Leonard Stanley Village Hall

Data Protection Policy and Procedures

May 18th 2021

Introduction

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 (PD) in order to carry on our work of managing Leonard Stanley Village Hall (LSVH). This personal information must be collected and handled securely.

The Data Protection Act 1998 (DPA) and General Data Protection Regulations (GDPR) govern the use of information about people (personal data). Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs.

The charity will remain the data controller for the information held. The trustees, staff and volunteers are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. Trustees, staff and volunteers who have access to personal information will therefore be expected to read and comply with this policy.

The Data Protection Act

This contains 8 principles for processing personal data with which we must comply.

Personal data:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
3. Shall be adequate, relevant and not excessive in relation to those purpose(s).
4. Shall be accurate and, where necessary, kept up to date,
5. Shall not be kept for longer than is necessary,
6. Shall be processed in accordance with the rights of data subjects under the Act,
7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

Applying the Data Protection Act within the charity

We will let people know why we are collecting their data, which is for the lawful purpose of managing the hall, its hiring, marketing, publicity for events, fundraising and finances. It is our responsibility to ensure PD is only used for this purpose unless specific consent is given or the PD is already in the public domain. Access to personal information will be limited to trustees, staff and volunteers.

Correcting data

Hirers information is entered by the hirers themselves into the online booking system, HallMaster. Hirers, therefore. have control over the accuracy of data stored. Should their details change, they are able to access their own account and make changes as necessary.

Should the hirer not have access to a computer and their hiring details be entered into the HallMaster system by an authorised member of the village hall committee, the hirer may request a copy of their details to be sent to them by post and may request any corrections to be made. Any such requests should be dealt with within 7 working days or receipt of such a request.

Responsibilities

LSVH is the Data Controller under the Act, and is legally responsible for complying with Act, which means that it determines what purposes personal information held will be used for.

Procedures for Handling Data & Data Security

LSVH has a duty to ensure that appropriate technical and organisational measures are taken to prevent:

- Unauthorised or unlawful processing of personal data
- Unauthorised disclosure of personal data
- Accidental loss of personal data

PD relating to hirers of the Village Hall should, where possible, be entered by the hirers themselves into the on-line booking system. This ensures any PD LSVH holds is accurate and under the control of the hirer.

Any PD relating to individual bookings of the Village Hall is under control of the hirer, who decides if their data should be made publicly visible or not in the online diary when they make their booking request.

Privacy Notice and Consent Policy

LSVH uses personal data for the purposes of managing hall bookings, finances, events and publicity. We will not sell PD to any 3rd Party.

Operational Guidance

Email:

All trustees, staff and volunteers should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained, it should be saved into an appropriate folder or printed and stored securely.

Emails that contain PD personal information no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" box.

Where someone not a trustee, employee, volunteer or contractor needs to be copied into an email e.g. a wider circulation list for an upcoming event, we encourage use of bcc instead of cc, so as to avoid their PD being shared through forwarding.

Phone Calls:

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- Personal information should not be given out over the telephone unless you have no doubts as to the caller's identity and the information requested is innocuous.
- If you have any doubts, ask the caller to put their enquiry in writing.
- If you receive a phone call asking for personal information to be checked or confirmed be aware that the call may come from someone impersonating someone with a right of access.

Laptops and Portable Devices:

All laptops and portable devices that hold data containing personal information must be protected with a suitable password which is changed regularly.

Data Security and Storage:

Store as little PD as possible relating to LSVH on your computer or laptop; only keep those files that are essential.

Passwords:

Do not use passwords that are easy to guess. Passwords should contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length.

Protect Your Password; common sense rules are:

- Do not give out your password.
- Do not write your password somewhere on your laptop.
- Do not keep it written on something stored in the laptop case.

Data Storage:

Personal data will be stored securely and will only be accessible to authorised volunteers or staff.

All documents that are in hard copy form should be kept in a secure location.

All personal data held for the organisation must be non-recoverable from any computer which has been passed on/sold to a third party.

Once documents are no longer needed they should be deleted from computers and any hard copies should be destroyed.

How long should data be stored?	What should be stored?
Indefinitely	• Legal documents • Minutes of meetings • All information regarding an employee or a former employee • Accident forms • Insurance policy documents
7 Years	• Financial records
Only as long as needed	• Correspondence • Emails

Photographs:

LSVH may use general photographs of events with groups of adults at the hall for publicity purposes in accordance with its lawful basis for using PD. Photos of children must not be used without the written consent of the parent or guardian. At private events or club meetings the consent of individuals (verbal) should be obtained if their image will be clearly identifiable. Hirers are encouraged to comply with this policy.

Data Subject Access Requests:

We may occasionally need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies in circumstances which are not in furtherance of the management of the charity. The circumstances where the law allows the charity to disclose data (including sensitive data) without the data subject's consent are:

a) Carrying out a legal duty or as authorised by the Secretary of State Protecting vital interests of a Data Subject or other person e.g. child protection

b) The Data Subject has already made the information public

c) Conducting any legal proceedings, obtaining legal advice or defending any legal rights

d) Monitoring for equal opportunities purposes – i.e. race, disability or religion.

We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. If an agency asks for PD not in compliance with one of the above e.g. to obtain information about improving a service a consent form will need to be issued to the data subjects asking for their consent to pass their PD on.

We intend to ensure that personal information is treated lawfully and correctly.

Risk Management:

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Trustees, staff and volunteers should be aware that they can be personally liable if they use customers' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access and sharing.

Compliance

This document will be made available to all Trustees, staff and volunteers who will be asked to comply with its contents.