

HARRISTON VILLAGE HALL GDPR POLICY

General Data Protection Regulations (GDPR)

Harriston Village Hall is legally obliged to follow certain rules relating to any personal data that it stores or uses, whether in hard copy or on a computer, memory stick, disc or mobile phone.

This policy sets out the guidelines that all volunteers must follow to comply with those legal rules.

What personal data is covered?

- Paper files – hire agreements.
- Volunteer and user personal details (names, addresses, telephone numbers and email in paper files and on computer.
- Photographs of users taken for website or advertising material – stored on phones/computer/memory stick or disc.

Obligations for personal data

1. Personal data must only be kept for the purposes it is collected for and not used for any other purposes.
2. The personal data is confidential and must be stored safely and securely:
 - the personal data must not be shown or given to any third party
 - any computer or mobile phone holding any of the personal data must be protected by a secure pass code.
3. The personal data must not be kept for longer than is necessary:
 - personal details will be deleted immediately on request.
4. Anyone handling hire agreements or using RVH contact lists will be briefed by a Committee member on the importance of confidentiality and of ensuring that the users understand what they are signing and what their rights are.
5. Emails to lists of people should use the blind copy (bcc) function to ensure confidentiality of email addresses.
6. The Data Protection Lead appointed by the Committee will carry out an annual review to ensure that this policy is being followed and that all volunteers/users are aware of it.
7. A copy of this policy will be sent out annually to all volunteers/users.

Data Protection Policy

HARRISTON VILLAGE HALL

Last updated **23rd November 2020**

Definitions

Charity means Harriston Village Hall a registered charity.

GDPR means the General Data Protection Regulation.

Responsible Person means Janice Barker/Henry Barker/Nathaniel Gunter

Register of Systems means a register of all systems or contexts in which personal data is processed by the Charity.

1. Data protection principles

The Charity is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

- a. processed lawfully, fairly and in a transparent manner in relation to individuals.
- 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 incompatible with the initial purposes.
- c. adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- 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;
- 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.
- 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.”

2. General provisions

- a. This policy applies to all personal data processed by the Charity.
- b. The Responsible Person shall take responsibility for the Charity’s ongoing compliance with this policy.
- c. This policy shall be reviewed at least annually.
- d. The Charity shall register with the Information Commissioner’s Office as an organisation that processes personal data.

3. Lawful, fair, and transparent processing

- a. To ensure its processing of data is lawful, fair, and transparent, the Charity shall maintain adequate records.
- b. These records shall be reviewed at least annually.

c. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the charity must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task, or legitimate interests.

b. The Charity shall note the appropriate lawful basis under which data is held in its records.

c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Charity's systems.

5. Data minimisation

a. The Charity shall ensure that personal data are adequate, relevant, and limited to what the Charity shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. The Charity shall take reasonable steps to ensure personal data is accurate.

b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Charity shall put in place an archiving policy for each area in which personal data is processed and review this process annually.

b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

a. The Charity shall ensure that personal data is stored securely using modern software that is kept-up to date.

b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

c. When personal data is deleted this should be done safely such that the data is irrecoverable.

d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

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, the Charity shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.