DATA PROTECTION POLICY & PROCEDURES

SIXPENNY HANDLEY VILLAGE HALL (SHVH)

Reviewed: 24/02/2026

We are committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of personal data in order to carry on our work of managing Sixpenny Handley Village Hall (SHVH). This personal information must be collected and handled securely.

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 govern the use of information about people (personal data). Personal data can be held on computers, laptops, mobile devices, or in manual files, and includes email, minutes of meetings, and photographs.

The charity will remain the Data Controller for the information held. Trustees, staff and volunteers are personally responsible for processing and using personal information in accordance with UK GDPR and the Data Protection Act 2018.

Trustees, staff and volunteers who have access to personal information will therefore be expected to read and comply with this policy.

Purpose

The purpose of this policy is to set out SHVH's commitment and procedures for protecting personal data. Trustees regard the lawful and correct treatment of personal information as particularly important to successful working and to maintaining the confidence of those with whom we deal.

We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

Definitions

- Data Controller – the trustees who collectively decide what personal information SHVH will hold and how it will be used.
- Act – the Data Protection Act 2018 and UK GDPR.
- Data Protection Officer – SHVH is not required to appoint a DPO.
- Data Subject – the individual whose personal information is being held or processed.
- Information Commissioner's Office (ICO) – the UK authority responsible for overseeing UK GDPR and the Data Protection Act 2018.
- Processing – collecting, amending, handling, storing or disclosing personal information.
- Personal Information – information about living individuals that enables them to be identified.

The Data Protection Principles

Personal data:

- Shall be processed fairly, lawfully and transparently.
- Shall be obtained only for specific purposes and not used in ways incompatible
- with those purposes.
- Shall be adequate, relevant and limited to what is necessary.
- Shall be accurate and kept up to date.
- Shall not be kept for longer than necessary.
- Shall be processed in accordance with the rights of data subjects.
- Shall be kept secure using appropriate technical and organisational measures.
- Shall not be transferred outside the UK unless appropriate safeguards are in place (e.g., adequacy decision or standard contractual clauses).

We will let people know why we are collecting their data, which is for the purpose of managing the hall, its hirings and finances. Access to personal information will be limited to trustees, staff and volunteers.

Correcting Data

Individuals have a right to make a Subject Access Request (SAR) to find out whether SHVH holds their personal data, what it is used for, and to have data corrected if it is wrong. Any SAR must be dealt with within 30 days.

Identity checks will be carried out before releasing information.

Responsibilities

SHVH is the Data Controller and is legally responsible for complying with UK GDPR and the Data Protection Act 2018.

The management committee will ensure that:

- Information is collected and used fairly.
- Purposes for which information is used are specified.
- Only necessary information is collected and processed.
- Information is accurate.
- Individuals' rights can be exercised.
- Appropriate security measures are in place.
- Information is not transferred outside the UK without safeguards.
- Requests for information are handled fairly and consistently.

A breach of this policy may lead to action being taken.

Data Protection Officer (if appointed): Not appointed.

Procedures for Handling Data & Data Security

All trustees, staff and volunteers must ensure that personal data is handled properly, whether held on paper, computer, tablet or mobile phone.

Personal data includes any information that can identify an individual and is not otherwise in the public domain.

Email

- Emails containing personal information that need to be kept must be stored securely.
- Emails no longer required must be deleted.

Phone Calls

Personal information should not be given out unless the caller's identity is certain.

Laptops and Portable Devices

Devices holding personal data must be password-protected and kept secure at all times.

Data Storage

- Personal data will be stored securely and only accessible to authorised volunteers or staff.
- Financial records will be kept for up to 7 years.
- Archival material such as minutes and legal documents will be stored indefinitely.

Personal data must be non-recoverable from any computer passed on or sold.

Employees and Former Employees

Employee records may be kept indefinitely where legally required.

Accident Book

Completed pages will be removed, acted upon, and stored securely.

Data Sharing

Data may be shared without consent only where legally permitted, such as:

- Legal obligations
- Protecting vital interests (e.g., safeguarding)
- Legal proceedings
- Equal opportunities monitoring

Risk Management

Breaches of data protection can cause harm or distress. Trustees, staff and volunteers may be personally liable for misuse of personal data.

This policy will be reviewed every two years.

Date of Review: 24/02/2026

Chair: Paul Styles

Deputy Chair: Ros Adams