Sandleheath Village Hall CIO
St. Aldhelm's, Main Road, Sandleheath, FORDINGBRIDGE, Hampshire SP6 1TD
Phone: 07512 741873. Email: info@sandleheathvillagehall.com.

SVH/7 22 Feb 19

SANDLEHEATH VILLAGE HALL - DATA PROTECTION POLICY

INTRODUCTION

1. Sandleheath Village Hall (SVH) is committed to a policy of protecting the rights and privacy of individuals. Trustees, staff and volunteers need to collect and use certain types of data to manage SVH. This personal information must be collected and handled securely.

2. The Data Protection Act 1998 (DPA) [1] 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 emails, minutes of meetings and photographs.

3. SVH trustees regard the lawful and correct treatment of Personal Data as important to successful working, and to maintaining the confidence of those who we deal with. They recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

4. SVH trustees are committed to protecting Personal Data. They have a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

   a. Unauthorised or unlawful processing of personal data.

   b. Unauthorised disclosure of personal data.

   c. Accidental loss of personal data.

5. Trustees, staff and volunteers who have access to Personal Data are expected to read and comply with this policy. They should be aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

PURPOSE

6. The purpose of this policy is to set out SVH procedures for protecting Personal Data[2].

7. 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.

DEFINITIONS

8. **Personal Data**. Information about living individuals that enables them to be identified, e.g. names, addresses, telephone numbers and email addresses. Personal Data:

   a. Does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers.

[1] The Information Commissioner's Office (ICO) is responsible for implementing and overseeing the DPA.
[2] This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the DPA.

b. Relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises Personal Data. However, combining various data elements such as a person's name and salary or religious beliefs etc. would be classed as personal data, and falls within the scope of the DPA.

c. It is therefore important that all staff consider any information, which is not otherwise in the public domain, that can be used to identify an individual, as Personal Data.

9. **Data Controller**. The trustees who collectively decide what Personal Data SVH will hold and how it will be held or used.

10. **Act**. The DPA and GDPR; the legislation that requires responsible behaviour by those using Personal Data.

11. **Data Protection Officer (DPO)**. The person responsible for ensuring that SVH follows its data protection policy and complies with the Act.

12. **Data Subject**. The individual whose personal information is being held or processed by SVH, for example a donor or hirer.

13. **Explicit Consent**. A freely given, specific agreement by a Data Subject to the processing of personal information about her/him. Explicit Consent is needed for processing sensitive data, which includes:

a. Racial or ethnic origin of the data subject.

b. Political opinions.

c. Religious beliefs or other beliefs of a similar nature.

d. Trade union membership.

e. Physical or mental health or condition.

f. Sexual orientation.

g. Criminal record.

h. Proceedings for any offence committed or alleged to have been committed.

14. **Processing**. Collecting, amending, handling, storing or disclosing Personal Data.

DATA PROTECTION ACT PRINCIPLES

15. There are eight principles for processing Personal Data which SVH must comply with. Personal Data:

a. Shall be processed fairly and lawfully and shall not be processed unless specific conditions are met.

b. 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.

c. Shall be adequate, relevant and not excessive in relation to those purpose(s).

d. Shall be accurate and, where necessary, kept up to date.

e. Shall not be kept for longer than is necessary.

f. Shall be processed in accordance with the rights of data subjects under the Act.

g. 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.

h. 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.

RESPONSIBILITIES

16. **Data Controller**. The SVH charity will remain the Data Controller for the information held, as follows:

a. The charity is legally responsible for complying with the Act, which means that it determines what purposes personal information held will be used for. It will let people know why it is collecting their data, which is for managing the hall, its hirings and finances. It is the charity's responsibility to ensure the Personal Data is only used for this purpose. Access to personal information will be limited to trustees, staff and volunteers. An SVH Data Map is at Enclosure 1. It describes the nature of Personal Data that trustees, staff and volunteers are permitted to acquire and retain.

b. The trustees[3] will consider legal requirements and ensure that they are properly implemented. Through use of appropriate management, strict application of criteria and the institution of controls, they will:

(1) Collect and use information fairly.

(2) Specify the purposes for which information is used.

(3) Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.

(4) Ensure the quality of information used.

(5) Ensure the rights of people about whom information is held, can be exercised under the Act. These include:

(a) The right to be informed that processing is undertaken.

(b) The right of access to one's personal information.

(c) The right to prevent processing in certain circumstances, and the right to correct, rectify, block or erase information which is regarded as wrong information.

[3] Or Management Committee if one is formed.

(6) Take appropriate technical and organisational security measures to safeguard personal information,

(7) Ensure that personal information is not transferred abroad without suitable safeguards,

(8) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,

(9) Set out clear procedures for responding to requests for information.

17. **Data Protection Officer**. The SVH DPO is **Michael Richardson**, who can be contacted as follows:

a. **Address**. Sandleheath Village Hall, St. Aldhelm's, Main Road, Sandleheath, Fordingbridge, Hampshire SP6 1TD.

b. **Email**. info@sandleheathvillagehall.com.

c. **Mobile**: 07887 763707.

18. **Data Protection Officer Responsibilities**. The DPO is responsible for ensuring that this policy is implemented and will have overall responsibility. He will:

a. Ensure that everyone processing personal information understands that they are contractually responsible for following good data protection practice.

b. Ensure that everyone processing personal information is appropriately trained to do so.

c. Ensure that everyone processing personal information is appropriately supervised.

d. Ensure that anybody wanting to make enquiries about handling personal information knows what to do.

e. Deal promptly and courteously with any enquiries about handling personal information

f. Describe clearly how the charity handles personal information.

g. Will regularly review and audit the ways it holds, manages and uses personal information.

h. Will regularly assess and evaluate its methods and performance in relation to handling personal information.

19. **Individual Responsibility**. All SVH trustees, staff and volunteers are personally responsible for processing and using personal information in accordance with the Act. In general:

a. They must ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether the information is held on paper, in a computer or recorded by some other means e.g. tablet or mobile phone.

b. 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.

CORRECTING DATA

20. Individuals have a right to make a Subject Access Request (SAR) to find out whether the charity holds their personal data, where, what it is used for and to have data corrected if it is wrong. This is to prevent use which is causing them damage or distress, or to stop marketing information being sent to them.

21. Any SAR must be dealt with within 30 days. Steps must first be taken to confirm the identity of the individual before providing information, requiring both photo identification e.g. passport and confirmation of address e.g. recent utility bill, bank or credit card statement.

22. The SVH SAR Inquiry Form and SVH Subject Access Response Form are available from the DPO.

CONSENT POLICY AND PRIVACY STATEMENTS

23. SVH consent to gather and retain Personal Data is gained by the initiation of Consent and Data Privacy Statement (DPS) templates. These are available from the DPO and consist of:

a. **Consent.** Consent is gained as follows:

(1) **Initial Contact**. The SVH Keeping in Touch form. It is used solely to allow individuals to express an interest in SVH matters.

(2) **Consent**. The SVH Consent Form.

b. **Data Privacy Statements**. DPSs are:

(1) DPS Supporters.

(2) DPS Volunteers.

(3) DPS Financial Donors.

24. Consent and DPS forms will be stored by the Secretary in a securely held electronic or paper file.

OPERATIONAL GUIDANCE

25. **Email**. Procedures for handling emails are:

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

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

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

a. 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.

b. If you have any doubts, ask the caller to put their enquiry in writing.

c. 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.

27. **Laptops and Portable Devices**. Procedures for handling laptops and portable devices are:

a. All laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program agreed with the DPO; a password.

b. Laptops or portable devices are to be locked (password protected) when left unattended, even for short periods of time. Do not use passwords that are easy to guess. All passwords should contain both upper and lower-case letters and at least one numbers. Ideally passwords should be nine characters or more in length. Common sense rules for passwords are:

(1) Do not give out a password.

(2) Do not write a password somewhere on a laptop.

(3) Do not keep it written on something stored in the laptop case.

c. When travelling in a car, laptops or portable devices are to be out of sight, preferably in the boot.

d. If laptops and portable devices must be left in an unattended vehicle at any time, they are to be put in the boot, all doors are to be locked and any alarm set.

e. Laptops and portable devices are never to be left in a vehicle overnight.

f. Laptops or portable devices are never to be left unattended in restaurants or bars, or any other venue.

g. When travelling on public transport, laptops and portable devices are to be kept with the person always, not left in luggage racks or even on the floor alongside.

DATA SECURITY AND STORAGE

28. **Principle**. Personal Data will be stored securely and will only be accessible to authorised volunteers or staff.

29. **Storage Rules**. As little Personal Data as possible is to be stored on a computer or laptop; only those files that are essential. Personal data received on disk or memory stick should be saved to the relevant file on the server or laptop. The disk or memory stick should then be securely returned, if applicable, safely stored or wiped and securely disposed of.

30. **Information Types**. Information will be stored for only if it is needed or required by statute and thereafter will be disposed of appropriately:

a. **Financial Records**. For financial records this will be up to seven years.

b. **Archives**. Archival material such as minutes and legal documents will be stored indefinitely.

c. **Employees**. Information regarding an employee or a former employee, will be kept indefinitely. If something occurs years later it might be necessary to refer to a job application or other document to check what was disclosed earlier, in order that trustees comply with their obligations e.g. regarding employment law, taxation, pensions or insurance.

d. **Other Correspondence**. Other correspondence and emails will be disposed of when no longer required or when trustees, staff or volunteers retire.

e. **Accident Book**. The Accident Book will be checked regularly. Any page which has been completed will be removed, appropriate action taken, and the page filed securely.

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

DATA SUBJECT ACCESS REQUESTS

32. SVH 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.

{Signed}

K BENNETT
Chairman SVH CIO