementing appropriate health and safety measures. Where a third party contractor is employed to deliver project activities, it may be necessary to share some special category data with the nominated volunteer supervisor, or in the case of an emergency with the first aid or emergency services responder, to ensure safe operations. Data subjects will always be informed of this policy at the point of data collection and given the opportunity to with-hold information they aren't comfortable sharing. Collection and processing of special category data will always be undertaken under the Article 6 lawful basis of consent and will only relate to vulnerable individuals, active and past volunteers. This data will also be processed under condition (d) of Article 9 of the GDPR which stipulates that: *"processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects."*

8.2 CLIENTS

Explanation of Lawful Basis: Client personal data is collected, retained and processed for contractual reasons, legitimate interests and with consent. The contractual basis applies in circumstances where a financial transaction takes place. Maintaining support and providing/ administering activities are the legitimate interests. Offering opportunities of direct relevance and benefit to clients is also a legitimate interest but will be supported by consent wherever possible. Grant recipients are the only clients whose personal information is shared with a third party, namely the Trust solicitor. This is carried out with consent and is part of a contractual grant agreement. Client personal data will be held securely and only for as long as necessary for the Trust to fulfil contractual obligations and to carry out organisation activities/administration.

PROCESSING PURPOSE	CATEGORY OF INDIVIDUAL	CATEGORY OF PERSONAL INFORMATION
Publication sales orders	Customers	Contact details; Financial details
Core & Project operations	Suppliers	Contact details; Financial details
	Contractors	Contact details; Financial details
Complaints Procedures	Complainants (e.g. vexatious)	Contact details;
Grant administration	Grant Enquirers	Contact details
	Grant Applicants	Contact details

	Grant Recipients	Contact details; Financial details
Direct marketing	Potential Grantees	Contact details; Property ownership
	Targeted Event Attendees	Contact details; Company of Employ
Event management	Customers	Contact details; Financial details
	Meeting/conference delegates	Contact details
	Activity participants	Contact details; relevant health details

8.3 STAFF & TRUSTEES

Explanation of Lawful Basis: Staff and Trustee personal data is collected, retained and processed to fulfil legal obligations pertaining to the operations and governance of the Trust. This includes sharing of personal information with third parties, namely HMRC, Companies House and the Office of the Scottish Charities Regulator (OSCR). It will be held securely and only for as long as necessary for the Trust to fulfil these requirements.

PROCESSING PURPOSE	CATEGORY OF INDIVIDUAL	CATEGORY OF PERSONAL INFORMATION
Staff/Trustee Recruitment	Applicants	Contact details; CV; Reference details
Staff administration	Employees	Contact details; Financial details
	Emergency Contacts	Contact details; Relationship to employee
Trustee administration	Board members	Contact details

9 Children

There are specific restrictions that apply to the processing of children's personal information under the GDPR, which are available at **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/.** The Trust does not gather personal data on any persons under the age of 16. The terms and conditions governing working relationships between children and staff are defined in the Trust's Child Protection Policy.

10 Direct Marketing

Direct marketing relates to communications (regardless of media) that deliver advertising or marketing material directly to individuals (e.g. fund raising requests, advertising courses, events or volunteering opportunities). The Trust will only maintain lists or databases of supporters and clients who have requested notification of upcoming/future opportunities (e.g. potential volunteers or grantees) related to their recorded interests or past/current participation. The Trust will always include an option for supporters and clients to easily withdraw from direct marketing and will ensure that such activities cease upon receipt of such a request.

11 Personal Data Breach

A personal data breach is defined in GDPR to mean "*a breach of security leading to the accidental or unlawful destruction, loss, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*".

The Trust is responsible for ensuring appropriate and proportionate security for the personal data that we hold. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. The Trust will make every effort to avoid personal data breaches, however, it is possible that mistakes will occur on occasions and external influences beyond the Trust's control could compromise the security of personal data that is held.

Examples of personal data breaches could include: Loss or theft of data or equipment • inappropriate access controls allowing unauthorised use • equipment failure • unauthorised disclosure (e.g. email sent to the incorrect recipient) • human error • hacking attack.

In the event of a data breach being discovered, the data processor will notify the Trust Director immediately. In accordance with the GDPR, any incident will then be reported to the Information Commissioner's Office by the Trust Director within 72 hours of receiving notification of the breach. All reasonable efforts will be made to contain a data breach, recover any losses and limit damage. Data subjects affected by a breach will be notified with specific and clear information on how their data has been compromised, the mitigation steps that have been put in place and where they can find advice on how to protect themselves.

Version V2: 09.05.18

Document prepared by: Gavin Lindsay, Research & Engagement Officer

Document authorised by: David Strachan, Director

Signed by: Sue Hendry, Chairman (with agreement of the Board of Trustees)

Signature: Sue Hendry

Date: 22nd May 2018