



Colne Valley Help Data Protection GDPR Policy

January 2021

Reviewed 30th June 2025

Approved 11th July 2025

Colne Valley Help – Data Protection GDPR Policy

Outline

This document is a statement of the aims and principles of Colne Valley Help (afterwards referred to as CVH), for ensuring the confidentiality of sensitive information relating to trustees, volunteers, users and staff in accordance with the requirements of the Data Protection Act 2018 which is the implementation of the EU General Data Protection Regulation (GDPR).

CVH complies with its obligations under the GDPR by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data

Introduction

CVH needs to keep certain information about its employees, trustees, volunteers, staff¹ (when relevant), and other users to allow it to monitor demand and take up of the service and health and safety, for example, and for use in relation to the everyday running of CVH.

In time it may also be necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, CVH must comply with the Data protection principles which are set out in the Data Protection Act 2018 (the 2018 Act).

In summary these state that personal data shall be:

- used fairly, lawfully and transparently
 - used for specified, explicit purposes
 - used in a way that is adequate, relevant and limited to only what is necessary
 - accurate and, where necessary, kept up to date
 - kept for no longer than is necessary
 - handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage
- and:
- that CVH are accountable for being able to demonstrate their compliance with GDPR

CVH trustees, volunteers and all staff or others who process or use personal information must ensure that they follow these principles at all times.

There is stronger legal protection for more sensitive information, such as:

- Race or ethnic background
- Political opinions
- Religious beliefs
- Trade union membership

¹ This document includes references to staff – at the time of writing this policy CVH is not able to employ staff. Staff are included here so that policy is relevant if CVH does come to employ staff.

- Genetic
- Biometrics (where used for identification)
- Health
- Sex life or orientation

Use and disclosure of Personal Information

CVH will never pass on Personal Information for marketing purposes to anyone. We are currently not using email or websites for personal information. However, we do use encrypted messages such as WhatsApp with limited information.

If you decide to instruct us to cease using your Personal Information as contemplated in this Policy, and notify us either in writing or by email, we shall destroy any retained personal information, unless it legally required to be held on file (e.g. Gift Aid details).

If you contact CVH, we reserve the right to keep a record of that correspondence and incorporate the information it contains into our database.

If we are required by law to provide information to a third party concerning your activities whilst using the service we shall do so.

Status of this Policy

This policy does not form part of the contract of employment for staff, or membership of the Trust, but it is a condition of employment that employees / charity members / volunteers / trustees will abide by the rules and policies made by CVH from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controllers

CVH as a body is the Data Controller under the 2018 Act, and the Trustees are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day-to-day matters.

CVH has four Designated Data Controllers: They are The Chair, Matthew Mcloughlin, Treasurer Stephanie Watson and Trustees Fiona Russell and Lee Seacombe

Any individual who considers that the Policy has not been followed in respect of personal data about himself or herself should raise the matter with one of the Designated Data Controllers.

Data Security

All staff / volunteers and trustees handling data must ensure that:

- Any personal data is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or

- If it is computerised, be coded, encrypted or password protected both on a local hard drive that is regularly backed up and on cloud storage; and
- If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

All data breaches are reported to the monthly meeting of the CVH Board.

Rights to Access Information

All individuals are entitled to:

- be informed about how their data is being used
- access their own personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of their data
- data portability (allowing subjects to get and reuse data for different services)
- object to how their data is processed in certain circumstances

Individuals also have rights when an organisation is using their personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests

CVH will, upon request, provide all relevant users with a statement regarding the personal data held about them. This will state all the types of data the CVH holds and processes about them, and the reasons for which they are processed.

All relevant users have a right under the 2018 Act to access certain personal data being kept about them either on computer or in certain files. Any person who wishes to exercise this right should contact the Designated Data Controller.

CVH aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 1 month² of receiving the request, as required by the 2018 Act.

These rights are set out in our Privacy Notice

Subject Consent

In many cases, CVH can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the 2018 Act, express consent must be obtained. Agreement to CVH processing some specified classes of personal data is a condition of acceptance of employment for staff. This includes information about previous criminal convictions.

² for complex request this timescale can extend up to 3 months by agreement

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to operate other CVH policies, such as the Equal Opportunities Policy. Because this information is considered sensitive under the 2018 Act, such persons will be asked to give their express consent for the CVH to process this data.

Retention of Data

CVH has a duty to retain some personal data for a period of time following their departure from the Trust, mainly for legal reasons, but also for other purposes. Different categories of data will be retained for different periods of time.

Conclusion

Compliance with the 2018 Act is the responsibility of all members of the Trust.

Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

This policy was formally agreed and adopted by the Board of Trustees of CVH and will be reviewed within 2 years by the board of trustees.

Approved at board meeting of 25th January 2021

Reviewed at the Board meeting 17th March 2023 & 11th July 2025

Approved 11th July 2025

