



Oulton Village Hall (Charity no 522771)

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 Data in order to conduct our work of managing Oulton Village Hall. This personal information must be collected and handled securely.

The Data Protection act 1998(DPA) and the General Protection Regulations (GDPR) govern the use of information about people (personal data) (PD). PD can be held on electronic devices or in manual files and includes emails, minutes of meetings and photographs.

Oulton Village Hall Trustees are the data controller (DC) for the information held. The Trustees/volunteers are personally responsible for processing and using PD in accordance with the DPA/GDPR. Trustees/Volunteers who have access to PD will therefore be expected to read and comply with this policy.

Purpose

The purpose of this policy is to set out the commitment of Oulton Village Hall and procedures for protecting PD. Trustees regard the lawful and correct treatment of PD as very important to successful working, and to maintaining the confidence of all stakeholders. We recognise the risks to individuals of identity theft and financial loss if PD is lost or stolen.

The following are definitions of terms used:

Data Controller	The trustees who collectively decide what PD Oulton Village Hall will hold and how it will be held/used.
ACT	Means the Data protection act 1998 & the General Data Protection Regulations and the legislation that requires responsible behaviour by those using PD.
Data Subject	The individual whose personal Information is being held or processed by Oulton Village Hall.
Explicit Consent	Is a freely given, specific agreement by a Data subject to the processing of PD about him/her
Personal Information	Information about living individuals that enables them to be identified e.g. name, address. It does not apply to information about organisations but applies to named persons i.e. volunteers.
Personal Data	Shall be processed fairly/lawfully and in particular, shall not be processed unless specific conditions are met. 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. Shall be adequate, relevant and not excessive in relation to those purposes. Shall be accurate and kept up to date Shall not be kept for longer than is necessary Shall be processed in accordance with the rights of Data Subjects under the Act. Shall be kept secure by the Data Controller who takes action to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to Personal information. Shall not be transferred to a country or territory outside the European Economic Area unless that country 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 Oulton Village Hall

We will let people know why we are collecting their Data, which is for the purpose of managing Oulton Village Hall, its Hiring 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/volunteers.

Correcting Data

Individuals have a right to make a Subject Access request (SAR) to establish whether Oulton Village Hall 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. Any SAR must be dealt with within 30 Days. Data Controllers must first establish that the SAR is from an individual whose identity is confirmed by providing substantive evidence (i.e. Passport).

Responsibilities

Oulton Village Hall trustees are the data controller under the act, and through the Hall's management committee (MC) are responsible for compliance, the MC determines what purposes Personal Information held will be used for. The MC will take into account legal requirements and ensure that it is properly implemented through appropriate Management and application of criteria/controls.

- Collection of used 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 information used
- Ensure the rights of people about whom information is held can be exercised under the act.

These include

- 1) The right to be informed that processing is undertaken
 - 2) The right of access to one's personal information
 - 3) The right to prevent processing in certain circumstances
 - 4) 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 & fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.

All trustees/volunteers are aware that a breach of the rules and procedures in this policy may lead to action being taken against them.

Procedures for Handling Data & Data Security

Oulton Village Hall 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/volunteers must ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether the information is a paper record or held on an electronic device. 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 classified as personal data, and falls within the scope of the acts. It is therefore important that all individuals consider any information (which is not in the public domain) that can be used to identify an individual as personal data and observe the guidance below.

Privacy Notice and Consent policy

Consent Forms All consent forms will be stored in a securely held electronic or paper file.

Operational Guidance

Email: - All Hall trustees 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 an appropriate folder or printed and stored securely. Emails that are no longer required for operational purposes should be deleted from the relevant mailbox and the "deleted items box".

Phone Calls: - Phone calls can lead to unauthorised use or disclosure of personal information (PI/PD)

- Personal information should not be disclosed 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 telephone call asking for personal information to be checked or confirmed, be aware that the call may come from an unreliable source impersonating someone with a right of access.

Electronic Devices All electronic devices that hold PI/PD must be protected with a suitable encryption programme.

- Ensure all devices are locked (password protected) when left unattended at all times.
- If travelling, leave these devices out of site preferably in the boot.
- Never leave these devices in your vehicle overnight.
- Do not leave these devices unattended at any venue.
- If travelling on public transport, keep these devices with you at all times.

Data Security & Storage - Store as little as possible personal data on electronic devices, only keep files that are essential. Personal data received on disk/memory stick should be securely returned (if applicable), safely stored or wiped and securely disposed of.

Passwords - Do not use passwords that are easy to guess. All passwords should contain both upper and lower case letters and contain some numbers. Ideally passwords should be 8 characters in length or more.

- Never divulge your device(s) password
- Do not write your password(s) somewhere on your devices
- Do not keep passwords written down stored in your device case

Data Storage - Personal Data will be stored securely and only be accessible to authorised Trustees/Volunteers. 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 can be up to 7 years. Archived material such as minutes and legal documents will be securely stored indefinitely. Other correspondence and emails will be disposed of when no longer required or when trustees/volunteers retire. All personal data on electronic devices must be non-recoverable from these devices which have been passed/sold to a third party.

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

Data Subject Access Requirements – The hall may occasionally need to share data with other organisations in circumstances which are not in furtherance of the management of the Hall. The circumstances where legislation allows the Hall to disclose Data without the data subject's consent are:-

- Carrying out a legal duty or as authorised by the secretary of state protecting vital interests of a data subject or other person
- The data subject has already made the information public
- Conducting legal proceedings, obtaining legal advice or defending any legal rights.
- Monitoring for equal opportunities, i.e. race, disability

The Hall regards the lawful and correct treatment of personal information very important to successful working, and to maintain the confidence of all stakeholders. 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 data subjects, or they could be denied a service to which they are entitled. Trustees/volunteers should be aware that they can be personally liable if they use customer's personal data inappropriately. This policy is to ensure that the reputation of Oulton village Hall is not damaged through inappropriate or unauthorised access and sharing.