WEST PECKHAM VILLAGE HALL CIO

Data Protection Policy

1. Introduction

The UK General Data Protection Regulation (**UK GDPR**) is the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) as defined in the Data Protection Act 2018 which governs Personal Data. WPVH is the Data Controller for Personal Data.

This Data Protection Policy sets out how WPVH will handle the Personal Data of hirers, prospective hirers, contractors, suppliers, Trustees and volunteers and other third parties.

WPVH will ensure that it treats Personal Data lawfully and correctly. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that WPVH takes seriously. A data protection breach can cause harm or distress to Data Subjects where their information is released to inappropriate people or they could be denied a service to which they are entitled. All Trustees and volunteers are aware that they may be personally liable if they use individuals' Personal Data inappropriately. This Policy is designed to minimise the risks and to ensure that the reputation of WPVH is not damaged through inappropriate or unauthorised access and sharing.

2. Definitions

WPVH means West Peckham Village Hall CIO.

Trustees means the trustees of WPVH.

Personal Data means any information relating to an identified or identifiable natural person (the **Data Subject**). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Contact Information means a person's name (including any preferences about how they like to be called); postal address; telephone and/or mobile numbers; e-mail addresses; and social media IDs/User Names (*eg:* Facebook, Skype, Hangouts, WhatsApp).

Processing or **Processed** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Consent of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to them; silence, pre-ticked boxes or inactivity will not be sufficient to indicate Consent.

Special Categories of Personal Data means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

References to the **Trustees and volunteers** includes employees (if any).

The definitions of other terms used in this Policy are the same as the definitions of those terms detailed in Article 4 UK GDPR.

3. Principles of the UK GDPR

WPVH will adhere to the 8 principles relating to the Processing of Personal Data set out in the UK GDPR which requires Personal Data to be:

a) Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);

b) collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation);

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);

d) accurate and, where necessary, kept up to date. Every reasonable step will be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay (accuracy);

e) kept in a form which permits identification of a Data Subject for no longer than is necessary for the purposes for which the Personal Data is processed or to fulfil legal requirements (storage limitation);

f) Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (security, integrity, and confidentiality);

g) not transferred to another country (if at all) without appropriate safeguards in place (transfer limitation); and

h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's rights and requests).

4. Lawful Processing

WPVH may only Process Personal Data (including Contact Information) for specific purposes, these include:

a) where the Data Subject has given their Consent;

b) the Processing is necessary for the performance of a contract with the Data Subject;

c) to meet WPVH's legal compliance obligations as is usually the case of Special Category Data;

d) to protect the Data Subject's vital interests;

e) to pursue WPVH's legitimate interests (or those of a third party) for the purpose of operating efficiently, effectively and economically except where they are overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

5. Individual Rights

This Policy and the identity and contact details of WPVH as the Data Controller, will be publically available on WPVH's website. Data Subjects have other rights in relation to their Personal Data, these include:

a) The right to request access to their Personal Data held by WPVH by submitting a subject access request, this includes the right to find out whether WPVH holds their Personal Data and the right to receive a copy of their Personal Data;

b) The right to require WPVH without undue delay to rectify any inaccurate or incomplete Personal Data concerning them;

c) Except where the Personal Data is held pursuant to a legal obligation, the right to require WPVH to erase Personal Data (the right to be forgotten) if it is no longer necessary in relation to the purposes for which it was collected or Processed;

d) The right to restrict Processing in specific circumstances;

e) The right to object:

   i. to Processing concerning them unless it is justified on the basis of WPVH's legitimate interests or pursuant to a contractual obligation;

   ii. to the use of Personal Data for direct marketing purposes;

f) The right to withdraw Consent at any time, where relevant;

g) The right to lodge a complaint with the supervisory authority;

h) The right to know of the existence of automated decision making, including profiling; and

i) The right, with certain exceptions, to receive notification of a data security breach.

6. Operational Policies and Procedures – the context

WPVH is a small charity holding a small amount of data on a limited number of individuals.

The Trustees understand and accept their responsibility under the UK GDPR to hold all Personal Data securely and use it only for legitimate purposes with the knowledge and approval of the Data Subjects.

By the following operational policies and procedures, the Trustees undertake to uphold the principles and requirements required by law in a manner which is proportionate to the nature of the Personal Data being held by WPVH. The policies are based on the Trustees' assessment, in good faith, of the potential impacts on both WPVH and its Data Subjects of the Personal Data held by WPVH being stolen, abused, corrupted or lost.

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

6.1 Accountability

a) WPVH must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. WPVH is responsible for, and must be able to demonstrate, compliance with the data protection principles.

b) WPVH may use general photographs of events with groups of adults at the hall for publicity purposes in accordance with its lawful basis for using Personal Data. Photos of children must not be used without the written consent of the parent or guardian. However, WPVH is aware that for some individuals publicising their location could place them or their families at risk. Consequently, at large events at which publicity photos may be taken, a notice should be posted at the entrance or an announcement made, providing opportunity for people to refuse taking part in publicity photographs. At small events the consent of individuals (verbal) should be obtained if their image will be clearly identifiable. Hirers are encouraged to comply with this Policy;

c) In general, sharing of Personal Data with third parties is not permitted unless certain safeguards and contractual arrangements have been put in place. It may be necessary to share Personal Data with other agencies such as the local authority and other voluntary agencies (eg, to protect vital interests such as child protection, to conduct legal proceedings or to monitor equal opportunities).

6.2 Data Retention Policy

Personal Data shall not be retained for longer than:

a) In the case of Personal Data held by Consent, the period for which the Data Subject consented to WPVH holding their data;

b) In the case of Personal Data held by legitimate interest of WPVH, the period for which that legitimate interest applies. For example, in the case of Data Subjects who held a role, such as a Trustee or volunteer, the retention period is that for which WPVH reasonably has a legitimate interest in being able to identify that individual's role in the event of any retrospective query about it;

c) In the case of Personal Data held by legal obligation, the period for which WPVH is legally obliged to retain the Personal Data;

d) In the case of financial records held for up to 7 years.

WPVH shall regularly – not less than every 12 months – review the Personal Data which it holds and remove any Personal Data where retention is no longer justified. Such removal shall be made as soon as is reasonably practicable after retention of the Personal Data was identified as no longer justified.

6.3 **Emails**

All Trustees and volunteers should 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 the appropriate folder or printed and stored securely. Emails that contain Personal Data should only be kept in accordance with the Data Retention provisions in clause 6.2 and otherwise deleted from the Trustee or volunteer mailbox and any "deleted items" box. Where someone not a Trustee, employee or contractor needs to be copied into an email e.g. a wider circulation list for a forthcoming event, bcc is preferable to cc.

6.4 **Phone Calls**

Phone calls can lead to unauthorised use or disclosure of personal information. Personal Data should not be given out over the telephone unless the caller's identity is certain and the information requested is innocuous. A caller should put their enquiry in writing if there are any doubts as to their identity.

6.5 **Laptops and Portable Devices**

Laptops and portable devices that hold Personal Data must be protected with a suitable password which is changed regularly. Where any Special Category of Personal Data or financial information is held an encryption program should be used. Laptops and portable devices should be locked (password protected) when left unattended. All Personal Data held for the organisation must be non-recoverable from any computer which has been passed on or sold to a third party.

6.6 **The Accident Book**

The Accident Book will be checked regularly. Any page which has been completed will be removed, appropriate action taken and the page filed securely and then be held in accordance with the other provisions of clause 6.2.

6.7 **Training**

The Trustees will periodically undergo appropriate training commensurate with the scale and nature of the Personal Data that WPVH holds and Processes under the UK GDPR.

7. Reporting a Data Breach

7.1. The UK GDPR requires Data Controllers to notify any Personal Data breach to the Information Commissioner's Office unless the breach is unlikely to result in a risk to the freedoms and rights of natural persons and, in certain instances, to the Data Subject.

7.2. WPVH has put in place procedures to deal with any suspected Personal Data breach and will notify the Data Subject or any applicable regulator where it is legally required to do so.

West Peckham Village Hall CIO
September 2023