HELPERBY 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 personal data in order to carry on our work of managing Helperby Village Hall (HVH). This personal data must be collected and handled securely.

The Data Protection Act 2018 (DPA) and the General Data Protection Regulations (GDPR) govern the use of information about people. Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings and photographs.

HVH is the data controller for the information we hold. The trustees, staff and volunteers are personally responsible for processing and using personal data in accordance with the DPA and GDPR. Trustees, staff and volunteers who have access to personal data will therefore be expected to read and comply with this policy.

Purpose

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

Here are some explanations of terms used in this document:

Data Controller – HVH, which, through its trustees, determines the purposes and means of processing personal data; the trustees decide what personal data HVH will hold and how it will be held or used.

Act – means the DPA and GDPR – the legislation that requires responsible behaviour by those using personal data.

Data Protection Officer – the person responsible for ensuring that HVH follows its data protection policy and complies with the Act.

Data subject – the individual whose personal data is being held or processed by HVH, for example a donor or hirer.

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

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

Personal data – is information that relates to an identified or identifiable individual e.g. names, addresses, telephone numbers and email addresses.

Sensitive data – includes the racial or ethnic origin of the data subject, political opinions, religious or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual orientation, criminal record, proceedings for any offence committed or alleged to have been committed.

GDPR

These regulations contain the principles for processing personal data with which HVH must comply.

Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected and processed for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and kept up to date
5. Kept for no longer than is necessary
6. Processed securely

The Data Controller is accountable for meeting these principles.

Applying data protection legislation within HVH

We will let people know why we are collecting their data, which is for the lawful purpose of managing HVH, 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 some volunteers.

Subject Access Requests

Individuals have a right to make a Subject Access Request (SAR) to find out whether HVH holds their personal data and what it is together with certain supplementary information. SARs may be made in writing or verbally. Any SAR must be dealt with within one month.

If a SAR is made it should be referred immediately to the Secretary.

Responsibilities

HVH acting through its trustees is the Data Controller under the Act and is legally responsible for compliance.

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

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 HVH's operational needs or to comply with any legal requirements.
d) Ensure the quality of information used.
e) Make sure the rights of people about whom information is held can be exercised.

These rights include:

- The right to be informed about the collection and use of their personal data
- The right of access (Subject Access Requests)
- The right to rectification of inaccurate or incomplete personal data
- The right to erasure – "the right to be forgotten"
- The right to restrict processing – to limit the way in which HVH uses their data
- The right to object – e.g. to direct marketing

The trustees will:

- Take appropriate technical and organisational security measures to safeguard personal data.
- Set out procedures to deal with a Subject Access Request.
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Implement procedures to correct, rectify, block or erase information which is inaccurate.
- Ensure that personal data is not transferred abroad.

All trustees, staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to serious consequences.

The HVH Data Protection Officer is the secretary to the trustees.

Name: Martine Laux

Contact details:

Helperby Village Hall, Main Street, Helperby, York YO61 2NS

Tel: 01423 360138

The Data Protection Officer will be responsible for policy oversight and in particular ensuring that:

a) Everyone processing personal data understands that they are responsible for following good data protection practice.
b) Everyone processing personal data is trained to do so.
c) Everyone processing personal data knows where to turn to for guidance.
d) Anybody wanting to make enquiries about handling personal data knows what to do.
e) HVH handles personal data transparently.
f) The policy is regularly reviewed.

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.

In case of any queries or questions in relation to this policy please contact the Data Protection Officer.

Procedures for Handling Data and Data Security

HVH 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, staff and volunteers 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 is data that relates to an identified or identifiable individual. What identifies an individual could be as simple as a name or a number. If it is possible to identify an individual from the information you are processing then that information may be personal data. If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual. Even if an individual is identified or identifiable, directly or indirectly, from the data you are processing, it is not personal data unless it 'relates to' the individual. When considering whether information 'relates to' an individual, you need to take into account a range of factors, including the content of the information, the purpose or purposes for which you are processing it and the likely impact or effect of that processing on the individual. Information which has had identifiers removed or replaced in order to pseudonymise the data is still personal data for the purposes of the GDPR. Information which is truly anonymous is not covered by the GDPR.

It is therefore important that all trustees, staff and volunteers 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 in this document.

Privacy Notice

The privacy notice is as follows:

“Helperby Village Hall uses personal data for the purposes of managing the hall, its bookings and finances, running and marketing events at the hall, staff employment and its fundraising activities. Data may be retained for up to 7 years for accounts purposes and for longer where required e.g. by the hall’s insurers. If you would like to find out more about how we use your personal data or want to see a copy of information about you that we hold, please contact the hall Secretary.”

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 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, 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 personal data being shared through forwarding.

Telephone 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 data 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 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 unattached, 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 your devices with you at all times, do not leave them in luggage racks or even on the floor alongside you.

Data Security:

Store as little personal data as possible relating to HVH 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, 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 or symbols. 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 must be stored securely and must only be accessible by authorised volunteers or staff.

Information should be stored for only as long as it is needed or required by statute and then must 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 held for the organisation must be non-recoverable from any computer which has been passed on/sold to a third party.

Information Regarding Employees or Former Employees:

Information regarding an employee or a former employee will be kept indefinitely. If something occurs years later it might be necessary to refer back 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.

Accident Book:

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

Photographs:

HVH 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, HVH 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.

Sharing Data:

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 HVH. The circumstances where the law allows HVH 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
b) Protecting vital interests of a data subject or other person e.g. child protection
c) The data subject has already made the information public
d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights
e) Monitoring for equal opportunity purposes – i.e. race, disability or religion.

We regard the lawful and correct treatment of personal data as being very important for the successful operation of HVH and for maintaining the confidence of those with whom we deal. If an agency asks for personal data otherwise than in compliance with one of the above e.g. to obtain information about improving a service, a consent form must be issued to the data subjects asking for their consent to pass on their personal data.

Risk Management:

The consequences of breaching data protection law can cause harm or distress to service users if their information is released wrongly. 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 HVH is not damaged through inappropriate or unauthorised access and sharing.

Data Breach:

Certain types of data breach must be reported to the Information Commissioner's Office and in some cases to the individuals affected. A report to the ICO must be made within 72 hours of becoming aware that an incident is reportable. The ICO helpline 0303 123 1113 can be called if we are unsure whether something represents a significant breach.

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

v03.07.21