

Data Protection Policy Acklington Village Hall

Personal data is information about a person which is identifiable as being about them. It can be stored electronically or on paper and includes images and audio recordings as well as written information.

Data protection is about how we, as an organisation, ensure we protect the rights and privacy of individuals, and comply with the law, when collecting, storing, using, amending, sharing, destroying or deleting personal data.

The Information Commissioner's Office has set out 7 key principles (see Appendix 1) that lie at the heart of the approach to processing personal data.

Responsibility

Overall and final responsibility for data protection lies with the Acklington Village Hall Trustees, who are responsible for overseeing activities and ensuring this policy is upheld.

All trustees and volunteers are responsible for observing this policy, and related procedures, in all areas of their work for the Hall.

Policy Statement

We will collect, store, use, amend, share, destroy or delete personal data only in ways which protect people's privacy and comply with the UK General Data Protection Regulation (GDPR) and other relevant legislation.

We will only collect, store and use the minimum amount of personal data that we need and will not collect, store or use data we do not need. We will not collect or store sensitive personal data nor special category data.

We will provide individuals with details of the data we have about them when requested by the relevant individual.

We will delete data if requested by the relevant individual, unless we need to keep it for legal reasons.

We will endeavour to keep personal data up-to-date and accurate.

We will store personal data securely and endeavour not to have data breaches.

We will keep clear records of the purposes of collecting and holding specific data, to ensure it is only used for these purposes.

We will not share personal data with third parties without the explicit consent of the relevant individual, unless legally required to do so.

Data Held

We hold no personal data on our own files except for details of our trustees, those whom we pay for services and personal data required for financial purposes.

The names and email addresses and in some cases telephone numbers of current and former local hall users with whom we have previously been in contact with are held on our email accounts and are not disclosed by us to any third party without their express consent.

Personal data including names, addresses, email addresses and telephone numbers as may be supplied by those booking the hall are held and processed by hallbookingonline.com managed by Fen Street Designs (see Appendix 2) and such personal data is used for managing bookings, invoicing and accounting purposes by the Trustees. Such details are not disclosed by us to any other third party.

All personal data held on IT systems, memory sticks or files must be password protected.

We do not retain any credit/debit card details supplied to us by telephone by persons booking our facilities or events.

Personal data consisting of names and addresses may be recorded in the Accident Book when required and this will be checked regularly. When personal data has been recorded in the Accident Book the relevant page(s) are removed and stored securely.

Details of the personal data held are shown in Appendix 3.

Any person wishing to check upon or seek removal of their details held on our email and booking systems should email their request to acklingtonvh@gmail.com

Data breach

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Any data breach (such as the loss of a laptop holding personal data or accident book) must be reported to the Treasurer or Chair as soon as possible.

Complaints Procedure

If you believe that Acklington Village Hall has not complied with data legislation or the commitments undertaken in this Data Protection policy, please put your complaint in writing to acklingtonvh@gmail.com. As required by the Information Commissioner's Office, we will endeavour to respond to your complaint within one calendar month, although complex requests may take up to 3 months to respond to.

Practical information about your data protection and information rights can be found at <https://ico.org.uk/>.

Appendix 1

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

“(a) processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’);

(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’).”

Article 5(2) adds that:

“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).”

Appendix 2

Hall Booking Online Privacy information

The calendar of bookings does not display the contact information for hirers.

The default level of privacy for the bookings is to Hide Contact Details so that only event info is accessible to the public. Hirers can also choose not to display the event title and list the event as a private event.

For hirers making one-off bookings who haven't created an account, he/she needs to choose a password. This is used by the hirer to make changes to a booking, or to delete it altogether. If an event password is lost and needed again, an administrator can set a new password.

All passwords (event, administrator and override) are encrypted. It isn't realistically possible to decrypt the password.

Hall Booking Online does not pass on any information from the bookings database to third parties. We also do not have any third-party advertising on the site.

As with most websites, they use cookies. These are used for two reasons:

- 1) To allow the Administrators to log in.
- 2) To optimise the site by keeping a general record of site usage.

Cookies don't identify individual users and are not used for advertising purposes

Appendix 3 Personal Data Audit



Acklington village hall
Data Audit January 20