Great Bromley Village Hall

Registered Charity Number 301310

Data Protection Policy and Procedures

Introduction

Great Bromley Village Hall (GBVH) is committed to a policy of protecting the rights and privacy of individuals. We collect and use certain types of Data in order to carry on our work of managing GBVH. This personal information is collected and handled securely.

The Data Protection Act 1998 (DPA) and General Data Protection Regulation (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 emails, minutes of meetings, and photographs.

The 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 Data Protection Act and GDPR. Trustees, staff and volunteers who have access to personal information must therefore read and comply with this policy.

Purpose

The purpose of this policy is to set out the GBVH commitment to, and also the procedures for, protecting personal data. Trustees regard the lawful and correct treatment of personal information as crucial 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 village hall management committee which decides what personal information GBVH will hold and how it will be held or used.

Act means the Data Protection Act 1998 and General Data Protection Regulation - the legislation that requires responsible behaviour by those using personal information.

Data Protection Officer – the person responsible for ensuring that GBVH follows its data protection policy and complies with the Act.

Data Subject – the individual whose personal information is being held or processed by GBVH - 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 eight principles for processing personal data with which we comply.

Personal data:

- Shall be processed fairly and 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 purpose(s).
- Shall be accurate and, where necessary, 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 appropriate technical and other measures 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 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

Personal data held by Great Bromley Village Hall which falls within the scope of the DPA and GDPR is categorised below. We will ensure that the data is used only for the purposes described. Access to personal information will be strictly limited to those trustees, staff and volunteers who require the information in order to discharge their responsibilities.

a. Information provided by hirers and held within the hall booking and accounting system which is required to process bookings of the hall and associated payment.

The information we require to enable us to properly provide facilities for hire is collected on one document - the Great Bromley Village Hall Booking Form. Our lawful basis for collecting this information is to enable a contract to be drawn up between hirer and us (the supplier), as requested by the hirer.

i. What Information do we require?

Name, address, email address, telephone numbers and, for bookings where deposits are repayable, bank details

ii. How do we use this information?

We use this information to communicate with the hirer to ensure that the booking and invoicing process can function efficiently. Bank details are held to facilitate the return of any deposit provided. The information is held securely on Google Calendar and our Quickbooks professional accounts system both of which are user-ID and password protected.

iii. How long do we keep this information?

We keep personal data on Google Calendar for 2 years from the date of the last booking made. We keep information on the Quickbooks accounting system for a period of 7 years to satisfy external accounting requirements.

b. Information held about trustees some of which is required to be submitted to the Charity Commission in the Annual Return.

Full contact and certain personal details of all current trustees are held for the purposes of good administration and also to enable the hall secretary to complete the annual return to the Charity Commission, which is required by law. All data held for a trustee is deleted from the village hall systems and the Charity Commission database when a trustee stands down.

c. Details about events and associated points of contact on website calendars, Facebook and other media outlets.

Any data in this category is only published with the full approval of the event sponsor, organiser or point of contact whose consent would therefore be deemed to have been given.

d. Cookies used to track, save and store information on the user's computer about the user's interactions with and usage of the GBVH website.

Cookies allow the website to provide users with a more tailored experience. No personal information is gleaned from them and users are advised that if they wish to deny the use and saving of cookies on the GBVH website on to their computer's hard drive they should take the necessary steps within their web browser's security settings to block all cookies from this website and its external serving vendors.

e. Google Analytics used to collect data to monitor the website usage and improve its functionality.

The GBVH website uses tracking software to better understand how it is being used. The software will save a cookie to your computer's hard drive to track and monitor your engagement and usage of the website, but will not store, save or collect personal information.

f. Information on the 'Contact Us' form which a member of the public can use to send a message to the village hall bookings manager.

This information is held by the bookings manager until the email exchange is complete at which time all emails are permanently deleted.

g. Village Hall Email List.

We maintain an up to date email list of subscribers who have given their specific consent to receive emails from the village hall about events, fundraising activities and general news. Subscribers can request for their name to be removed from this list at any time.

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. We will deal with any SAR within 30 days and a copy of the information held on the applicant will be provided free of charge unless the request is manifestly unfounded or excessive in which case a charge will be made. Steps will 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

GBVH is the Data Controller under the Act and is legally responsible for complying with the Act, which means that it determines for what purposes personal information held will be used.

The management committee takes into account legal requirements and ensures through appropriate management that criteria and controls are properly applied. In particular it will:

a) Collect and use information fairly.

b) Specify the purposes for which information is used.

c) Collect and process appropriate information, but only to the extent that is needed to fulfil its operational needs or to comply with any legal requirements.

d) Ensure good quality and accurate information is 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.

The Data Protection Officer on the management committee is:

Name: Mrs Mary Fawcett (Bookings Manager)

Contact Details:
villagehallbookings@greatbromley.org.uk
or
The Data Protection Officer
Great Bromley Village Hall
Parsons Hill
Great Bromley
Colchester
Essex CO7 7JA

The Data Protection Officer is responsible for ensuring that the policy is implemented and has overall responsibility for ensuring that:

a) Everyone processing personal information understands that they are responsible for following good data protection practice.

b) Everyone processing personal information is appropriately trained to do so.

c) Everyone processing personal information is appropriately supervised.

d) Anybody wanting to make enquiries about handling personal information knows the process for doing so.

e) Any enquiries about handling personal information and dealt with promptly and courteously.

f) The charity lays down clearly how it handles personal information.

g) There is a regular review and audit of how the charity holds, manages and uses personal information.

h) There is a regular assessment and evaluation of methods and performance in relation to handling personal information.

This policy 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 Data Protection Act 1998 or General Data Protection Regulation.

In case of any queries or questions in relation to this policy please contact the Data Protection Officer.

Procedures for Handling Data & Data Security

GBVH has a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

a) Unauthorised or unlawful processing of personal data.
b) Unauthorised disclosure of personal data.
c) 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 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. 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 for Great Bromley Village Hall

The Privacy Notice for GBVH is given below:

Great Bromley Village Hall uses personal data for the purposes of managing the hall, its booking and finances, running and marketing events at the hall, staff employment, trustee documentation and its fundraising activities. Data may be held for up to 7 years for accounts purposes but data retention is regularly reviewed and when no longer required personal data will be deleted permanently from the village hall information systems. If you would like to know more about how we use your personal data or want to see a copy of information about you that we hold, please contact the village hall Data Protection Officer via:

Email: villagehallbookings@greatbromley.org.uk

Post: The Data Protection Officer
Great Bromley Village Hall
Parsons Hill
Great Bromley
Colchester
Essex
CO7 7JA

A consent notice is included on official emails associated with bookings and bookings enquiries, on the GBVH booking form and on all invoices. The requirement for it is detailed in the GBVH Conditions of Hire.

Consent forms and declarations from trustees will be stored by the Secretary in a securely held electronic or paper file.

Operational Guidance

Email:
All trustees, staff and volunteers must consider whether an email (both incoming and outgoing) needs 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.
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:
Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:
a) Personal information should not be given out over the telephone unless you have no doubts as the caller's identity and the information requested is innocuous.
b) If you have any doubts, ask the caller to put their enquiry in writing.
c) 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 another person 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, bars or any public venue.
- When travelling on public transport, keep them with you at all times and do not leave them in
- luggage racks or even on the floor alongside you.

Data Security and Storage:
Store as little personal data as possible 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 server or laptop. The disk or memory stick should then be securely returned (if applicable), safely stored or wiped and securely disposed of.
Always lock (password protect) your computer or laptop when left unattended.

Passwords:
Do not use passwords that are easy to guess. All your passwords should contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length.
Common sense rules for passwords are:
a) Do not give out your password.
b) Do not write your password somewhere on your laptop.
c) Do not keep it written on something stored in the laptop case.

Data Storage
Personal data will be stored securely and will only be accessible to authorised volunteers or staff.

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 7 years. For booking records this will be 2 years from the last booking received. For fundraising and events management this will be 2 years from the activity or event. For details of trustees this will be until the end of the trustee's term of office. For employee records see below.

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, staff or volunteers retire.

All personal data held for the 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, in order that trustees comply with their obligations e.g. regarding employment law, taxation, pensions or insurance.

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

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 charity. The circumstances where the law allows the charity 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 to protect the vital interests of a Data Subject or other person (eg 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.

We 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.

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 customers' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access and sharing.