BELSTEAD VILLAGE HALL CHARITY TRUST
CHARITY NUMBER 272206

Data Protection Policy and Procedures

June 2024

CONTENTS

Introduction

Belstead Village Hall Charity Trust (BVHCT) is 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 Belstead Village Hall (BVH). 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 file, and includes email, minutes of meetings, and photographs.

The charity and trustees are data controllers for the information held. The trustees and volunteers are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. Trustees and volunteers who have access to personal information will therefore be expected to read and comply with this policy.

Purpose of the policy

The purpose of this policy is to set out the BVH 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. 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. The trustees recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

Definitions

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

Data Controller - the trustees who collectively decide what personal information BVH 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 Subject – the individual whose personal information is being held or processed by BVH 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.

Data protection principles

The Data Protection Act contains 8 principles for processing personal data with which all trustees and volunteers 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 Controllers 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 U.K. 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.

Roles and responsibilities of trustees and volunteers

The following rules and operational guidance apply to all trustees and volunteers when undertaking their roles on behalf of BVHCT and are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

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 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 in this policy.

Where needed, we will let people know why we are collecting their data, which is for the purpose of managing the hall, its hirings, finances, events management and fundraising activities. It is all our responsibility to ensure the data is only used for these purposes. If information is held for any other purpose specific consent to use the information will be needed from the individual concerned.

Access to personal information will be limited to trustees and volunteers.

All trustees and volunteers are legally responsible for complying with the relevant data protection legislation and for ensuring that any personal information held will be used solely for the purposes stated above, stored securely and disposed of securely when no longer required.

All trustees and volunteers are responsible for:

a) Collecting and using information fairly.
b) Where applicable specifying the purposes for which information is used.
c) Collecting and processing appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.
d) Ensuring the quality of information used.
e) Ensuring 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) Taking appropriate technical and organisational security measures to safeguard personal information.
g) Ensuring that personal information is not transferred abroad without suitable safeguards.
h) Treating people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
i) Setting out clear procedures for responding to requests for information.

BVHCT has a duty to ensure that appropriate technical and organisational measures 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.

The following operational guidance apply:

Paper records;

- Any paper records should be stored securely in a locked drawer or room and disposed of securely when no longer required.

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.

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

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, do not leave it in luggage racks or even on the floor alongside you.
- 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.
- 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: 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.

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 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.

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.

If any trustee or volunteer receives such a request this should be brought to the attention of the BVH committee to discuss and allow timely action to take place.

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 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
If any trustee or volunteer receives such a request this should be brought to the attention of the BVH committee to discuss and allow timely action to take place.

Privacy notices

The following privacy notice is included on the BVH website and is also shown on the hall notice board inside the entrance hall:
"Belstead Village Hall uses personal data for the purposes of managing the hall, it's bookings, finances, marketing and running events at the hall, using volunteers and it's fundraising activities. If you would like to know more about how we use your personal data or want to see a copy of the information we hold, please contact any member of the BVH committee"

The following information is included in our hirers form:
"Your personal data will be used solely to manage your booking for the hall and it's finances. It will not be shared with anyone else and will be disposed of when no longer required".

Accident Book

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

Other documentation

This policy is concerned with the proper use of personal information. There are other forms of documentation that trustees may hold to manage the running of the hall, which are unlikely to contain personal information. For example, meeting agendas, minutes and financial summary information that trustees are given at each meeting. The Secretary holds master copies of past agendas and minutes and the Treasurer holds master copies of all financial information. Therefore, it is best practice for other trustees to dispose of such documents in a timely manner.

Risk Management

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.
A GDPR mapping template is in place and completed by all trustees as and when felt necessary.
A data protection risk is included in the risk assessments that are reviewed annually by the BVH committee.

Policy updates

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.

SIGNED: DATE:

P Keen (Chairman)