Borden Heritage Group Data Protection Policy

1. Introduction

Borden Heritage Group (BHG) is committed to adhering to the Data Protection Act 2018 (DPA) and the General Data Protection Regulations (GDPR).

BHG maintain personal data information about members, speakers, recorded guests and other individuals involved in heritage business.

This policy identifies how BHG manages the protection of personal data and ensures that those members whom have access to such data understand the rules governing the handling of that personal information.

The nominated Data Protection Officer has overall responsibility for the implementation of this policy ensuring members adhere to these procedures.

BHG must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that BHG should not process personal data unless the individual whose details the committee are processing has consented to this happening.

2. The Data Protection Officer Responsibilities.

The Data Protection Officer will: -

i. Keep the members updated about data protection responsibilities, risks, and issues.
ii. Review all data protection procedures and this policy on a regular basis.
iii. Where required arrange data protection training, advice and answer questions on data protection from members, speakers and other interested parties.
iv. Be responsible for responding to individuals who wish to know which data is being held on them by BHG.
v. Check and approve with third parties that handle BHG's data any contracts or agreement regarding data processing.
vi. Ensure all systems, services, software and equipment meet acceptable security standards.
vii. Check any security hardware and software regularly used by BHG to ensure it is functioning properly.

viii. Address data protection enquiries from persons connected to BHG business.

3. Committee & Members Responsibilities

The committee and members will: -

i. Ensure the BHG website displays a Privacy Notice relating to data protection.

ii. Where BHG process sensitive personal data the committee will ensure that the data subject has consented to this action. This consent need not apply in an instance required by law. Subject consent will identify what the relevant data is, why it is being processed and to whom it will be disclosed.

iii. Ensure that any personal data that the BHG process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained.

iv. Ensure that data collected by BHG is subject to active consent from the individual concerned and which that person can revoke at any time unless bound by a legal requirement.

v. Guarantee that all personal data is secure against loss or misuse.

vi. Where other organisations process personal data as a service on behalf of BHG, the member will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

vii. Ensure that where data is stored on printed paper, it should be kept in a secure place where unauthorised persons cannot access it. Where that printed paper is no longer required it should be competently shredded immediately.

viii. Ensure that where data is stored on a computer it should be protected by strong passwords that are changed regularly. A password manager will be used to create and store their passwords.

ix. Make certain that data stored on CDs or memory sticks must be locked away securely when they are not being used.

x. Ensure that any Firewall software that comes with any network access device should be set to high security mode and any personal data stored in hard copy format should be stored in a secure location.

xi. Ensure that personal data is retained for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, but should be determined in a manner consistent with these data retention guidelines.

xii. Not forward on emails or email threads that may contain personal data.

xiii. Inform the Data Protection Officer of any data breaches within the organisation as soon as practicable.

4. Subject Information Access Request

The DPA and GDPR identify that individuals are entitled, subject to certain exceptions, to request access to information about them. If a subject access request is received, the receiving member will refer the request to the Chairman or nominated Data Protection Officer.

If you as the reader of this document would like to correct or request information that BHG holds about you then please contact the Chairman or Data Protection Officer.

5. Breaches of the DPA or GDPR

All members have an obligation to report actual or potential data protection compliance failures. This allows BHG to investigate the failure and take remedial steps if necessary and notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right, or as part of a pattern of failures

6. Data Portability Upon Request

A data subject should have the right to receive a copy of their data in a structured format. These requests should be processed as soon as practicable provided it does not compromise the privacy of other individuals.

A data subject may also request that their data is transferred directly to another system which will be assisted providing there is no unreasonable cost or time factor.

7. Individual Right To Be Removed

A data subject may request that any information held on them is deleted or removed, and any third parties who process or the use that data must also comply with the request. An erasure request can only be refused if a legal exemption applies.

8. Processing Data & Marketing

Members should abide by any request from an individual not to the use their personal data for direct marketing purposes and notify the Data Protection Officer about any such request.

Direct marketing material must not be sent to someone electronically (e.g. via email, mobile phone or other electrical system) unless BHG has an existing business relationship with them in relation to the services being marketed.

9. Data Audit, Registering & Monitoring

A regular data audit and compiled register should be maintained to manage and mitigate DPA and GDPR breach risks. The data register will contain information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

All members particularly those involved in collating data must observe this policy.

The Data Protection Officer will monitor the implementation of the policy regularly to make sure it is being adhered to.