	Coxheath Residents Village Hall Registered Charity No: 295467

Introduction

Coxheath Village Hall (CVH) is committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of data in order to carry on our work of managing the Hall. This personal information will 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 laptops, mobile phones or in a manual file.

CVH will remain the data controller for the information held, The trustees are personally responsible for processing and using the personal information in accordance with the DPA and GDPR. Trustees 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 the CVH commitment and procedures for protecting personal data. Trustees 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 with, we recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

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 purposes(s),
4. Shall be accurate and, where necessary kept up to date,
5. Shall not be kept for longer than necessary,
6. Shall be processed in accordance with the rights of data subjects under the Act,
7. Shall be kept secure by Trustees who take appropriate 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 abroad.

Applying the Data Protection Act within the charity

Personal data is collected by CVH for the purpose of managing the hall, its hirings and finances. It is our responsibility to ensure the data is only used for this purpose. Access to personal data will be limited to the Trustees who deal with the day to day hiring and finances.

Correcting Data

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, to prevent use which is causing them damage or distress. Any SAR must be dealt

providing information, requiring both photo identification and confirmation of address.

Responsibilities

CVH is the data controller under the Act, and is legally responsible for complying with the Act, which means that it determines what purposes information held will be used for.

The management committee will take into account legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

a) Collection and use information fairly
b) Specify the purpose for which information is used
c) 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
d) Ensure the quality of information used
e) Ensure the rights of people about whom information is held, can be exercised under the Act
f) Take appropriate technical and organisational security measures to safeguard personal information
g) Ensure that personal information is not transferred abroad without suitable safeguards
h) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
i) Set out clear procedures for responding to requests for information

Procedures for Handling Data and Data Security

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

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

All trustees must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper, in a computer, or recorded by some other means e.g. mobile phone.

Personal data 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 person's name, email address would be classed as personal data, and falls within the scope of DPA. It is therefore important that all trustees consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and observe the Operational Guidance below,

Operational Guidance

Email:

All trustees should consider whether an email (both incoming and outgoing) will need to be kept as an official record.

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

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 identityand the information requested is onnocuous
- 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 encryption program (password)

Data Security and Storage

Store as little personal data as possible on your computer or laptop, only keep those files that are essential.

Protect your password

Common sense rules for passwords are do not give out your password

Do not write your password somewhere on your laptop

Do not keep it written on something store in the laptop case

Data storage

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately. For financial records this will be up to 7 years, Archival material such as minutes and legal documents stored indefinitely and securely. Other correspondence such as hiring agreements, diary pages and emails will be disposed of when no longer required.

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

Accident Book

This will be checked regularly. Any page which has been completed will be removed, appropriate action taken and the page filed securely.

Reviewed and agreed by the Committee 13th August 2024