

<b>Title of policy:</b>	Data Protection Policy
<b>Date of original issue:</b>	19 November 2014
<b>Version:</b>	2.2
<b>Date of this version:</b>	June 2024
<b>Author:</b>	Chris Stelling, Chief Executive Officer
<b>Owned by:</b>	Chief Executive Officer
<b>Approved by/date:</b>	Board of Trustees/Sept 2024
<b>Date of next review:</b>	June 2027 [3 years from approval]

This is a discretionary policy which does not form part of a contract of employment. The Board of Directors of Carers in Bedfordshire may vary or amend the policy as it deems necessary.

The term staff is used in this document as a generic statement to refer to any person working for Carers in Bedfordshire in any capacity and includes volunteers, part time staff, Board members, sessional/ temporary workers and work placement students working with younger children. This policy is applicable to all Carers in Bedfordshire staff.

## **Policy statement**

Carers in Bedfordshire aims to ensure that all personal data collected about Carers, Volunteers Employees and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Carers in Bedfordshire is a data controller. It is registered a data controller with the ICO and will renew this registration annually or as otherwise legally required.

A full description of how we use Personal Data can be found in our Privacy Notice.

Where Carers in Bedfordshire are carrying out work under contract, the requirements of the commissioning body in respect of Data Protection are taken into account and may modify this policy. Carers in Bedfordshire will, however, work with the commissioning body to agree a consistent approach wherever possible.

## **Responsibilities of all staff**

Staff, including volunteers and any contractors processing personal data on behalf of Carers in Bedfordshire are responsible for:

- Attending Data Protection training when invited
- Collecting, storing and processing any personal data in accordance with this policy
- Contacting the Data Protection Lead in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- They need to rely on or capture consent, update the privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties.

## **Managing Data Protection**

The Board of Trustees recognises its overall legal responsibility for Data Protection compliance.

Carers in Bedfordshire takes the view that we are not required to have a formal Data Protection Officer. Oversight of Data Protection is the responsibility of the Chief Executive, acting as our Data Protection Lead, assisted by the Digital Infrastructure and Data Security Lead.

The role of the Data Protection Lead is:

- Reporting to the Board of Trustees on Data Protection compliance
- Maintaining records that demonstrate how Carers in Bedfordshire complies with Data Protection
- Advising colleagues on Data Protection practice
- Ensuring that policies and procedures take Data Protection into account
- Ensuring that all relevant staff (including volunteers) receive Data Protection induction and regular training
- Reviewing contracts or contract amendments with Data Processors before they are entered into
- Handling all requests from Data Subjects to exercise their Data Protection rights
- Being the point of contact for the Information Commissioner.

All managers are responsible for Data Protection compliance within their teams and areas of responsibility, with advice and support from the Data Protection Lead.

Data Protection and Confidentiality are covered explicitly in the induction of all paid staff and volunteers. Refresher training for all staff is provided at appropriate intervals.

## **Sharing personal data**

We will not normally share personal data with anyone else, but may do so where:

- There is an issue that puts the safety of our staff, carers and volunteers at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff – for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our staff.

Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with data protection law.


When we are sharing data, we will only do so through a Carers in Bedfordshire approved provider.

We will share your data with the local authorities and clinical commissioning groups where we are contracted to do so. By sharing information, we are able to work more collaboratively for the betterment of services and ultimately to improve carers lives. This is done so by consent which is gained at the point of registration and can be withdrawn at any time.

## **Data Protection by design and by default**

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data should be kept under lock and key when not in use. Papers containing confidential personal data must not be left on office desks, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the relevant office. Staff must ensure information is stored securely whilst off site
- Carers in Bedfordshire computers, laptops and other electronic devices must be protected by strong passwords (passwords that are at least 8 characters in length including at least 1 number and a special character, or a 6-digit pin)
- Mobile devices such as memory sticks,  and other removable media must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. All

such devices must hold data only in encrypted format or must be encrypted by design. All such devices must be authorised and provided by (include name/job title)

- To keep information safe when using public Wi-Fi, staff should only login to networks that are password protected. Staff should check that websites contain 'https' (the 's' stands for secure) before logging into any accounts and log out when finished. File sharing should be disabled and Wi-Fi/Bluetooth turned off when not in use
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

## **Legal bases for processing**

Carers in Bedfordshire carries out all Processing of Personal Data under an appropriate Legal Basis, which is typically assessed as follows:

- Where the Processing is necessary for a contract that is normally the Legal Basis
- Where the Processing is necessary under a legal obligation that is normally the Legal Basis
- Where the Processing is necessary in the course of routine activities the Legal Basis is normally legitimate interests, provided Carers in Bedfordshire has carried out and documented an appropriate assessment (see Appendix One)
- Where it is appropriate to offer the Data Subject a genuine choice, or where no other basis applies, the Legal Basis is normally consent.

Carers in Bedfordshire does not carry out any public functions, and recognises that the vital interests Legal Basis is only to be used in the case of serious emergencies.

See also Direct Marketing below.

It is normally the responsibility of the team manager to assess the appropriate Legal Basis for the activities of their team and to carry out an assessment if required. Complex or potentially controversial cases may be referred to the Data Protection Lead or, exceptionally, to the Board.

## **Special categories of data**

Carers in Bedfordshire obtains and processes Special Category Data only where fully justified, including in the following situations:

- Where it is appropriate to carry out diversity monitoring, with the explicit consent of the Data Subjects
- Where the medical diagnosis or condition of an individual client is pertinent or essential for the delivery of the charity's routine activities
- For staff, volunteers or contractors, information about health, including any medical condition, health and sickness records.
- For staff, volunteers or contractors, Information about criminal convictions and offences
- In case of an accident taking place during our activities. Under this circumstance we may be required to share this data with statutory authorities.

## **Data Protection Principles**

Carers in Bedfordshire recognises the importance of complying with the six Data Protection Principles.

### ***Obtaining and processing data (first and second Principles)***

Whenever Carers in Bedfordshire obtains information from Data Subjects, verbally or in writing, we ensure that they understand the purpose(s) for which we will use it and we present clearly any options they have, either to prevent or restrict our use of their data, or to provide consent for specific activities. Carers in Bedfordshire also informs them of any intended disclosures or transfers of data to third parties. Data Subjects are always given a choice over ancillary activities such as whether or not they receive information from Carers in Bedfordshire and whether or not Carers in Bedfordshire may approach them for fundraising or other marketing purposes.

The statements used are, as far as possible, standardised so that the information and options are provided consistently.

It is left to the carer to decide whether or not to inform the person they care for about the carer's involvement with Carers in Bedfordshire and the fact that limited data about the person being cared for is therefore held.

Data on carers is held with their consent and is normally disclosed to third parties only with their consent. Consent is not sought from people cared for by clients of Carers in Bedfordshire, on the basis that the information held is limited and that the use can be justified as a Legitimate Interest.

### ***Data quality and retention (third, fourth and fifth Principles)***

Carers in Bedfordshire provides all staff and volunteers who maintain records on clients and other contacts with guidance and training so that they can produce consistently accurate, useful and appropriate records.

Our recording systems are designed and maintained to promote data quality, to meet the requirements of the Data Protection Principles (including the need to demonstrate whether and if so how consent has been obtained), and to remove duplication wherever possible.

We typically retain personal and financial information for seven years however there are circumstances where we need to retain information for longer periods.

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on our behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Calls may also be recorded for training purposes and these call recordings will be kept for a maximum of three months.

We operate and maintain a data retention schedule for all data

### ***Security (sixth Principle)***

Carers in Bedfordshire has a clear procedure that sets out how staff and volunteers are authorised to access which data and for which purpose(s).

Carers in Bedfordshire ensures that our computer systems and record handling systems incorporate appropriate security measures to prevent unauthorised access, and keeps these under review in the light of technical developments and evolving threats.

All staff and volunteers are required to abide by any security measures designed to protect personal data from loss, misuse or inappropriate disclosure.

### **Direct marketing**

Carers in Bedfordshire provides straightforward ways for Data Subjects to exercise their right not to receive direct marketing material, including fundraising appeals.

Direct marketing is generally undertaken on the legal basis of consent. However, materials closely related to our service delivery may be provided on the Legal Basis of legitimate interests, even if they contain marketing elements. Data Subjects are always given a clear opportunity to opt out of receiving such materials.

### **Data Subject rights**

All staff and volunteers are given guidance on how to respond when an individual asks to see information held about them or to exercise any of their other Data Protection rights.

All requests are forwarded to the Data Protection Lead, to ensure that our response is timely and complies with the relevant requirements.

### **Transfers abroad**

Carers in Bedfordshire does not intentionally transfer Personal Data outside the UK, either directly or in the context of employing a Data Processor.

### **Collaboration with joint Controllers**

Whenever Carers in Bedfordshire collaborates with other organisations, we establish at the outset whether we will be acting as joint Controllers of Personal Data. In that case we draw up a formal data sharing agreement, setting out the respective responsibilities of all parties involved in the collaboration.

### **Data Processors**

Whenever Carers in Bedfordshire engages an external contractor to act as a Processor on our behalf the Data Protection Lead reviews any contractual terms and conditions offered, in order to establish that they meet Data Protection requirements. Where they do not, or where no standard terms and conditions are offered, Carers in Bedfordshire does not proceed until a compliant contract is agreed.

### **Data breaches**

In the event of a Data Protection breach, possible breach or near miss, the Data Protection Lead, as a matter of priority, obtains all the necessary information and notifies the Information Commissioner – and any affected Data Subjects – if required.

Whether or not the breach is reported, the Data Protection Lead investigates fully, proposes any necessary mitigating action or changes to procedure, and makes a report to the Board.

### **Definitions**

Term	Definition
<b>Personal data</b>	Any information relating to an identified, or identifiable, individual. This may include the individual's: <ul style="list-style-type: none"><li>• Name</li></ul>

	<ul style="list-style-type: none"> <li>• Telephone number</li> <li>• Location data</li> <li>• Online identifier, such as a username</li> </ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
<b>Special category data</b>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> <li>• Racial or ethnic origin</li> <li>• Political opinions</li> <li>• Religious or philosophical beliefs</li> <li>• Trade union membership</li> <li>• Genetics</li> <li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li> <li>• Physical or mental health or condition</li> <li>• Sex life or sexual orientation</li> </ul>
<b>Processing</b>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
<b>Data subject</b>	The identified or identifiable individual whose personal data is being held or processed.
<b>Data controller</b>	The person or organisation who determines the purposes and means for processing personal data.
<b>Data processor</b>	Any person or organisation that processes data on behalf of the data controller but is not employed by them.
<b>Consent</b>	Clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the individual's agreement to their personal data being processed, such as by a written (including electronic) statement.
<b>Personal data breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
<b>UK Data Protection Legislation</b>	All applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation ((EU) 2016/679); the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.