WORLD HERITAGE UK
DATA PROTECTION POLICY

April 2018

Next review due April 2019

Contents

Statement

Penelope Jane Gibson is the Trustee designated for oversight of Data Protection issues for the period April 2018 – March 2019

Chris Mahon, Development Director is responsible for control of data held by World Heritage UK.

This policy was approved at the meeting of the Board of Trustees of World Heritage UK on 11 April 2018

Signed:_____ Date: _____

Chair

1. Introduction

(i) World Heritage UK (*WH:UK*) is committed to managing the data which it holds to achieve the vision and aims of the organisation and following the Eight Principles of Data Protection

Namely:
1. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

2. Personal data shall be processed fairly and lawfully and shall not be processed unless –
(a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

3. Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

(ii) The Trustees of *WH:UK* have reviewed the data held by the organisation and its officers and the way that it is held and managed and is satisfied that this is being done so lawfully and in accordance with the guidelines of the Information Commissioner's Office (ICO) and the General Data Protection Regulations 2017.

(iii) One member of the Board of Trustees will be designated as maintaining oversight of the Data Protection Policy.
For the period April 2018 – March 2019 this person is Penelope Jane Gibson.

(iv) The Trustees of *WH:UK* will review this policy annually to ensure that procedures continue to comply with the guidelines of the ICO and the General Data Protection Regulations 2017.

(v) *WH:UK* has undertaken a self-assessment (https://ico.org.uk/for-organisations/register/self-assessment/) and determined that *WH:UK* does not need to register with ICO.

2. Definitions / glossary

Data Controller - means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed

Data Processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information and additional obligations under the EU General Data Protection Regulations

Data Subjects – The individual whose personal information is being held or processed by *WH:UK* for example: a client, an employee, or supporter.

Explicit consent – is a freely given, specific and informed agreement by an Individual / Organisation in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

Data Protection Officer is the responsible person who ensures compliance. This can be an internal or external resource, if external, there still needs to be a designated employee named as responsible.

Personal Data is what the Act covers, i.e. data that relates to an individual as opposed to a company.

Sensitive Personal Data is data that is subject to much higher levels of protection, such as racial or ethnic origin, religious beliefs, physical or mental health, trade union and political memberships, criminal records and offences and information about the subject's sexual life.

Data Protection Risk Register is the document and process that should exist in your charity – i.e. how you have identified weak spots and how you plan to mitigate the associated risks.

Data Protection Policy is where you document data and how you handle and protect it.

3. What data is held

(i) *WH:UK* holds the following data:

- Email, telephone numbers and postal addresses of individual members
- Email, telephone numbers and postal addresses of representatives of member organisations
- Email, telephone numbers and postal addresses of individuals and individuals who represent organisations who work with *WH:UK* such as Heritage Alliance
- Financial data including bank account details of payees of *WH:UK*

Data held by *WH:UK* is not "*Sensitive Personal Data*" as defined in the glossary at item 2 above. For example, WH:UK does not hold data about children, young people, or vulnerable adults. many of the details are publicly available as it relates to public roles where information can be found in the public domain. However, *WH:UK* acknowledges that it holds data on individual members which is not necessarily available from public sources and should therefore be protected.

(ii) Third parties acting on behalf of *WH:UK*

- WordPress (Ministry of Automattic Ltd) collects data on behalf of *WH:UK* in the course of its business. *WH:UK* has no access to this data and it is the responsibility of WordPress to maintain this data lawfully.
- Eventbrite UK Ltd collects emails, contact details and financial information on behalf of *WH:UK* for events and conferences. Email addresses are provided to *WH:UK* for the purpose of necessary communication with delegates for the management of its events. Eventbrite is responsible for maintaining any data it collects in accordance with the law.

4. Lawful purpose for holding the data

The data held by *WH:UK* is collected for the **legitimate purpose** of carrying out the services required as part of the membership of *WH:UK* – membership invoices, matters related to charity governance such as AGM and other members' meetings, notification of events and activities, keeping members up to date on current affairs as related to World Heritage, and correspondence related to peer support for *WH:UK* members.

5. How the data is managed and by whom

(i) Collection

Data is collected through the following means:

1) Membership application form
2) Gathered through correspondence with individuals working for member organisations
3) Internet searches
4) Gathered when members and non-members book for events organised by *WH:UK* and partners
5) Gathered through correspondence with partners and associated organisations whilst conducting the business of *WH:UK*

(ii) How data is held by WH:UK

1) Data is held in paper (membership application form, correspondence), electronically (membership application form, excel spreadsheet (database)) held on the computer of the Development Director and outlook contact list.
2) All data is stored on the personal computers of the *WH:UK* officers. These are password protected.
3) World Heritage UK is migrating all data to a Google Drive account which is only accessible to authorised persons.

(iii) Processes

1) The Development Director maintains a central database of members and associated organisations and individuals
2) The Finance Manager holds records related to membership invoices and individual payments through BACS and PayPal.
3) A central database is being developed in a Google Drive folder to which only Development Director, Chris Mahon and Finance Manager, Beth Thomas have access.
4) Any correspondence related to charity governance is created by the Secretary (Gillian Clarke) and circulated by the Development Director.
5) The Secretary only holds data on individuals that s/he deals with directly on individual matters.
6) The *WH:UK* website has an option to "follow" and receive regular updates generated through WordPress. WH:UK has no access to this database.
7) A privacy notice will be sent out to all members on an annual basis and included on membership application forms.
8) A privacy notice will be displayed on the WH:UK website (https://worldheritageuk.org).

(iv) Deletion of data

1) Any individual who is no longer a member of WH:UK will be deleted from the central database within 6 months of the end of the membership year (April – March).
2) Paper copies of the membership application form will be shredded.
3) Electronic versions of the membership application form will be deleted from the central Google Drive folder and from the records held by the Finance Manager for the purposes of administering membership fees and income.

(v) Sharing of data

1) Data held by *WH:UK* may be shared within officers and Trustees to enable the business of WH:UK to be carried out.
2) *WH:UK* will not share data with third parties unless required to do so or permitted by law.

6. How data is protected

1) Officers of WH:UK will maintain one database that can only be accessed by authorised persons
2) Database is stored on Google Drive
3) Training of officers so that data is not shared with 3rd parties in contravention of the Data Protection Policy of *WH:UK* and GDPR
4) Data should not generally be placed on portable media. If this is necessary, then the file must be password protected
5) Requiring members to provide confirmation annually with membership payment that they consent to have their data stored and recording this in the central database.

7. How requests for information on data held on an individual are handled

1) Any request by a data subject to obtain a copy of their personal data held by *WH:UK* should be directed to the Development Director.
2) Confirmation of identity will be required and WH:UK may charge a fee of no more than £10.
3) A written list of the information held by WH:UK on the data subject will be provided to them within 1 calendar month of the request.

8. How data breaches are handled

1) Data breaches must be reported to the Trustees of *WH:UK* at the first available instance.
2) Any breach will be investigated by the Trustee designated as having oversight of the Data Protection Policy. He/she will determine the nature of the breach, who has been affected and any further measures required to rectify any consequences including recommendations on how to improve the procedures so that the breach cannot occur again.
3) Those people affected by the data breach will be contacted to inform of the nature of the breach, what action is taking *WH:UK* and any possible consequences of the data breach.
4) The breach will be reported to the ICO.
5) A data breach may be considered gross misconduct and the officer dismissed or Trustee asked to resign.