CHIPPERFIELD VILLAGE HALL

Data Protection Policy

1. Introduction

We need to collect and use certain types of data in order to carry on our work of managing Chipperfield Village Hall. This personal information must be collected and handled securely. The Data Protection Act 1998 (DPA) and the UK General Data Protection Regulations (GDPR) govern the use of information about people (personal data). While the charity (Chipperfield Village Hall) will remain the data controller for the information held, Trustees, Committee members and any staff and volunteers are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR and anyone who has access to personal information will therefore be expected to read and comply with this policy.

2. Purpose

This policy sets out the Hall's 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, loss of privacy and financial loss if personal data is lost or stolen. This policy is designed to minimise the risks of these and to ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access to, and sharing of, peoples' data.

The following are definitions of the terms used:
Data Controller – the trustees who collectively decide what personal information Chipperfield Village Hall will hold and how it will be held or used.
Act – 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 the Hall follows its data protection policy and complies with the Act. Chipperfield Village Hall is not required to appoint a DPO and has not done so.
Data Subject – the individual whose personal information is being held or processed by the Hall, for example a hirer, contractor, Trustee.
'Explicit' consent – freely given, specific agreement by a Data Subject to the processing of personal information about them.
Processing – 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.

3. 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.

4. Applying the Data Protection Act within the charity

a) We collect people's data for the purpose of managing the hall, its hirings 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, Committee members and staff.

b) 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.

c) The Trustees of Chipperfield Village Hall acting collectively constitute the Data Controller under the Act, and are legally responsible for complying with Act, which means that they determine what purposes personal information held will be used for.

d) The Committee will take into account the legal requirements of the Act and ensure that they are properly implemented, including ensuring that information is collected and used fairly and appropriately and only to the extent needed to fulfil its operational needs or to comply with any legal requirements. The Committee will also ensure that people about whom information is held are able to exercise their rights under the Act including the right of access to their personal information and the right to correct, rectify, block or erase information which is regarded as wrong information. The Committee will also ensure that appropriate technical and organisational security measures are in place to safeguard personal information (see below, Data Security).

e) All Trustees, Committee members and staff are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

f) At this stage, Chipperfield Village Hall has not appointed a Data Protection Officer. If at some point it chooses to do so then that person will be named here in the policy document.

g) This policy and associated procedures 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 legal framework or required by the Charity Commission.

5. Data Security

Chipperfield Village Hall has a duty to ensure that appropriate measures are in place to prevent:

- Unauthorised or unlawful processing of personal data
- Unauthorised disclosure of personal data
- Accidental loss of personal data.

All trustees, committee members and staff must ensure that personal data is dealt with properly no matter how it is collected, recorded or used, and whether held on paper, on 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 age or religious beliefs etc. would be classed as personal data, and fall 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.

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

Phone Calls: 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 suitable encryption (strong password) and appropriately stored/secured.

Data Security and Storage: As little personal data as possible/necessary for operational reasons should be stored electronically. Personal data will be stored securely and will only be accessible to authorised Committee members. 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. 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, committee members or staff retire.

Authorised disclosure: There are a very limited set of circumstances where the law allows the charity to disclose data (including sensitive data) without the data subject's consent such as for example carrying out a legal duty or as authorised by the Secretary of State or protecting vital interests of a Data Subject or other person e.g. child protection.

Chipperfield Village Hall Committee
March 2024