Comberton Village Institute Trust

Charitable Incorporated Organisation 1189495

Data Protection Guidance and Declaration

The Trustees of the Comberton Village Institute Trust are collectively (and legally) responsible for processing and using personal information in accordance with the Data Protection Act 1998 (DPA), General Data Protection Regulations (GDPR) and the Data (Use and Access) Act 2025. This includes responsibility for ensuring that our Data Protection Policy is implemented and for regularly reviewing and auditing the ways we hold, manage and use personal information. In addition, the trustees have overall responsibility for ensuring that everyone processing personal information (including employees and volunteers) understands that they are responsible for following good data protection practice.

This document is to be read (in conjunction with the CVIT Data Protection Policy) by all trustees, staff and volunteers who have access to personal information, and has been written to help you understand your responsibilities and to provide advice and guidance on how to ensure compliance. You will be asked to review this once a year and to confirm that you are meeting your obligations. This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with current legislation.

Data Definition and Collection

See CVIT's Data Protection Policy for this information.

Operational Guidance

Email:

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.

Whilst explicit consent is no longer required to send emails to people whose details we have, as long as the emails relate to similar activities (e.g. cinema/opera), an opt-out option must be included in the mail, the lawful basis on which we have collected their data must be clarified in the email (e.g. 'because you attended the cinema and agreed to join our mailing list') and when/how people opted in or were added to the mailing list must be documented.

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 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.

Laptops and Portable Devices:

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) 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.

Information must be stored for only as long as it is needed or required by statute and must be disposed of as appropriate. For financial records this will be up to seven years. Information regarding an employee or a former employee will be kept indefinitely. Archival material such as minutes and legal documents can be stored indefinitely. Other correspondence and emails must be deleted/destroyed 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.

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.

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