Founded in 1924 through a bequest by the late Mrs GAH Henty

Ferring Village Hall
90 Ferring Street
Ferring
BN12 5JP

DATA PROTECTION POLICY AND PROCEDURES

(GDPR Legislation effective from May 2018)

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 (PD) in order to carry on our work of managing Ferring Village Hall (FVH). The 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 FVH charity will remain 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 the 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 1998 and General Data Protection Regulations - the legislation that requires responsible behaviour by those using personal information.

Data Protection Officer - if appointed. The person responsible for ensuring that FVH follows its data protection policy and complies with the Act. FVH is not required to appoint a DPO.

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 Data Protection Act 1998.

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 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 this 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 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 in relation to the processing of personal data.

Applying the Data Protection Act with FVH

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 PD is only used for this purpose unless specific consent is given or the PD is already in the public domain. Access to personal information 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 FVH 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 credit card statement.

Any concerns about complying with a SAR need to be discussed promptly with the FHV'S named DP Contact 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 what personal 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 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 its operational needs or to comply with any legal requirements.
d. Ensure the quality of the information used.
e. Ensure the rights of people about whom information is held, can be exercised under the Act.

These rights include:

- The right to be informed that processing is undertaken.
- The right of access to one's personal information.
- 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 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.

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 & 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 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.

The privacy and consent policy are as follows:

"Ferring Village Hall uses personal data for the purposes of managing the hall, its bookings and finances, fundraising, running and marketing events of the hall, staff employment and its fundraising activities. Data may be retained for up to 7 years or longer where required (eg: 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 hall Secretary"

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

Operational Guidance:

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 PD personal information no longer required for operational use should be deleted from the personal mailbox and any "deleted items" mailbox.

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, it is recommended that bcc instead of cc is used to avoid their PD (email address) being shared through forwarding. (NOTE for explanation: To is used for action addressees, cc is used for information addressees and bcc is used for blind addressees (email address NOT shown).

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 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 & Portable Devices

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

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 them 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 PD as possible relating to FVH on your computer or laptop: only keep those files that are essential. PD 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.

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 our 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 will be stored securely and will only be accessible to authorised volunteers and staff.

Information will be stored for only as long as it is needed 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 or when trustees, staff or volunteers retire.

All PD held by an organisation must be non-recoverable from any computer which has been passed on/sold to a third party.

Information Regarding Employee 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:

The Secretary will check this regularly. Any page which 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 Hall for publicity purposes in accordance with its lawful basis for using PD. Photos of children must not be used without the written consent of the parent or guardian. However FVH 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 an opportunity for people to refuse taking part in publicity photographs. At small events the consent of individuals (verbal) should be obtained if their image is 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 FVH. Circumstances where the law allows FVH 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.

FVH regard the law and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. If an agency asks PD 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 their PD on. 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. Trustees, staff and volunteers should be aware that they can be personally liable if they use customer's PD 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.

Complaints Policy:

If you think we have failed to provide satisfactory levels of service please let us know. Your complaint will be taken seriously and we are committed to equal opportunity responsibilities:

You should write to the Secretary in the first instance. If you are not happy with the response you should then address your complaint to the Management Committee.

We will let you know, in writing or by telephone, when we have received your complaint. This will usually be within 10 working days.

You will receive a full written response in writing within twenty working days. If we cannot give a full reply within this time we will write and let you know why and how we are dealing with your complaint. If your complaint is complex we will aim to have a full reply to you within twenty-five working days.

Safety concerns that would endanger users will be dealt with immediately.

When complaining please state:

1. Your name and organisation.
2. Address including post code.
3. Telephone and email.
4. Tell us about your complaint (why are you not satisfied and what do you want us to do to put it right?)
5. Have you tried to resolve the complaint before (If yes then when and how?)
6. Any other comments

Signed. .....

Print Name.....

Organisation (if applicable).....

Date.....

Ferring Village Hall POLICY ON PUBLIC INTEREST DISCLOSURE (Whistle Blowing Policy)

The Ferring Village Hall is committed to ensuring the highest possible standards of care and the highest possible ethical standards in delivering the services it provides. This policy demonstrates the Committee's commitment to recognise and take action in respect of malpractice, illegal acts or omissions by the Committee members, Hall users and/or volunteers. It is the responsibility of all committee members and volunteers to ensure that if they become aware that the actions of other committee members, Village hall users or volunteers might compromise this objective, they will be expected to report the matter in the safe knowledge that this matter will be treated seriously and sensitively**.**

What might you need to report could include:

- Malpractice or ill treatment of individuals.
- Suspected fraud.
- Any criminal offence is, has or likely to be committed.
- Disregard for legislation (e.g. health and safety)
- Damage to the environment

Who should you report to:

- Any committee member (ideally recognising their sub-committee responsibilities).
- The Chairman or Secretary if there are personal issues or other serious confidentiality issues.

Responsibilities - Committee Members (either individually or collectively) must ensure that they:

- Take complaints seriously, act with sensitivity and confidentiality.
- Ensure that the concerned is aware that no subsequent action will be taken against them.
- Provide the concerned with the opportunity to speak with the Chairman if wished.
- Take appropriate measures to resolve the issue completely and sensitively.
- Recognise that the situation may be very difficult for the concerned individual.
- Reassure the concerned that they will be protected from reprisals or victimisation.

The concerned is to be provided with an initial written response within five working days, including details of any further action to be taken and a full written response within seven working days of the completion of the investigation.

If the concerned person is not satisfied with the outcome of the internal process the committee recognises the individual's right to pursue the matter further.

Concerns about the Chairman should, in the first instance, be considered by the Secretary or the trustee with the longest service on the committee.

Signed

Original signed and held by Secretary

Date: 9th January 2019

Chairman
Ferring Village Hall Committee