

# CROPREDY VILLAGE HALL

## Data Protection Policy and Procedures



Registered Charity  
No.: 304288

### 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 in order to carry on our work of managing Cropredy Village Hall (CVH). 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 data in accordance with the Data Protection Act and GDPR. Trustees, staff and volunteers who have access to the personal data will therefore be expected to read and comply with this policy.

### PURPOSE

The purpose of this policy is to set out the Cropredy Village Hall commitment and procedures for protecting personal data. Trustees regard the lawful and correct treatment of personal data as very important to successful working, and to maintaining the confidence of those whom we deal with. We recognise the risks to individuals of identity theft and financial loss if data is lost or stolen.

The following are definitions of the terms used:

**Data Controller** – the trustees who collectively decide what personal information Cropredy Village Hall 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.

**Data Subject** – the individual whose personal data is being held or processed by Cropredy Village Hall for example a donor or hirer.

**'Explicit' consent** – is a freely given, specific agreement by a Data Subject to the processing of personal data 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 Data Protection Act 1998.

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

**Personal Data** – 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 data,
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 data.

## **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 personal data is only used for this purpose unless specific consent is given, or the personal data is already in the public domain. Access to personal data will be limited to trustees, staff and volunteers.

Where individuals need to be identified in public documents e.g. minutes and harm may result, initials rather than full names will normally be used.

## 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 that 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.

Any concerns about complying with a SAR need to be discussed promptly with the ICO, e.g. if it is manifestly unfactual or excessive.

## Responsibilities

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

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

- a) Collect 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

These include:

- The right to be informed that processing is undertaken
- The right of access to one's personal data
- The right to prevent processing in certain circumstances, and
- The right to correct, rectify, block or erase information which is regarded as wrong information.
- Take appropriate technical and organisational security measures to safeguard personal data.
- Ensure that personal data is not transferred abroad without suitable safeguards
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information

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

## PROCEDURES FOR HANDLING DATA AND DATA SECURITY

Cropredy Village Hall 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 trustees (committee members) must therefore 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.

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 trustees (committee members) 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**

Personal information is collected directly from you when you interact with Cropredy Village Hall or when you provide information when booking an event. We collect this information in order to keep in touch with you until completion of our interaction or event. The information which we collect in this way will typically include your name, address, email address and telephone number. Information collected will not be shared with any other organisation and we promise to keep your details safe and secure by holding data either electronically on a password protected device, or as hard copy filed chronologically and securely.

We will retain your information for as long as you have an active relationship with Cropredy Village Hall, after which your information will be securely deleted and/or destroyed.

## **OPERATIONAL GUIDANCE**

### **Email:**

All trustees 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 the appropriate folder or printed and stored securely.

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

Where someone not a trustee, employee 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, to avoid their personal data being shared through forwarding.

## **Phone Calls:**

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

- Personal data 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 Personal Devices:**

All laptops and portable devices that hold data containing personal data must be protected with a suitable password which is changed regularly. Where sensitive data or financial information is held an encryption program should be used.

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 must 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 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 information as possible relating to Cropredy Village Hall 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.

## **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 you password somewhere on your laptop
- Do not keep in written on something in the laptop case

## **Data Storage:**

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

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. For employee records see below. 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 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 will be taken and the page filed securely.

Cropredy Village Hall may use general photographs of events with groups of adults at the hall for publicity purposes in accordance with its lawful basis for using personal data. Photos of children must not be used without the written consent of the parent or guardian. However, Cropredy Village Hall is aware that for some individuals publicising their location could place them or their families at risk. Consequently at large events at which publicity photos may be taken a notice should be posted at the entrance, or an announcement made, providing opportunity for people to refuse taking part in publicity photographs. At small events 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 data as very important to successful working, and to maintaining the confidence of those with whom we deal. If an agency asks for personal data 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 the personal data on.

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

### **Risk Management:**

The consequences of breaching Data Protection can cause harm or distress to service users if their personal data 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 hirers' personal data inappropriately. This policy is designed to minimise the risk and ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access and sharing.

**DATE POLICY ADOPTED:**

**Review: Annually**

**Signature of Chairman**

A handwritten signature in black ink, appearing to read "A. B. ...", followed by a period.

**Signature of Secretary**

A handwritten signature in black ink, appearing to read "A. Payne", followed by a period.