Friends of PENDLE HERITAGE

Privacy Policy

Whilst we are exempt from registering for The General Data Protection Regulations (GDPR) we respect the privacy of our members and employ best practice to adhere to the principles of the Data Protection Act 1998.

Electronic data is stored on a password protected spreadsheet which is maintained by the Membership Secretary and new information forwarded to the Treasurer. Amendments to personal details will be made in a timely manner and earlier copies will be deleted by both parties, including the copy in the recycle bin. This information is required to maintain contact with our members and may include members' names, postal and email addresses, telephone numbers and subscription records including Gift Aid authority. Original copies of application forms are retained for 12 months after their membership ends. Signed Gift Aid forms and Photography Consent forms will be kept securely by the Membership Secretary.

Names and email addresses for bulk communication are stored on password protected online software created by Mail Chimp and can only be accessed by the Publicity Officer and a designated member of PAG. A facility to opt out of further communications is available on the recipient's email. Sub groups e.g. Pendle Archaeology Group will obtain permission from their members to share details with other members of the group. In the event of application for an organised trip, the contact details of the applicant(s) will be retained by the trip organisers and deleted afterwards.

We will not share personal details without the permission of the individual concerned. Individuals have the right to view their personal data and we will respond to all requests to do so in a timely manner.

Members' personal information will be stored as long as they are members. If a member's subscription is not paid within 60 days of the due date, their details will be archived for 12 months to enable them to reinstate their membership. If membership is not renewed the record will be deleted.

Passwords will be changed immediately following the resignation of an authorised user.

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, we will promptly assess the risk to people’s rights and freedoms.

Last review July 2021.