

## Ferring Village Hall (Charity No. 1167736)

### DATA PROTECTION POLICY AND PROCEDURES

#### Introduction

Ferring Village Hall (FVH) is a charity registered under Charity No. 1167736. FVH's objects are to run a village hall and to promote for the benefit of the inhabitants of Ferring without distinction of sex, sexual orientation, age, disability, nationality, race or political, religious or other opinions, the provision of facilities for recreation and leisure.

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 the Village Hall. The personal information must be collected and handled securely.

The Data Protection Act 2018 (DPA) and UK 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.

FVH will be the Data Controller for the information held. The trustees, staff and volunteers are personally responsible for processing and using personal information in accordance with the DPA and GDPR. Trustees, staff and volunteers 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 FVH's 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 following are definitions of the terms used:

**Data Controller** - the trustees who collectively decide what personal information FVH will hold and how it will be held.

**Act** - means the Data Protection Act 2018 and UK General Data Protection Regulations - the legislation that requires responsible behaviour by those using personal information.

**Data Subject** - the individual whose personal information is being held or processed by FVH; for example, a donor or hirer.

**Explicit Consent** - is a freely given, specific arrangement 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.

**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.

### **Data protection principles for processing personal data**

We will comply with the following principles for processing personal data:

- Personal data shall be processed fairly and lawfully and in a transparent manner.
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary kept up to date.
- Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under the Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the UK unless that country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data.

### **Applying the Act**

We will let people know why we are collecting their data, which is for the lawful purpose of managing FVH, its hiring, marketing, publicity for events, fundraising and finances. It is our responsibility to ensure personal data is only used for this purpose unless Explicit Consent (where applicable) or general consent is given or the personal data is already in the public domain.

Access to personal information will be limited to trustees, staff and volunteers and only where necessary.

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 FVH holds their personal data, where and how it is held, 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 one month of receipt. 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, such as by recent utility bill, bank or credit card statement.

Any concerns about complying with a SAR need to be discussed promptly with FHV's Secretary at [Ferringvh.sec@gmail.com](mailto:Ferringvh.sec@gmail.com) or with the ICO if it is manifestly inaccurate or excessive.

## **Responsibilities**

FVH is the Data Controller under the Act, and is legally responsible for complying with the Act, which means that it determines how the personal information it holds is to be used for.

FVH's Trustees will take into account all appropriate legal requirements and ensure that they are properly implemented, and will do so through appropriate management and the strict application of criteria and controls as follows:

- Collect and use information fairly
- Specify the purposes for which information is used
- 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
- Ensure the quality of the information used
- Ensure the rights of Data Subjects about whom information is held, can be exercised under the Act
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information 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

Rights of individuals include:

- The right to be informed that processing is undertaken
- The right of access to one's personal information
- The right to rectify information if it is incorrect
- The right to erase information
- The right to prevent processing in certain circumstances
- The right to obtain and use data for one's own purposes
- The right to object to data being used, such as for direct marketing

All trustees, staff and volunteers 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**

FVH 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 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 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 Act. 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 given below.

## **Privacy notice and consent policy**

FVH uses personal data for the purposes of managing the hall, bookings, finances, fundraising, running and marketing events of the hall and trustee and volunteer recruitment. Data may be retained for up to 7 years or longer where required (e.g. by our 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 Secretary at [ferringvh.sec@gmail.com](mailto:ferringvh.sec@gmail.com).

By making a hire booking with us, the hirer consents to us holding their relevant personal information on our systems. It is FVH's policy that hirer contact details and booking emails are held on a cloud based platform and not stored on any one laptop.

FVH will hold data regarding a booking in line with this policy. The hirer's surname will appear on the online calendar to identify the booking. Hirers have the right to opt out of having this information displayed by emailing the Booking Secretary at [ferringvh@gmail.com](mailto:ferringvh@gmail.com).

Consent forms, if used, will be stored by the Secretary in a securely held electronic or paper file.

## **Operational guidance for trustees, employees, volunteers and contractors**

### **Email**

All Trustees, staff and volunteers should consider whether an email (incoming or 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 secured securely.

Emails that contain an individual's personal information, which is no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" mailbox.

Where someone, not being a trustee, employee, volunteer or contractor, needs to be copied into an email e.g. a wider circulation list for an upcoming event, it is recommended that the **bcc** circulation option is used instead of the **cc** option to avoid their personal data (email address) being shared with others on the email circulation.

### **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 identity and are satisfied that providing the information requested would not lead to a data breach.
- 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 password. It is recommended that the password is changed regularly. Where sensitive data or financial information is held an encryption programme should be used.

It is FVH's policy that hirer contact details and booking emails are held on a cloud based platform and not stored on any one laptop.

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

When travelling by car ensure that the laptop is kept out of sight preferably in the boot and that the car is alarmed when unattended. Do not leave the laptop in your car for extended periods or overnight.

Do not leave your laptop unattended in public places such as restaurants, airports and hotels.

When travelling by public transport keep your laptop in your possession and do not place in luggage racks.

## **Data security and storage**

Store as little personal data as possible relating to FVH 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 laptop or server. The disk or memory stick should then be securely returned (if applicable), safely stored or wiped and securely disposed of.

It is FVH's policy that hirer contact details and booking emails are held on a cloud based platform and not stored on any one laptop.

## **Passwords**

Do not use passwords that are easy to guess. Passwords should contain both upper and lower case letters and preferably some numbers. Ideally passwords should be 6 characters or more in length.

Do not:

- Give out your password.
- Write your password somewhere on your laptop.
- Store your password somewhere in your laptop case.

## **Data storage**

Personal data should be stored securely and only accessible to authorised persons, such as trustees, staff and volunteers and only where necessary.

Information will be stored for as long as it is needed for the original purpose or required by statute and will be disposed off 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 off when no longer required.

All personal data held by an 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 or in order for Trustees to comply with their obligations e.g. regarding employment law, taxation, pensions or insurance. FVH does not employ staff currently.

## **Accident book**

A nominated trustee will check this regularly. Any page that has been completed will be removed, appropriate action taken and the page filed securely.

## **Photographs**

FVH may use general photographs of events with groups of adults at the village hall for publicity purposes in accordance with its lawful basis for using personal data. Photographs of children must not be used without the Explicit Consent of the parent or guardian.

FVH is aware that some individuals will not wish to appear in photographs or publicity material for personal reasons. Consequently, at any events involving large groups of people, where publicity photographs may be taken, a notice should be posted at the entrance, or an announcement made, providing an opportunity for people to avoid taking part or expressly refuse to take part in publicity photographs. At small events, verbal consent of individuals present should be obtained for their image to appear in any photographs or publicity material. 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 or other voluntary organisations in circumstances other than in furtherance of the management of FVH. Circumstances where the law allows FVH to disclose data (including sensitive data) without the Data Subject's Explicit Consent include:

- A. Carrying out a legal duty or as authorised by the Secretary of State for 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

FVH regards the law and correct treatment of personal information as very important to our reputation and 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 Subject asking for their Explicit Consent to disclose or share their personal data. We intend to ensure that personal information is treated lawfully and correctly.

## **Risk management**

FVH recognises the consequences of breaching data protection legislation, particularly that prejudice, harm or distress could be caused to individuals if their personal information is disclosed inappropriately. Trustees, staff and volunteers should be aware that they can be personally liable if they use an individual's personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of the FVH is not damaged through inappropriate or unauthorised access or sharing.

## **General questions and concerns**

If anyone has a general question about this policy or is unsure whether a matter might give rise to a data protection concern, please contact the Secretary, in the first instance, at [ferringvh.sec@gmail.com](mailto:ferringvh.sec@gmail.com).

## **Review**

This policy shall be circulated to all Trustees for information and review annually.

Approved by the Trustees on 15 March 2023