Contents
1. Introduction .................................................................................................................. 3
   Purpose of Data Protection Policy ................................................................................. 3
   World Heritage UK ........................................................................................................ 3
   Security of personal information .................................................................................. 3
   Individual rights on personal information ................................................................. 3
   Changes to this Policy ................................................................................................... 3
   Statement ....................................................................................................................... 3
2. Definitions / glossary ................................................................................................... 5
3. What data is held ......................................................................................................... 5
4. Lawful purpose for holding the data ........................................................................... 6
5. How the data is managed and by whom ................................................................. 6
   (i) Collection .............................................................................................................. 6
   (ii) How data is held by WH:UK ................................................................................ 6
   (iii) Processes ............................................................................................................. 7
   (iv) Deletion of data .................................................................................................... 7
   (v) Sharing of data ...................................................................................................... 7
6. How data is protected .................................................................................................. 7
7. How data subject access requests are handled ........................................................ 8
8. How data breaches are handled ................................................................................ 8
Appendix One - Data breach procedure ...................................................................... 9
Appendix Two - Data Breach flowchart .................................................................... 11

World Heritage UK
Registered Office
c/o Ironbridge Gorge Museum Trust
Coach Road
Coalbrookdale
Telford TF8 7DQ

Chris Mahon, Development Director
chris.mahon@worldheritageuk.org
1. Introduction

Purpose of Data Protection Policy
World Heritage UK (WH:UK) is committed to protecting personal information of and being transparent about what information it holds. WH:UK will use information that it collects in accordance with the General Data Protection Regulation 2016 and Data Protection Act 2018.

Using personal information allows WH:UK to develop a better understanding of its members, partners, employees and any other individual that it may come into contact with. In this way, WH:UK aims to provide relevant and timely information about the work that it does. As a charity, it also helps WH:UK to engage with potential donors and supporters. It ensures that it fulfils its obligations as an employer.

WH:UK aims to be clear when it collects personal information and only to process that data in a way that might reasonably be expected.

WH:UK uses personal information in accordance with all applicable laws concerning the protection of personal information. This document explains:
- What information WH:UK may collect
- How WH:UK may use that information
- In what situations WH:UK may disclose information to third parties
- How WH:UK keeps personal information secure, how WH:UK maintains it and the rights of individuals to be able to access it

World Heritage UK
World Heritage UK is a Charitable Incorporated Organisation registered in England and Wales (no. 1163364).

The Data Controller is Chris Mahon, Development Director on behalf of the Trustees of World Heritage UK.

Security of personal information
WH:UK will put in place appropriate safeguards (both in terms of its procedures and the technology it uses) to keep personal information as secure as possible. WH:UK will ensure that any third parties it uses for processing personal information do the same.

Individual rights on personal information
Any individual has the right to request a copy of the personal information that WH:UK holds about them and to have any inaccuracies in this data corrected. The contact details on page 2 of this Policy should be used to exercise this right. For further information on the rights of individuals, please see the Information Commissioners Office (ICO) website.

Changes to this Policy
WH:UK may need to change this Policy from time to time. WH:UK will alert individuals to material changes by, for example, placing a notice on its website and/or by sending individuals an email when required to do so by applicable law. The date on which the Policy was last updated is at the top of this document.

Statement
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 Principles of Data Protection.

Namely:
(a) processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness,
(b) 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 (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 individuals (‘storage limitation’);

(f) 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 (‘integrity and confidentiality’).”

(i) 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 ICO, the Data Protection Act 2018 and the General Data Protection Regulations 2016.

(ii) One member of the Board of Trustees will be designated as maintaining oversight of the Data Protection Policy.

For the period April 2019– March 2020 this person is Penelope Jane Gibson.

(iii) The Trustees of WH:UK will review this policy annually to ensure that procedures continue to comply with the guidelines of the ICO, the Data Protection Act 2018 and the General Data Protection Regulation 2016.

(iv) 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.

Penelope Jane Gibson is the Trustee designated for oversight of Data Protection issues for the period April 2019 – March 2020

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 17 September 2019

Signed: ____________________  Date: ____________________

Tony Crouch, Chair
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 2018** – 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 relevant to the work of **WH:UK** such as Heritage Alliance
- Email, telephone numbers and postal addresses of those who have expressed interest in the work of **WH:UK**
- Financial data including bank account details of payees of **WH:UK**
- Personal information about employees

Whilst the majority of information collected and processed by **WH:UK** is limited in nature and much is not covered under the data protection regulations, personal data is held on individual members and information collected about its employees may include Sensitive data as defined at Section 2 above.
Third parties acting on behalf of *WH:UK*

- **WordPress (Ministry of Automattic Ltd)** collects data on behalf of *WH:UK* through the ‘follow me’ facility. *WH:UK* has no access to this data and it is the responsibility of WordPress to maintain this data lawfully.
- **MailChimp (The Rocket Science Group, LLC)** data is shared with MailChimp when sending out e-newsletters to members and supporters. This newsletter is sent to those who have expressed an interest in the work of *WH:UK* and to heritage organisations and individuals relevant to its work. They can unsubscribe from this at any time.
- **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.
- *WH:UK* may employ third parties such as consultants to undertake research on their behalf. Where information held by *WH:UK* is shared for these purposes an appropriate data sharing agreement will be put in place and *WH:UK* will inform those affected in advance.
- *WH:UK* employs a third party (Chappell Associates) to process payroll information.

4. **Lawful purpose for holding the data**
The data held by *WH:UK* is collected and processed in the legitimate interest of *WH:UK* to carry out its business including (but not exclusively) 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 of *WH:UK* members.

In the case of employees of *WH:UK* this data is collected, held and processed to fulfil the lawful basis of **Contract** and for **Legal Obligation** as required by statutory authorities.

5. **How the data is managed and by whom**

(i) **Collection**

Personal 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*
6. Information gathered by officers and trustees, third parties and consultants undertaking research as part of the work of *WH:UK* which may include personal data
7. Information provided by employees as part of the recruitment process and as required to fulfil contractual obligations

(ii) **How data is held by *WH:UK***

1. Data is held on paper (membership application form, correspondence), electronically (membership application form, excel spreadsheet (database).
2. Data is held on the personal computers of the *WH:UK* officers. These are password protected.
3. Data is held on a central database that is accessed by the Development Director, Finance Manager, Beth Thomas and others as authorised by the Trustees.
4. Data held on employees of *WH:UK* is held on computers of the Finance Manager, Development Director and relevant trustees.
(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 held to which only Development Director and Finance Manager, and others as authorised by the Trustees have access. The database is used for communications to members and other individuals and organisations that WH:UK believes are interested in its work.
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) The Data Protection Policy will be displayed on the WH:UK website (https://worldheritageuk.org).
9) Any correspondence using personal information will be sent by Development Director or others authorised by him and in accordance with the Data Protection Policy.
10) All information held on an employee’s personnel file will be treated in the strictest confidence. Records may include information in relation to sickness absence, including records concerning the reasons for absences and any related medical reports obtained by WH:UK.

(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 folder and from the records held by the Finance Manager for the purposes of administering membership fees and income.
4) Data gathered through any recruitment process will be retained for 6 months and then destroyed.

(v) Sharing of data
1) Data held by WH:UK may be shared by officers and Trustees and their agents to enable the business of WH:UK to be carried out.
2) Data may be shared with third parties such as consultants and researchers as authorised by the Board of Trustees and where there is a data sharing agreement in place.
3) Data is shared with Chappell Associates for the purposes of processing salary and related information of employees.
4) Data is shared with HMRC and other government bodies in relation to employment of officers of WH:UK.
5) WH:UK will not share data with third parties in any other circumstance unless required to do so or permitted by law.

6. How data is protected
1) Data held by WH:UK can only be accessed by authorised persons.
2) All databases are password protected.
3) Officers and trustees are reminded annually of their responsibilities and best practice as part of the annual review process.
4) Data should not generally be placed on portable media. If this is necessary, then the file
must be password protected.
5) Members are asked to update their membership details on an annual basis on an application form which includes a privacy statement.

7. **How data subject access requests 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) 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**

   A data breach is defined as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data”.

   1) Any data breach must be reported to the designated Data Protection Trustee and Development Director as soon as it is discovered.
   2) Any breach will be investigated by the designated Data Protection Trustee. He/she will determine the nature of the breach, who has been affected and assess the risk to the individuals concerned and to *WH:UK*.
   3) The designated Data Protection Trustee will inform the Chair and consult as necessary.
   4) If the breach is deemed to have led to a risk to the rights and freedoms of individuals the ICO will be informed within 72 hours of the data breach being discovered.
   5) The individuals concerned will be informed as appropriate. They will be informed of the nature of the breach, what action *WH:UK* is taking and any possible consequences of the data breach.
   6) The Data Protection Trustee may recommend further measures to rectify any consequences including recommendations on how to improve the procedures so that the breach cannot occur again.
   7) The breach, the details and what action was taken, and any follow up actions are recorded in the *WH:UK* data log.
   8) Data breaches must be reported to the Trustees of *WH:UK* at the first available instance.
   9) A data breach may be considered gross misconduct and the officer dismissed or Trustee asked to resign.

Appendix One - Data breach procedure

1. **IF A DATA BREACH IS SUSPECTED OR REPORTED**
   - Inform designated Data Protection Trustee
   - Inform Data Controller, the Development Director
   - Inform Chair of Trustees

2. **CONTAIN THE BREACH**
   - Stop the breach if appropriate. This may include changing passwords or stopping any further processing.
   - Consider who will need to be informed, including the ICO, the data subjects, industry regulators and the police.

3. **ASSESS THE RISK**
   How can the breach cause harm to:
   - To the business
   - To staff
   - To reputation
   - To data subjects?
   - How many people could be affected and how many records? (one person might have multiple records and one record might mention multiple people)
   - What type of data has been breached?
   - How sensitive is the data?
   - Could this breach lead to distress, financial or even physical harm?
   - Will the breach affect the rights and freedoms of the individuals’ concerned?
   - Are there any mitigating factors?
     o Are there any safeguards in place that could lower the risk? For example, is the data encrypted?
     o Has it gone to a trusted body?
     o Are there more safeguards you can put in place now?

4. **NOTIFICATION**
   Are you required to inform ICO?
   This decision is on a case by case basis depending on the nature of the breach.

   Notify data subjects if appropriate based on the risk assessment undertaken.

   Trustees should be informed at an appropriate time which may be the next Trustees meeting.

<table>
<thead>
<tr>
<th>The ICO require the following information when reporting an incident:</th>
</tr>
</thead>
<tbody>
<tr>
<td>the nature of the personal data breach including, where possible;</td>
</tr>
<tr>
<td>the categories and approximate number of individuals concerned;</td>
</tr>
<tr>
<td>the categories and approximate number of personal data records concerned;</td>
</tr>
<tr>
<td>the name and contact details of the data protection officer (if you have one) or other contact point where more information can be obtained;</td>
</tr>
<tr>
<td>a description of the likely consequences of the personal data breach; and</td>
</tr>
<tr>
<td>a description of the measures you have taken, or propose to take, to deal with the personal data breach and, where appropriate, of the measures you have taken to mitigate any possible adverse effects.</td>
</tr>
</tbody>
</table>
APPENDIX 1

5. RECORDING INCIDENTS
All incidents should be logged in WH:UK Data Log

6. LEARNING FROM THE INCIDENT
• What can be learned from the incident?
• What follow up actions are required?
• Is further training required?
• Should the guidance be improved?
• Do security measures need to be improved?
• Can this type of incident happen again?
• Does the Data Protection Policy need to be updated?
Appendix Two - Data Breach flowchart

World Heritage UK Data Breach Procedure Flowchart

- Has there been a data breach?
  - Yes: Report to DP Trustee
    - Carry out risk assessment
  - No: Is the breach reportable to ICO?
    - Yes: Report to ICO & inform Trustees
    - No: Do the individuals need to be informed?
      - Yes: Inform Trustees
      - No: Carry out further remedial action as required
    - No: Record incident
- Review DP Policy and take action as appropriate to prevent incident reoccurring
- Inform Trustees