



BRAYFORD VILLAGE HALL

DATA PROTECTION POLICY

Registered Charity No. 300780

INTRODUCTION

Brayford Village Hall Management Committee will adhere to a policy of protecting the rights and privacy of individuals. Certain types of Data need to be collected in order to carry on the work of managing the Hall. This personal information will be collected and handled securely.

1. PURPOSE

The purpose of this policy is to set out Brayford Village Hall's commitments and procedures for protecting personal data. The lawful and correct treatment of personal information is very important to successful working, and to maintaining the confidence of those with whom the Management Committee deal with. The risks to individuals of identity theft and financial loss if personal data is lost or stolen are recognised...

2. PROCEDURE

- (i) The Data Protection Act 1998 (DPA) and General Data Protection Regulations (GDPR) govern the use of information about people's personal data. Personal data can be held on computers, laptops and mobile devices, or in a manual file, and can include photographs as well as personal information, i.e. email, address, etc.
- (ii) The Charity will remain the data controller for the information held. Trustees/ volunteers and staff are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. Trustees/ volunteers and staff who have access to personal information will therefore be expected to read and comply with this policy.

3. DEFINITIONS

The following are definitions of the terms 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 Controller – Brayford Village Hall is not required to appoint a DPO

Data Subject – the individual whose personal information is being held or processed by Brayford Village Hall for example Trustees/ volunteers, staff, a donor or hirer.

'Explicit' consent – is a freely given, specific agreement by a Data Subject to the processing of personal information about them. Explicit consent is needed for processing "sensitive data", which includes:

- Racial or ethnic origin of the data subject
- Political opinions
- Religious beliefs or other beliefs of a similar nature

- Trade union membership
- Physical or mental health or condition
- Sexual orientation
- Criminal record
- 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.

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.

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

4. THE DATA PROTECTION ACT

This contains 8 principles for processing personal data with which The Management Committee must comply. Data will be:-

- i) processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
- ii) 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,
- iii) adequate, relevant and not excessive in relation to those purpose(s).
- iv) accurate and, where necessary, kept up to date,
- v) not kept for longer than is necessary,
- vi) processed in accordance with the rights of data subjects under the Act,
- vii) 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,
- viii) not 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.

5. APPLYING THE DATA PROTECTION ACT WITHIN THE CHARITY

The reasons Brayford Village Hall Management Committee collect personal data is for the purpose of managing the Hall, its hire thereof and finances. It is the Management Committee's responsibility to ensure the data is only used for this purpose. Access to personal information will be limited to trustees and, staff.

6. CORRECTING DATA

- i) 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.

- ii) 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.

7. RESPONSIBILITIES

- i) Brayford Village Hall_Management Committee is the Data Controller under the Act, and is legally responsible for complying with Act, which means that it determines what purposes personal information held will be used for.
- ii) The management committee will take into account legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls.
- iii) Collection and use information fairly.
- iv) Specify the purposes for which information is used.
- v) Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements.
- vi) Ensure the quality of information used.
- vii) Ensure the rights of people about whom information is held, can be exercised under the Act. These include:
 - The right to be informed that processing is undertaken.
 - The right of access to one's personal information.
 - The right to prevent processing in certain circumstances, and
 - 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 and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
 - 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.

8. PROCEDURES FOR HANDLING DATA & DATA SECURITY

- i) Brayford Village Hall Management Committee 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

- ii) All trustees, volunteers and staff 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.
- iii) 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.
- iv) It is therefore important that all trustees, volunteers and 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.

9. PRIVACY NOTICE AND CONSENT POLICY

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

10. OPERATIONAL GUIDANCE EMAIL:

- i) All trustees, volunteers and staff 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.
- ii) Emails that contain personal information no longer required for operational use should be deleted from the personal mailbox and any "deleted items" box.

11. PHONE CALLS:

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- i) 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.
- ii) If you have any doubts, ask the caller to put their enquiry in writing.
- iii) 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.

12. LAPTOPS AND PORTABLE DEVICES:

All laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program (password). Steps should be taken to ensure:-

- Laptops are locked (password protected) when left unattended, even for short periods of time.
- When travelling in a car, ensure the laptop is out of sight, preferably in the boot.
- If a laptop is in an unattended vehicle at any time, to put it in the boot, and check all doors are locked and any alarm set.
- Laptops or portable devices are never left in a vehicle overnight.
- Laptops or portable devices are never left unattended in restaurants or bars, or any other venue.
- When travelling on public transport, to keep it with the person at all times – never leave it in luggage racks or on the floor.

13. DATA SECURITY AND STORAGE:

The following will apply:-

- To store as little personal data as possible on the computer or laptop; only keeping 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.
- To always lock (password protect) the computer or laptop when left unattended.

14. PASSWORDS:

Never use passwords that are easy to guess. All passwords should contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length.

Protecting 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.

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 up to 7 years. 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.

15. 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. This is in order that trustees comply with their obligations e.g. regarding employment law, taxation, pensions or insurance.

16. ACCIDENT BOOK:

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

17. DATA SUBJECT ACCESS REQUESTS:

- i) Occasionally data may need to be shared 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.
- ii) The circumstances where the law allows the charity to disclose data (including sensitive 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 e..g. child protection

- The Data Subject has already made the information public
 - Conducting any legal proceedings, obtaining legal advice or defending any legal rights
 - Monitoring for equal opportunities purposes – i.e. race, disability or religion
- iii) The Management Committee 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. The Management Committee therefore intend to ensure that personal information is treated lawfully and correctly.

18. RISK MANAGEMENT:

- i) 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.
- ii) Trustees/ volunteers and staff 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.

19. POLICY REVIEW

The Village Hall Management Committee will carry out an annual review of this policy