WEST HILL VILLAGE HALL

Registered Charity No. 1160370

DATA PROTECTION POLICY

FEBRUARY 2021

CONTENTS **Page**

Data Protection Policy and Procedures

1. Introduction

This policy (including Appendix A) controls the protection of rights and privacy of individuals in respect of data handling at West Hill Village Hall (WHVH), which is a Charitable Incorporated Organisation (CIO) and managed by its Trustees. The Trustees have been guided by ACRE Information Sheet No. 4 relating to 'Data Protection'.

We are committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of data to carry on our work of managing WHVH. 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, photographs and recorded images.

The charity will remain the data controller for the information held. The Trustees are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. Trustees who have access to personal information will therefore be required to read and sign to confirm they have read and will comply with this policy.

2. Statement of Purpose

The purpose of this policy is to set out the WHVH commitment and procedures for protecting personal data. The Trustees regard the lawful and correct treatment of personal information as important 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. Definitions of the terms used in this document can be found at Appendix A.

3. 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 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 the Trustees. Please refer to our CCTV Policy in relation to applying the DPA for recorded images.

4. 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. The Trustees reserve the right to apply a reasonable charge for any

administrative costs incurred when complying with a request if it is manifestly unfounded or excessive of if an individual requests further copies of their data.

5. Responsibilities

WHVH is the Data Controller under the Act, and is legally responsible for complying with the Act, which means that it determines what purposes personal information held will be used for. The Trustees will consider legal requirements and ensure that it is properly implemented, and will through appropriate management, 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 (see 4. above).

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

6. Procedures for Handling Data & Data Security

WHVH 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 will therefore ensure that personal data is dealt with properly no matter how it is collected, recorded, or used. This applies whether the information is held on paper, in a computer or recorded by some other means e.g. tablet, mobile phone, CCTV camera.

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 ensure any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data observe the guidance given below.

7. Operational Guidance

Email: All the Trustees will 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 must be saved into the appropriate folder or printed and stored securely.

Emails that contain personal information no longer required for operational use, will 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 will be taken:

• Personal information will not be given out over the telephone unless there are no doubts as to the caller's identity and the information requested is innocuous.

• Where there is doubt, the caller will be asked to put their enquiry in writing.

• We recognise a phone call asking for personal information to be checked or confirmed may come from someone impersonating someone with a right of access.

Desktop Computers, Laptops and Portable Devices: All laptops and portable devices that hold data containing personal information will be protected with a suitable encryption program (password).

We will ensure laptops are locked (password protected) when left unattended, even for short periods of time.

When travelling in a car, the laptop will remain out of sight, preferably in the boot and will never be left in a vehicle overnight.

8. Data Security and Storage:

We will store as little personal data as possible on computers or laptops; only those files that are deemed essential will be kept. Personal data received on disk or memory stick will be saved to the relevant file on the server or laptop. The disk or memory stick will then be securely returned (if applicable), safely stored or wiped and securely disposed of.

Data Storage:

Personal data will be stored securely and will only be accessible to authorised Trustees.

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 retire.

We will ensure all personal data held for WHVH is non-recoverable from any computer which has been passed on/sold to a third party.

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

9. 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.

We regard the lawful and correct treatment of personal information as important to successful working, and to maintaining the confidence of those with whom we deal.

We will ensure that personal information is treated lawfully and correctly.

10. 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. The Trustees are 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.

APPENDIX A

The following are definitions of the terms used in this document, or otherwise in the Act (as defined below):

The Trustees – in the context of this policy, any reference to 'The Trustees' also encompasses the roles of Bookings Secretary, Hall Manager and Treasurer.

Data Controller - the Trustees who collectively decide what personal information WHVH 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 Protection Officer – the person responsible for ensuring that WHVH follows its data protection policy and complies with the Act. [WHVH is not required to appoint a DPO].

Data Subject – the individual whose personal information is being held or processed by WHVH 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 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.