



# CMH Data Protection Policy

## 1. Introduction

1.1 Clenchwarton Memorial Hall ( CMH) takes seriously its responsibilities with regards to the collection and processing of personal data. We are committed to protect the rights and privacy of individuals.

1.2 CMH complies with the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) in line with our aims and objectives and recruitment of staff/volunteers.

1.3 This policy applies to anyone who, in the process of their work with CMH, collects and holds personal data. Anyone who deals with personal data is legally required to comply with the Act.

## 2. Data Principles

2.1 The Data Protection Act contains eight principles for processing personal data which must be followed;

### **Personal data:**

- Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met
- 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
- Shall be adequate, relevant and not excessive in relation to those purpose(s).

- Shall be accurate and, where necessary, kept up to date,
- Shall not be kept for longer than is necessary,
- Shall be processed in accordance with the rights of data subjects under the Act,
- 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,
- 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.

### 3. Applying the Data Protection Act

3.1 CMH collects personal data for the following reasons;

- In connection with the recruitment and employment of individuals, their management and care (including volunteers).
- In connection with our support services provided to our hirers to allow us to comply to our Aims and Objectives
- In connection with our booking system provided by Lemon Booking

3.2 CMH will let people and hirers know why we are collecting data, and it is our responsibility to ensure the data is only used for this purpose

3.3 Access to personal data will be limited to the chair, treasurer and secretary. **And the Lemon Booking System?**

3.4 CMH will hold personal data for **10** years from the time of initial contact or until the individual asks for their details to be removed

3.5 Personal data will be stored securely and will only be accessible to authorised parties

3.6 If requested to do so by an individual CMH will remove all data related to them immediately

### 4. Operational Guidance

4.1 All Trustees, staff 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.

4.2 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.

4.3 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) and not 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.

4.4 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.

4.5 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. Advice from the Nation Cyber Security Centre is to create passwords based on three random words and add a Symbol and or number.

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.

4.6 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 seven 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.

4.7 Information regarding a volunteer/ self-employed person or a former volunteer/ self-employed person, 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, in order that Trustees comply with their obligations e.g. regarding employment law, taxation, pensions or insurance.

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

## **5. Responsibilities**

5.1 The Trustees/ Management Committee are responsible for ensuring that all staff/volunteers are aware of the data protection policy and have been provided with appropriate training, and guidance to ensure compliance.

5.2 Anyone who collects and holds personal data on individuals is legally required to comply with the Act

Clenchwarton Memorial Hall Management Committee

Adopted: July 2026

Review Date: July 2027

