Privacy and Information Security Policy

Privacy Policy

Washburn Heritage Centre is committed to protecting the privacy of all visitors to this web-site. Any and all information collected is used exclusively to facilitate services provided. We will not communicate with you unless you expressly request it and will not share, sell or divulge any personal information.

Our website or any subsequent email correspondence may contain links to other sites. We do not share personal information with those sites and are not responsible for their privacy practices.

Types of information automatically collected

We collect data through two forms on this website, Enquiries and Newsletter sign-up, These forms gather data including name, telephone number, email address and postal address. This data is entirely voluntary and only used in business communication. **We do not share it with any third party.**

The Washburn Heritage Centre complies fully with General Data Protection legislation (GDPR). We recognise the rights of individuals to make sure their data is held securely, correctly, and lawfully.

Information Security Policy

1. The Washburn Heritage Centre (WHC) gathers and stores the following data:

1.1. For WHC suppliers

- Contact details: including some but not necessarily all of telephone number, email address, postal address. This data is stored electronically both on hard drive and in the cloud. It is accessed by the Heritage Centre Administrator, the Chairman and the Treasurer.

1.2. For WHC volunteers

- Contact details: including some but not necessarily all of telephone number, email address, postal address. This data is stored electronically both on hard drive and in the cloud.
- Contact details for next of kin. This is kept as hard copy and electronically on hard drive.
- Records relating to rota participation and event management. This is kept electronically in the cloud.

1.3. For attendees of WHC Events

- Contact details: including some but not necessarily all of telephone number, email address, postal address.
- Dietary requirements where appropriate
- Records of events attended including dates and payments made.

This data is stored electronically in the cloud.

1.4. For WHC members (in addition to the information kept for attendees as in 1.3 above)

- The date of enrolment
- Records of subscriptions paid (dates, amounts and how they are paid) and whether they are Gift Aided and if the tax has been reclaimed.
- Date at which their membership ceases

This data is stored electronically in the cloud.

2. The following people have direct access to data relating to volunteers, members and attendees (1.2, 1.3 and 1.4 above) via WHC or personal computer linked to the data stored in the cloud:
   - Heritage Centre Administrator
   - Treasurer (Member of the WHC Management Committee)
   - Volunteer Manager (Member of the WHC Management Committee)

   Event Lead Volunteers have access to lists of names and limited contact details for event attendees at the time of an event.

Data Processor	Data	Reason for access	How is the data accessed
Lead Volunteer	Names and limited contact details for event attendees	Management of event	Printed paper copy
Heritage Centre Administrator	All data listed in 1.1, 1.2, 1.3 and 1.4 above	General administration of WHC events, premises and membership	Electronically via laptop linked to cloud.
Treasurer	Data listed in 1.2, 1.3 and 1.4 above	Maintenance of data systems	Electronically via laptop linked to cloud.
Volunteer Manager	Data listed in 1.2, 1.3 and 1.4 above	Management of Volunteer rotas	Electronically via laptop linked to cloud.

3. The WHC does not share any data with Third Parties.

4. Data Retention: the organisation has been operating for 7 years. All data collected as listed in section 1 has been retained. A review will be made after 10 years of the retention policy for data.

5. Data Security
   5.1. Access to cloud based data requires passwords known only to the Heritage Centre Administrator, Data Systems Manager and Volunteer Manager.
   5.2. Hard copy of sensitive data is kept in a locked office.

6. Breaches of data security should be reported to the Chair *Ian Bergel.*

7. All processing of data is done internally, no third party data processors are used.