BRUSHFORDPARISH HALL

REGISTERED CHARITY NO: 1176214

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 carry on our work of managing Brushford Parish Hall. This personal information must be collected and handled securely. 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 Data Protection Act 2018 (DPA) and General Data Protection Regulations (GDPR) govern the use of information about people (personal data). Brushford Parish Hall is not required to register with the Information Commissioners Office (ICO) but it is required to comply with the DPA and GDPR.

Brushford Parish Hall is not required to appoint a Data Protection Officer, the charity will remain the data controller for the information held. The trustees and volunteers are personally responsible for processing and using personal information in accordance with the DPA and GDPR. Trustees 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 Brushford Parish Hall Trustees' 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. We recognise the risks to individuals including identity theft and financial loss if personal data is disclosed or lost.

The following are definitions of the terms used in this Policy:

Information Commissioner's Office (ICO) - the ICO is responsible for implementing and overseeing the Data Protection Act 2018.

Data Controller – the trustees who collectively decide what personal information Brushford Parish Hall will hold and how it will be held or used.

Data Processor – an organisation which is responsible for processing personal data on behalf of a Controller. GDPR requires a Data Controller to ensure its contracts with processors comply with the GDPR.

Processing – means collecting, amending, handling, storing or disclosing personal information.

The Act - means the Data Protection Act 2018 and General Data Protection Regulations - the legislation that requires responsible behaviour by those using personal information.

Data Subject – the individual whose personal information is being held or processed by Brushford Parish Hall for example volunteers, trustees, donors or hirers.

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.

'**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 personal 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

Brushford Parish Hall does not collect nor retain any sensitive personal data.

A personal data breach – broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. If a personal data breach has occurred, the data controller needs to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then the data controller must notify the ICO; if it's unlikely then the data controller does not have to report it.

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 hire 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 and a limited number of volunteers.

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

Brushford Parish Hall is the Data Controller under the Act, and is legally responsible for complying with the DPA, which means that it determines what purposes personal information held will be used for. It may use suitable Data Processors for activities such as the website, emailing and other legal purposes but retains overall responsibility for compliance.

The management committee will take into account legal requirements to ensure that GDPR is properly implemented, and will, through appropriate management, enforce 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 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 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 Trustees will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

a) Everyone processing personal information understanding that they are contractually responsible for following good data protection practice
b) Everyone processing personal information being appropriately trained to do so
c) Everyone processing personal information being appropriately supervised
d) Anybody wanting to make enquiries about handling personal information knowing what to do
e) Dealing promptly and courteously with any enquiries about handling personal information
f) Describing clearly how the charity handles personal information
g) Regularly reviewing and auditing the ways it holds, manages and uses personal information
h) Regularly assessing and evaluating its 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 2018.

In case of any queries or questions in relation to this policy please contact enquiries@brushfordparishhall.org.uk

Procedures for Handling Data and Data Security

Brushford Parish 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 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 fall within the scope of the DPA. It is therefore important that all trustees and volunteers 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 Notice is as follows:

Privacy Notice

Brushford Parish Hall uses personal data for the purposes of managing the hall, its bookings and finances, running and marketing events at the Hall, and its fundraising activities. Data is not shared with any other organisation. Data may be retained for up to 7 years for accounts purposes and for longer where required by law or by the Hall's 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 cio@brushfordparishhall.org.uk

The Consent Policy is as follows:

Consent Policy

Brushford Parish Hall uses personal data for the purposes of managing hall bookings, finances, events and publicity without explicit consent. The charity relies on legitimate interest and legal obligations as the lawful reasons for everything except the contact details of volunteers (including trustees) and the recipients of email newsletters where explicit consent will be requested.

Trustees will also need to confirm on appointment that they consent to their personal data being used for the lawful purposes of managing the Hall and that regulatory and banking organisations may need (photographic) proofs of identity and address, dates of birth and national insurance numbers as well as contact details.

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

Data Storage:

Personal data will be stored securely and will only be accessible to authorised Trustees or volunteers. Secure storage includes on-line and off-line back up (including printed copies) to ensure data availability for the legal purposes of the charity.

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.

All personal data held for the organisation must be non-recoverable from any computer or other device which has been passed on/sold to a third party. Paper records must be completely destroyed, e.g. by shredding, before disposal.

Data Breaches:

The DPA requires a Data Controller to report certain breaches of data privacy to the ICO within 72 hours of becoming aware of the breach. Any Trustee or other volunteer who causes or identifies a breach must inform the Trustees/ the Data Protection Officer without delay in order to evaluate its severity. If a report is needed it should include a description of the nature of the personal data breach including, where possible:

- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Personal Data Breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

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.

Data Subject Access Requests:

We intend to ensure that personal information is treated lawfully and correctly.

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 such as 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

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.

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 and volunteers should be aware that they can be personally liable if they use anyone's 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.

POLICY APPROVED BY THE BRUSHFORD PARISH HALL TRUSTEES ON 17th February 2022

Date for next review: 16th February 2023

Appendix to the Data Protection Policy: Operational Do's and Don'ts

Email:

All 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 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:

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.

Computers, Laptops and Portable Devices:

All computers, laptops and portable devices that hold data containing personal information relating to the Hall must be protected with a suitable password. See below for more on Passwords

Ensure your device is locked (password protected) when left unattended, even for short periods of time. Keep your device out of sight in your home if you go out without it.

When travelling in a car, make sure the device 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 devices in your vehicle overnight.

Do not leave devices unattended in restaurants or bars, or any other venue.

When travelling on public transport, keep your device with you at all times, do not leave it in luggage racks or even on the floor alongside you.

Data Storage, Back Up and Recovery:

Data relating to Brushford Parish Hall as well as personal data relating to the Charity's activities should be held securely and regularly backed up. This will generally be achieved by using the shared drive (Google G-Drive) established for all BPH records and documents.

The capability to recover data and to resume processing after interruption should be tested periodically.

Passwords:

Common sense rules for passwords are:

- Do not give out your password
- Do not write your password somewhere on your laptop
- Do not keep it written on something stored in the laptop case.

If you share your device (for example, with a family member) you should have separate passwords that prevent access to Hall data by anyone other than yourself.

Do not use the same passwords for Brushford Parish Hall data and applications as you use for your own data and applications.

If more than one Trustee or volunteer uses a BPH application they should each have their own user identity and password. Do not share passwords between users.

Do not password protect individual files on Google GDrive: if you forget the password you will have locked out all users. (And never delete Google GDrive files that others may be using.)

Helpful guidance on passwords from GCHQ/National Centre for Cyber Security:

- When creating passwords, **make sure they can't be easily guessed** by people who know you, or derived from information gleaned from your social media profiles. Avoid the use of single dictionary words, or variations of these - use **three random words** instead. Don't bother replacing the letter 'O' with a zero (or replacing the letter 'I' with the number one) or any other techniques as hackers can exploit these rules.

- Always **use unique passwords for your work accounts**. Always change them immediately, and report it, if you think they may have been compromised or you notice anything else suspicious.

- **Store your passwords** rather than trying to remember them all. This enables you to use longer, stronger, unique passwords and change them whenever you want, without making life too hard for yourself. There are two ways you can do this:
    - **Use a password manager**. These can easily create and maintain long, complex, unique passwords for every service you use.
    - Alternatively, **write your passwords down on a piece of paper** that you guard very carefully (and keep separate from the devices they relate to). Disguise them if you can, and don't write your usernames alongside the passwords.