



Registered Charity No. 276859

Haslemere Methodist Church
Lion Green
Haslemere
Surrey
GU27 1LD

Telephone: 01428 652505

<https://www.careinhaslemere.org.uk>

Data Protection Policy

1 Scope

This policy applies to committee members, and volunteers, where services are provided *directly* by the charity known as Care in Haslemere.

2 Overview and Definitions

Wherever Care in Haslemere collects or uses personal or sensitive personal data, we act in accordance with the General Data Protection Regulations, EU Regulation 2016/679 (GDPR)

The GDPR requires that personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the

public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

- 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.”

Definitions:

Personal Data is defined as information from which you can identify a person, for example name, address, phone number, email address or photograph of the person.

Sensitive Personal Data is defined as information concerning a person’s racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offences.

The person whose data is collected is called the “Data Subject”

3 Responsibilities

Care in Haslemere is not required by law to appoint a Data Protection Officer.

The Trustees are responsible for ensuring overall compliance with GDPR through establishing and monitoring this policy. Volunteers handling information are to be made aware of their responsibilities regarding the holding and movement of personal data on behalf of Care in Haslemere.

4 Lawful Basis for Collecting Information

The GDPR provides six valid lawful bases on which personal data can be processed:

- a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- d) **Vital interests:** the processing is necessary to protect someone’s life.

- e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

In practice, most personal data collected and processed by Care in Haslemere is covered by "Legitimate Interest", because

- a) people would reasonably expect us to collect their data, for example so that we can provide them with a service such as hospital transport , and/or
- b) we are required to collect the information in order to meet reporting obligations to prepare accounts, provide details of our impact and to claim gift aid.

On occasion, we will need to seek **Consent** for the collection of personal information and/or use in different ways which would not be covered by Legitimate Interest. For example, for marketing and promotional communications, or use of photographs for publicity purposes.

5 Data Audit

We will identify, for all areas of our work:

- What personal data we collect
- The lawful basis in the GDPR under which we are entitled to collect this information
- Where and how the information is stored
- How long the information is retained for
- Who it is shared with
- Any risks and risk mitigation factors

We will carry out a Privacy Impact Assessment for any new project which will require the processing of personal data, using the same headings as above, to plan data protection measures from the outset.

6 Collecting Personal Data, and Privacy Notices

As a general principle, we will seek to collect the minimum personal data required to carry out our work and to fulfil any contractual requirements (e.g., reporting to our funders).

Whenever we collect personal data, we will inform (orally or in writing, including on forms collecting data) Data Subjects of the availability of our Privacy Notice, which explains:

- who we are;
- under what lawful basis we are collecting their information
- what we are going to do with their information; and
- who their information will be shared with (if anyone).

We will make our Privacy Notice readily accessible to all data subjects through various convenient methods, including:

- Available on our website
- Sent via email on request.
- Being read aloud upon request.
- Sent via postal mail on request.

7 Consent

Where Consent is required, we will normally get confirmation in writing. The consent form will include details of how to withdraw consent.

We will keep clear records of who has given Consent. We will act promptly on any requests to withdraw consent.

Any mail-outs or marketing communications will include clear information about who to contact if someone wishes to withdraw their consent to be contacted.

8 Storage and Retention of Personal Data

Whether in hard copy or electronically, we will take steps to ensure that Personal Data is stored securely:

- Hard Copies will be stored in locked cupboards or cabinets at the office or at the homes of committee members.
- Electronic information will be stored in password protected or encrypted files
- Information recorded on the devices (PC, tablet or mobile phone) of volunteers will be protected by a device password
- For data stored with third parties – for example data stored on cloud services, or within the VIA web app, we will ensure that the service provider meets stringent data protection standards, including appropriate security measures and data processing agreements, and that access by committee members and volunteers is restricted to authorised personnel only via secure, authenticated logins.

We will not keep data for longer than necessary. This will be identified as part of the Data Audit.

We are aware of the need to dispose of personal data securely. Hard copies will be shredded. We will take reasonable precautions to ensure Personal Data is removed from Care in Haslemere IT equipment prior to disposal.

9 Sharing Information with Others

Care in Haslemere works closely with partner organisations. These include organisations directly relating to Data Subjects (for example hospitals or a Care Home), and also organisations providing us with software to support our transport and other services, and organisations which host data on our behalf ("cloud service providers"). This will sometimes require us to share Personal and Sensitive Personal Data about our clients to ensure that they get the service they require.

We will normally **only** share Personal Data with others where we have a lawful basis to do so, and where this has been explained to the Data Subject in the Privacy Notice.

On rare occasions, where we have legitimate safeguarding concerns, we may share Personal Data with other organisations without prior notice. For further information see Care in Haslemere's Safeguarding Policy.

Where necessary, we will put in place Data Sharing Agreements with key partners and contractors. These Agreements will clearly define the role and responsibilities of both parties in relation to the Personal Data, in particular which Organisation has the role of Data Controller, and which is the Data Processor. In practice our partners' standard wording is likely to be adopted.

We will take proportionate steps to ensure that Data is shared *securely*, for example using encrypted emails.

10 Subject Access Requests

Under GDPR, individuals have the right to obtain confirmation that their data is being processed; access to their personal data; and information about how and why we are using their personal data (i.e., the information provided in the Privacy Notice).

We will respond to all Subject Access Requests within one month, unless the request is complex or numerous in which case this may be extended to up to three months.

We will take reasonable steps to verify the identity of the person making the request.

11 Right to Erasure and Restriction

Individuals have the right to have their personal data erased if:

- (Where we are relying on consent as our lawful basis for holding the data) the individual withdraws their consent;
- (Where we are relying on legitimate interests as our lawful basis) the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;

If we have disclosed the personal data to others, we will contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort.

Individuals also have the right to request that their personal data be restricted or suppressed.

12 Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data

On becoming aware of a breach, we will take steps to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect the individuals whose personal data has been

compromised, for example by causing emotional distress or physical and material damage.

If a data breach is likely to cause a resulting risk to people's rights and freedoms, we will be required to notify the ICO within 72-hours. If not, we are not required to notify the ICO but should still take steps to document the breach any resulting actions.

Where we are processing data on behalf of another organisation, any breaches should be notified to them

If a breach is likely to result in a high risk to the rights and freedoms of individuals, we will be required to inform them as soon as possible.

13 Electronic Messaging (Emails, texts, WhatsApp etc)

The GDPR covers Personal Data stored and sent via email, by text or by WhatsApp and similar messaging services. Any emails containing Personal Data should be deleted and/or securely archived once they have been dealt with.

When communicating Personal Data via electronic messaging, committee members and volunteers should take reasonable and practical steps to ensure its security. The most secure methods should be prioritised, particularly for sensitive or extensive Personal Data.

14 Home Working and Working Out of the Office

The nature of Care in Haslemere work means that committee members and volunteers may choose to perform some data processing tasks including collecting personal data from home.

As a general rule, all Personal Data should usually be kept securely in the office. However Personal Data stored securely on the cloud may be accessed from home. The data may be stored on personal devices from home

In limited circumstances, volunteers will be permitted to take Personal Data out of the office, for the purpose of carrying out specific duties such as a visit to a prospective client to complete the Registration Form.

The Volunteers concerned should *only* carry the minimum information they require with them (i.e., just the form for that individual and not the whole registration file), and any personal information should be securely destroyed or returned to the Office at the earliest opportunity.

Personal Data should never be processed or sent from unsecured WiFi hotspots.

15 Use of Personal Devices

Care in Haslemere volunteers may use their own personal devices (e.g., mobile phone, home computer) to receive Personal Data on behalf of Care in Haslemere, ie, volunteers might be given contact details for a Service User. It is anticipated that many driver volunteers will keep information of drives on their mobile phone calendars.

Such personal devices are likely to store data on cloud services. It is not practical for Care in Haslemere to review all volunteers' data storage contracts, however volunteers are asked to be aware of the requirements of this policy and to consult with Care in Haslemere if they believe they are using a service which is not a widely recognised platform.

It is noted that any such Personal Data remains the property of Care in Haslemere and must NEVER be shared with others, including on personal social media, without express permission.

Personal Data on volunteers' personal devices should be deleted as soon as it is no longer required. Data collected on mobile phones should be deleted at latest within two months of the journey. Any information collected when out, e.g., photographs, should be transferred to Care in Haslemere own computer system as soon as reasonably practical and deleted from the personal device immediately.


When a staff member or volunteer leaves the organisation, we will take reasonable steps to ensure that any Personal Data belonging to Care in Haslemere has been removed from their personal devices.

Staff and volunteers using personal devices to store and access Personal Data on behalf of Care in Haslemere will be required to enable basic security features on their device, such as screen locking with password or PIN protection.

16 Monitoring and Review

We will review the policy periodically to consider changes in legislation or in Care in Haslemere activities. The policy will be reviewed as a matter of course every two years.

Signed on behalf of the Trustee Board:

 IVOR BARRETT

Date: 01 DEC 2025

Signed on behalf of the Trustee Board:

 GILLIAN EGERTON

Date: 01 DEC 2025

Further Information

Organisations storing personal data on computers must register under the Data Protection Act 1998. Any information relating to a living individual who can be identified by name, address or registration number in a volunteer database, must be registered under the Act.