COLN VALLEY VILLAGE HALL

DATA PROTECTION POLICY AND PROCEDURES

Introduction

We are 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 Coln Valley Village Hall ('CVVH'). 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.

CVVH will remain the data controller for the information held. The Trustees, Committee Members and any Volunteers ('Personnel') are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. Personnel 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 CVVH commitment and procedures for protecting personal data. 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 with. We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

The following are definitions of the terms used:

Data Controller - the Personnel who collectively decide what personal information CVVH will hold and how it will be held or used.

Act means the Data Protection Act 1998 and General Data Protection Regulations - the legislation that requires responsible behaviour by those using personal information.

Contacts Database – a database of basic contact details for people within the CVVH catchment area

Database Co-ordinator – the person responsible for maintaining the Contacts Database.

Data Subject – the individual whose personal information is being held or processed by CVVH, for example a donor, hirer or Valley resident.

'Explicit' consent – is 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

Information Commissioner's Office (ICO) - the ICO is responsible for implementing and overseeing the Act.

Personnel - The Trustees, Committee Members and any Volunteers appointed from time to time

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers.

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 hold data for the purpose of managing the hall, bookings, finances, publicity, its fundraising activities, running and marketing events at the hall and public relations.

We also circulate a newsletter and information to our residents regarding items of interest associated with the village hall and of general interest regarding our catchment area, which data is held in a separate Contacts Database. It is our responsibility to ensure the Contacts Database is only used for this purpose. Access to personal information will be limited to the Database Co-ordinator.

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, or to stop marketing information being sent to them. 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.

To make an SAR please contact the Chairman of the Village Hall Management Committee.

Responsibilities

CVVH 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.

The CVVH Management Committee will take into account legal requirements and ensure that they are properly implemented, and through appropriate management, strict application of criteria and controls will:

a) Collect and use information fairly.

b) Specify the purposes 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.

These rights include:

i) The right to be informed that processing is undertaken.

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

iii) The right to prevent processing in certain circumstances, and

iv) the right to correct, rectify, block or erase information which is regarded as wrong information.

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.

All Personnel are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

The Personnel will be collectively responsible for ensuring that the policy is implemented and will have individual responsibility for ensuring that they comply with this Policy.

Compliance with data privacy regulations will be a standing item on the CVVH AGM.

Procedures for Handling Data & Data Security

CVVH 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 data

All Personnel 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. tablet or 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 a person's name and salary or religious beliefs etc. would be classed as personal data, and falls within the scope of the DPA. 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 and observe the guidance given below.

Privacy Notice and Consent Policy

CVVH will obtain explicit consent for inclusion on the Contacts Database. Consent will be given in email form to the Database Co-ordinator.

Consent forms will be stored by the Database Co-ordinator in a securely held electronic or paper file.

Consent to be included on the Contacts Database can be withdrawn at any time by notifying the Database Co-ordinator.

Details held in the Contacts Database will normally include:

A. Full Name
B. email address
C. Address (House name or number, and village only)
D. Telephone and / or mobile phone number (optional)

Operational Guidance

Email:

All Personnel 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 the appropriate computer folder or printed and stored securely.

Remember, 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:

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.

Laptops and Portable Devices:

All laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program (password or PIN).

Ensure your laptop is locked (password protected) when left unattended, even for short periods of time.

When travelling in a car, make sure the laptop is out of sight, preferably in the boot.

If you have to leave your laptop in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set.

Never leave laptops or portable devices in your vehicle overnight.

Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.

When travelling on public transport, keep it with you at all times, do not leave it in luggage racks or even on the floor alongside you.

Data Security and Storage:

Store as little personal data as possible on your computer or laptop; only keep 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.

Always lock (password protect) your computer or laptop when left unattended.

Passwords:

Do not use passwords that are easy to guess. All your 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 for passwords are:

a) Do not give out your password

b) Do not write your password somewhere on your laptop

c) 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 Personnel.

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 will be stored indefinitely. Other correspondence and emails will be disposed of when no longer required or when trustees, staff or volunteers retire.

All personal data held for the organisation must be non-recoverable from any computer 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.

Abortive bookings:

If there is a booking enquiry which does not lead to a booking then any relevant data should be deleted.

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.

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. Personnel should be aware that they can be personally liable if they use individuals' 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.

Data Breach Procedure:

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. CVVH have to notify the ICO where it is likely to result in a risk to individuals. For example, damage to reputation, financial loss, loss of confidentiality. If a data breach occurs, it is important to check whether anything could be done to avoid it happening again.

All Personnel need to be aware that it is essential that any PC, laptop, mobile, tablet, CD or memory stick used for CVVH purposes is password or PIN protected and that if any of these items are stolen or hacked, and risk to individuals results, the breach is reported. The same applies to paper files.

If you discover that data has been lost, or if you believe there has been a breach of the data protection principles in the way that data is handled, you must immediately or no later than within 72 hours of first coming to notice, inform the ICO. The priority must then be to close or contain the breach to mitigate/minimise the risks to those individuals affected by it. Ring the ICO's helpline for clarification if unsure whether something represents a significant breach.

Consider the following points:

- Containment and recovery
- Assessment of on-going risk

- Notification of breach

Containment and recovery

The initial response is to investigate and contain the situation and instigate a recovery plan, including damage limitation.

- Inform the Management Committee and seek assistance in the containment exercise. This could be recovery of released documents, finding a lost piece of equipment or simply changing any related access codes
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.

Assessing the risks

1. Consider the following points:
    - What type of data is involved?
    - How sensitive is the data?
    - If data has been lost or stolen, are there any protections in place such as encryption?
    - What has happened to the data?
    - If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate? If it has been damaged, this poses a different type and level of risk.
    - Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
    - How many individuals' personal data has been affected by the breach?
    - Who are the individuals whose data has been breached?
    - What harm can come to those individuals?

2. Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause and inform the Management Committee.

Notification of breaches

1. Inform the Management Committee or its appointee immediately or within 24 hours of being made aware of the breach with your name, the date/time of breach, date/time you detected it and give basic information about the type of breach and information about personal data concerned. Include details of what you have already done to respond to the risks posed by the breach.

2. The Management Committee or its appointee will assess the type and level of risk and any further actions and, if necessary, inform the ICO by phone.

3. The ICO, whom if necessary will be informed by the Management Committee or its appointee, will investigate the breach in their capacity as the independent regulator for Data Protection.