Data Protection and General Data Protection Regulations Policy

1.0 Introduction and Purpose

The Trustees of Watford Village Hall (WVH) 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 intend to ensure that personal information is treated lawfully and correctly.

1.1 The Trustees of Watford Village Hall are defined by legislation as Data Controllers.

1.2 The purpose of this policy is to ensure that we comply with Data Protection Act (DPA) 1998 and the General Data Protection Regulations (GDPR) legislation 2018. This legislation governs 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 e-mail, minutes of meetings and photographs.

This legislation concerns any personal data that the Village Hall Trustees collect as part of their function.

1.3 Trustees understand that the lawful and correct treatment of personal information is important to successful, trust-based working.

2.0 Personal Data

2.1 The purpose of the legislation is to protect an individual from unauthorised access or use of their personal data which could result in identity fraud, financial loss or reputational loss.

3.0 Our Commitment

3.1 We will let people know why we are collecting their data, which will be for the purposes of managing the hall, lettings and finances and for any purposes that the law may require. We will not pass on any personal data that we collect or hold without the specific consent of the individual(s) concerned or unless the law demands that we do so. Access to personal information will be limited to current Trustees only.

3.2 Each individual whose personal data we hold has the following rights:

- The right to be informed of any processing that is undertaken
- The right of access to their own information that we hold
- The right to prevent processing in certain circumstances
- The right to correct, rectify, block or erase information which is regarded as incorrect

- The right to be removed from our database on request (unless the information we hold is necessary for financial, audit or legal purposes)

4.0 Responsibilities

4.1 We are not required to appoint a Data Protection Officer (DPO) however the Trustee with specific responsibility for Data Protection is Janine Brooks.

4.2 The Treasurer is responsible for renewing the Village Hall Council's Data Protection registration.

4.3 All Trustees are responsible for holding personal data that they use in connection with their role securely. This means keeping any paperwork in a locked filing cabinet and using personal computer devices that are password protected and have up to date anti-virus and malware protection.

4.4 All Trustees are responsible for ensuring that they only use personal data collected as part of their function.

4.5 Trustees are aware that in the event an individual makes a request for the personal data we hold about them this could include emails sent from their personal email account if it is regarding village hall business.

5.0 Privacy Statement

5.1 *General Privacy Statement* - The Village Hall Trustees uses personal data for the purposes of managing the hall and holds information regarding Trustees, hall bookings, suppliers and contractors, volunteers, running fundraising events, donations and financial information. We do not use personal data for any other purposes. Personal data will be retained for 7 years for financial purposes and for 1 year for any other purpose. The exception is that minutes of meetings that contain names will be retained indefinitely for the purposes of providing a historic record of village hall.

If you would like to find out more about how we use your personal data or want to see a copy of the information that we hold about you then please contact our Secretary: Janine.brooks47@gmail.com

5.2 *Web Site Privacy Statement* - By using our website, you agree to us placing cookies on your computer. Cookies are small text files created by websites you have visited that store browsing information like the pages you visit. The next time you visit the site, the cookie will tell the site that you have been there before. We use this information to improve our website and enhance your experience on our site, for example to avoid showing you information or screens you have already seen. We use two types of cookies:

- First-party cookies are set by the site you are visiting

- Third-party cookies come from other sites that have items embedded in our pages (for example Google Analytics which we use to monitor visitors to our web site)

Please note that cookies cannot harm your computer and the cookies we create do not store any information that could personally identify you."

5.3 *CCTV Privacy Statement* - The use of CCTV is covered by both Data Protection and Freedom of Information legislation. The village hall uses CCTV monitoring 24 x 7 for the purposes of deterring and preventing crime and protecting our premises. CCTV footage is not used for any other purposes but images captured will be passed on to the police where appropriate. In general, CCTV footage is stored for around 72 hours and is then overwritten.

5.4 *Trustee Details Privacy Statement* - Trustee names will be published on the web site but not their addresses or telephone numbers.

In meeting minutes, Trustees will be referred to by name but no other personal details will be used. In the event that it is necessary to minute more than just a Trustees' name, then any other details will be redacted when the minutes are made public.

5.5 *Accident Book Privacy Statement* - Accident records containing personal data will not be left in the Accident Book and will be removed and stored securely.

6.0 Data Breaches

A data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It is a legal requirement that certain types of data breach are reported to the Information Commissioner's Office 0303 123 1113 within 72 hours of the data breach occurring.

It is unlikely that the Village Hall Council will experience a major data breach because of the very limited personal data it holds but Trustees are made aware of this requirement through this policy.

Specifically, Trustees will need to report to the Chairman if their computer, tablet, mobile phone, memory stick etc. used for village hall purposes is stolen, or if the same applies to paper files held.

7.0 Subject Access Requests

Any individual may contact any Village Hall Trustee to request full details of the personal information we hold about them. This is called a Subject Access Request (SAR).

Requests should be passed to the Secretary who will acknowledge receipt and co- ordinate a response within the 30-day timescale.

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 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.

Operational Guidance

E-mail:

All trustees and volunteers should consider whether an e-mail (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.

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 some- one impersonating someone with a right of access.

Laptops and Portable Devices:

- All laptops and portable devices that hold data containing personal data 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.

Data Security and Storage:

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.

Passwords:

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.

Protect Your Password: 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 individuals.

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.

Date to be reviewed: January 2023

Appendix A – Definition of terms

Data Controller - the trustees who collectively decide what personal information WVH 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 WVH follows its data protection policy and complies with the Act. [WVH is not required to appoint a DPO].

Data Subject – the individual whose personal information is being held or processed by [WVH] 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 (data) – 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.

Appendix B – The 8 Data Principles

First principle - Personal data must only be used for the legitimate purpose for which it was originally collected.

Second principle - Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. It cannot be further processed or shared with others in a manner incompatible with those purposes without consent from the individual. Consent can be withdrawn at any time.

Third principle - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.

Fourth principle - Personal data shall be accurate and, where necessary, kept up to date.

Fifth principle - Personal data processed shall not be kept for longer than is necessary for that purpose or those purposes.

Sixth principle - Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.

Seventh principle - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Eighth principle - Personal data 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 data.