DARSHAM VILLAGE HALL MANAGEMENT COMMITTEE

Cheyney Green, The Street, Darsham, IP17 3FA

REGISTERED CHARITY NO: 230730

DATA PROTECTION & PRIVACY POLICY & 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 Darsham Village Hall (DVH). 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, and includes email, minutes of meetings, and photographs. The charity will remain the data controller for the information held. The trustees are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. Trustees 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 DVHMC 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 DVHMC 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 Protection Officer – the person responsible for ensuring that DVHMC follows its data protection policy and complies with the Act. [DVHMC is not required to appoint a DPO].

Data Subject – the individual whose personal information is being held or processed by DVHMC for example a donor or hirer. '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 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:
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 will let people know why we are collecting their data, which is for the purpose of managing the hall, its hiring's and finances. It is our responsibility to ensure the data is only used for this purpose.

Access to personal information will be limited to trustees.

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.

Responsibilities

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

a) Collection 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 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 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

DVHMC 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 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.

Privacy Notice and Consent Policy

The privacy notice and consent policy are as follows:

● Consent forms 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 (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. 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 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 and Portable Devices:

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

● 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.