# Data Protection and GDPR Policy

| | |
|---|---|
| Document Owner | Chair of Board of Trustees |
| Version | August 2023 |
| Approved | September 2023 |
| Review | August 2024 |

| DATE REVIEWED | SUMMARY OF AMENDMENTS / CHANGES |
|---|---|
| August 2023 | New policy to replace the previous policy |
| | |
| | |
| | |

## 1. ABOUT THIS POLICY

1.1 The Data Protection Act 2018 controls how personal information is used by organisations. The Data Protection Act 2018 is the United Kingdom's implementation of the UK General Data Protection Regulation. (UK GDPR)

1.2 Everyone responsible for using personal data has to follow strict rules called data protection principles. Carers' Support East Kent is registered with the Information Commissioners Office as the Data Controller under registration number Z2453970, and is also a 'data processor'.

1.3 This Policy exists to ensure that Carers' Support East Kent is fully compliant with all legal requirements in relations to all aspects of data management. This is in respect of personal data, as well as safeguarding the rights and freedoms of persons whose information Carers' Support East Kent collects pursuant to the Data Protection Act 2018, UK GDPR, and the Privacy and Electronic Communications Regulations (PECR).

## 2. POLICY SCOPE

2.1 This Policy applies to all staff, volunteers, trustees and contractors of Carers' Support East Kent.

## 3. RESPONSIBILITIES

3.1 Whilst it is understood that the Board of Trustees carry ultimate responsibility for ensuring that Carers' Support East Kent complies with this Policy, all Managers must ensure they are aware of their specific responsibility for operating within the boundaries of this policy. This includes ensuring that all staff understand the standards required of them and taking action if actions occur that do not comply with the requirements of this policy.

3.2 The named individual responsible for the operation of this Policy is the responsible individual (the CEO) and is advised by the Data Protection Officer (DPO) accordingly.

3.3 Carers' Support East Kent uses a Customer Record Management System (CRMS). Overall management of the CRMS is the responsibility of the CEO with an expectation that all staff, volunteers, and Trustees understand their personal responsibility regarding its use.

## 4. COMMITMENT TO GOOD PRACTICE

4.1 Carers' Support East Kent is committed to ensuring high standards of practice are maintained in order to: -

- Enable the organisation to meet its personal data obligations about how personal information is managed.
- Support the aims and objectives of the organisation
- Set appropriate systems and controls according to Data Protection principles.
- Ensure compliance with all applicable data protection obligations, whether statutory, regulatory, contractual and/or professional.
- To safeguard personnel and stakeholder interests.
- To ensure the rights and freedoms of living individuals, and to protect their personal data by ensuring that it is never processed without their knowledge and, when possible, their consent

4.2 Carers' Support East Kent will seek to ensure compliance with data protection legislation and uphold good practice by: -

- Processing personal information only when it is absolutely necessary for organisational purposes.
- Ensuring that the least possible amount of personal data is collected, and that personal data is never processed unduly.
- Informing individuals of how their personal data is or will be used and by whom.
- Processing only pertinent and adequate personal data.
- Processing personal data in a lawful and fair manner.
- Keeping a record of the various categories of personal data processed.
- Ensuring that all personal data that is kept, is accurate and up to date.
- Retaining personal data no longer than required by statute or regulatory body, or for organisational purposes.
- Giving individuals the right to 'subject access', as well as all other individual rights pertaining to their personal data.
- Ensuring that all personal data is maintained securely.
- Identifying personnel that are responsible and accountable for UK GDPR Compliance.
- Pseudonymisation is used where possible.
- Processing is transparent allowing individuals to monitor what is being done with their data.

## 5. NOTIFICATION

5.1 Carers' Support East Kent has registered with the Information Commissioner as a 'data controller' – i.e., an organisation that engages in processing the personal information of data subjects.

5.2 All third parties working with or for Carers' Support East Kent who have or may have access to personal data are required to read, and fully comply with this policy at all times. All third parties are required to enter into a data confidentiality agreement before accessing any personal data. The data protection obligations imposed by the confidentiality agreement shall be equally onerous as those to which Carers' Support East Kent has agreed to comply with. Carers' Support East Kent shall at all times have the right to audit any personal data accessed by third parties pursuant to the confidentiality agreement.

## 6. ENSURING UK GDPR COMPLIANCE AND MANAGEMENT

6.1 Carers' Support East Kent is a Data Controller and Data Processor pursuant to the Data Protection Act 2018 / UK GDPR. As such, Carers' Support East Kent is responsible for ensuring overall compliance with the UK GDPR and for demonstrating that each of its processes is compliant with requirements. To this extent, the organisation is required to: -

- Maintain relevant documentation regarding its processes and operations.
- Implement proportionate security measures.
- Carry out Data Processing Impact Assessments.

6.2 Appointed staff of Carers' Support East Kent with managerial or supervisory responsibilities are responsible for ensuring that good personal data handling practices are developed, reviewed, and encouraged.

6.3 The position of responsible individual involves the management of personal data within the organisation as well as compliance with the requirements of the Data Protection Act 2018 / UK GDPR and demonstration of good practice protocols. The responsible individual is advised by the DPO and works closely with them.

## 7. PRINCIPLES OF DATA PROTECTION

7.1 All personal data must be processed lawfully, fairly and with transparency in mind at all times and in accordance with Carers' Support East Kent policies and procedures.

7.2 Policies and notices made available to data subjects and published in the public domain must also be clear, drafted using clear and plain language and written in such a way that everyone may understand the content and therefore intended purpose for processing. The data subject must be provided with the information in accordance with Article 13 and 14 of the UK GDPR.

7.3 Personal data may only be collected for specified, explicit and legitimate reasons. When personal data is obtained for specific purposes, it must only be used in relation to that purpose and cannot be different from the reasons formally notified to the Information Commissioner's Office (ICO) Registration. The Carers' Support East Kent makes this decision based on reasonableness and where suitable on the basis of an existing relationship.

7.4 Personal data must be adequate, relevant, and restricted to only what is required to processing.

7.5 Ensure that personal data which is superfluous and not necessarily required for the purpose(s) for which it is obtained, is not collected.

7.6 Approve all data collection forms, whether in hard copy or electronic format.

7.7 Carry out an annual review of all methods of data collection, checking that they are still appropriate, relevant, and not excessive.

7.8 Securely delete or destroy any personal data that it is no longer necessary to process in accordance with Carers' Support East Kent technical and organisational standards.

7.9 Personal data must be accurate and up to date; data should not be kept unless it is reasonable to assume its accuracy, and data that is kept for long periods of time must be examined and amended, if necessary.

7.10 All staff and volunteers must receive training on privacy and data protection at least on an annual basis. It is the responsibility of the responsible individual and the Data Protection Officer (DPO) to comply and undertake the training. Further training may be necessary for employees where there may have been identified risk (i.e., they made a data breach).

7.11 Individuals (data subjects) are personally responsible for ensuring that the personal data held by Carers' Support East Kent is accurate and up to date. Carers' Support East Kent will assume that information submitted by individuals (data subjects) via data collection forms is accurate at the date of submission.

7.12 All employees and volunteers of Carers' Support East Kent are required to update Carers' Support East Kent as soon as reasonably possible of any changes to personal information to ensure records are up to date at all times.

7.13 The data controller (Carers' Support East Kent) must ensure that relevant and suitable additional steps are taken to ensure that personal data is accurate and up to date.

7.14 The responsible individual shall, on an annual basis, carry out a review of all personal data controlled by Carers' Support East Kent and decide whether any data is no longer required to be held for the stated purposes and where required, arrange for that data to be deleted or destroyed in accordance with the requirements of the UK GDPR.

7.15 The responsible individual shall also ensure that where inaccurate or out-of-date personal data has been passed on to third parties, that the third parties are duly informed and instructed not to use the incorrect or out-of-date information as a means for making decisions about the data subject date information as a means for making decisions about the data subject involved. The responsible individual shall also provide an update to the third party, correcting any inaccuracies in the personal data.

## 8. RISK ASSESSMENT

8.1 Carers' Support East Kent will ensure that all risks associated with personal data processing are assessed and ensure that recorded risk assessment processes are in place.

8.2 Carers' Support East Kent is also required to carry out assessments of the personal data processing undertaken by other organisations on its behalf and to manage any identified risks, so as to mitigate the likelihood of potential non-compliance with this policy.

8.3 Where personal data processing is carried out by using new technologies, or when a high risk is identified in relation to the "rights and freedoms" of natural persons, a risk assessment of the potential impact must be undertaken. (Data Protection Impact Assessment – 'DPIA'.) More than one risk may be addressed in a single assessment.

8.4 If the outcome of a DPIA identifies a high risk that the intended personal data processing could result in distress and/or may cause damage to data subjects, the responsible individual will then decide whether Carers' Support East Kent ought to proceed i.e. the matter must be escalated to the responsible individual. In turn, this may be escalated the to the regulatory authority if significant concerns have been identified.

8.5 It is the role of the responsible individual to ensure appropriate controls are in place to ensure that the risk level associated with personal data processing is kept to an acceptable level, as per the requirements of the UK GDPR.

8.6 The organisation will ensure that security controls are in place to ensure that risks to personal data are appropriately mitigated as much as possible to reduce potential for damage or distress to those whose personal data is being processed. Such security measures will be subject to regular audit and review.

## 9. MANAGING PERSONAL DATA

9.1. Personal data only includes information relating to persons who can be identified or who are identifiable, directly from the information in question, or who can be indirectly identified from that information in combination with other information.

9.2 All personal data must be processed lawfully and fairly at all times, as per Carers' Support East Kent's Privacy Policy and Statement.

9.3 Policies must also be transparent, meaning that Carers' Support East Kent must ensure that its personal data processing policies, as well as any specific information provided to a data subject, are readily available, easily accessible and clearly understood.

9.4 The data subject- i.e. any living person who is the subject of personal data must be able to be provided with the following information:-

- The identity and contact details of the data controller and any of its representatives.
- The contact details of the Senior Responsible Individual.
- The purpose or purposes and legal basis of data processing.
- The length of time for which the data will be stored.
- The categories of personal data.
- The recipients and/or categories of any recipients of personal data, if applicable.
- Location of data if the data controller intends to make a transfer of personal data to a third party and the levels of data protection provided for by the laws of that country, if applicable.
- Any further information required by the data subject in order to ensure that the processing is fair and lawful.
- Confirmation of the rights to request access, rectification, erasure, and to raise of an objection to the processing of the personal data.

9.5 Personal data may only be collected for specified, explicit and legitimate reasons. When personal data is obtained for specific purposes, it must only be used in relation to that purpose.

9.6 Personal data must be adequate, relevant and restricted to only what is required for processing. The responsible individual shall be involved in monitoring, managing, and providing advice to:-

- Ensure that any personal data that is superfluous and not required for the purpose(s) for which it is obtained is not collected.
- Approve all data collection forms, whether in hard-copy or electronic format.
- Carry out an annual review of all methods of data collection, checking that they are still appropriate, relevant and not excessive.

- Securely delete or destroy any personal data that is collected in a manner that is excessive or unnecessary according to Data Protection / UK GDPR related Policies.

9.7 Personal data must be accurate and up-to-date. All staff must receive training to ensure they fully understand the importance of collecting and maintaining accurate personal data, understanding that individuals are personally responsible for ensuring that personal data held is accurate and up-to-date.

9.8 Data should not be kept unless it is reasonable to assume its accuracy and data that is kept for long periods of time must be examined and amended, if necessary.

9.9 The responsible individual must ensure that where inaccurate or out-of-date personal data has been passed on to third parties, that the third parties are duly informed and instructed not to use the incorrect or out-of-date information as a means for making decisions about the data subject involved. Carers' Support East Kent shall also provide an update to the third party, correcting any inaccuracies in the personal data.

9.10 The form in which the personal data is stored must be such that the data subject can only be identified when it is necessary to do so for processing purposes.

9.11 Personal data that is kept beyond the processing date must be either encrypted or anonymised and kept to an absolute minimum, to ensure the protection of the data subject's identity should a data breach incident occur.

9.12 Personal data must be retained according to the Data and Document Retention Policy and must be destroyed or deleted in a secure manner as soon as the retention date has passed. This includes items such as data disks, removable flash drives and hard drives.

9.13 Should any personal data be required to be retained beyond the retention period set out in the Data and Document Retention Policy, this may only be done after seeking advice from the of the responsible individual which must be in line with data protection requirements.

9.14 The processing of personal data must always be carried out in a secure manner.

9.15 Personal data must not be processed in an unauthorised or unlawful manner, nor should it be accidentally lost or destroyed at any time. Robust technical and organisational measures must be in place to ensure the safeguarding of personal data.

## 10. ENSURING THE RIGHTS OF DATA SUBJECTS ARE UPHELD

10.1 Data subjects - i.e. a living person who is the subject of personal data – have the following legal rights in relation to personal data that is processed and recorded: -

- The right to make access requests in respect of personal data that is held and disclosed.
- The right to refuse personal data processing, when to do so is likely to result in damage or distress.
- The right to refuse personal data processing, when it is for direct marketing purposes.
- The right to be informed about the functioning of any decision-making processes that are automated which are likely to have a significant effect on the data subject.
- The right not to solely be subject to any automated decision making process.
- The right to claim damages should they suffer any loss or harm from a breach of the Data Protection and UK GDPR Policy.

10.2 Data subjects also have the right to take appropriate action in respect of the following:-

- The rectification, blocking and erasure of personal data, as well as the destruction of any inaccurate personal data.
- The right to request that the Information Commissioners Office carry out an assessment as to whether any of the provisions of the UK GDPR have been breached.
- The right to be provided with personal data in a format that is structured, commonly used and machine-readable.
- The right to request that his or her personal data is sent to another data controller.
- The right to refuse automated profiling without prior approval.

## 11. DATA ACCESS AND SUBJECT ACCESS REQUESTS

11.1 Data subjects have the right to access all personal data in relation to them held by Carers' Support East Kent, whether as manual records or electronic format. Data subjects therefore may at any time request to have sight of confidential personal data, as well as any personal data received by Carers' Support East Kent from third parties. To do so, a data subject must submit a Subject Access Request.

11.2 All individuals who are the subject of any personal data that is held by us are entitled to: -

- Ask what information we hold about them and why.
- Ask how to gain access to it.
- Be informed how we keep it up to date.

- Be informed how we are meeting our data protection obligations.

11.3 If an individual contacts us requesting the information detailed above, this is called a 'Subject Access Request'. Subject Access Requests from individuals should be made by email or in writing to the responsible individual.

11.4 In most cases Carers' Support East Kent will not charge a fee to comply with a subject access request. However, as noted above, where the request is manifestly unfounded or excessive, we may charge a "reasonable fee" for the administrative costs of complying with the request. Carers' Support East Kent may also charge a reasonable fee if an individual requests further copies of their data following a request. This fee would be based on the administrative costs of providing further copies.

11.5 The responsible individual will aim to provide the relevant data within 14 days.

11.6 The responsible individual will always verify the identity of anyone making a Subject Access Request before handing over any information.

11.7 A Subject Access Request Form is provided for the data subject to complete in order to access their data, although they have no obligation to fulfil the request form it is provided in order to help us fulfil the subject access request to the best of our abilities and direct us in identifying a 'scope' of what they may be looking for in particular.

## 12. CONSENT

12.1 Consent to the processing of personal data by the data subject must be: -

- Freely given and should never be given under duress when the data subject is in an unfit state of mind or provided on the basis of misleading or false information.
- Explicit.
- Specific.
- A clear and unambiguous indication of the wishes of the data subject.
- Informed.
- Provided either in a statement or by unambiguous affirmative action.
- Demonstrated by active communication between the data controller and the data subject and must never be inferred or implied by omission or a lack of response to communication.
- Consent should be considered not to be forever, and only the time being.

12.2 The consent checklist (Appendix 1) sets out how to ask for, record and manage consent, including consent in relation to sensitive data.

12.3 Consent is a positive action on behalf of the data subject having read a clear, transparent and unambiguous “Privacy Notice (General)”. It does not necessarily have to be a box that is ticked, it could be the completion of a form, or the supply of contact information.

12.4 When promoting the aims and objectives of our organisation we reserve the right to use data wherever we believe a data subject has indicated their wishes and where we have collected the data for that particular purpose. We only use data for the purpose for which it was collected.

12.5 When the data subject is an employee Carers’ Support East Kent will usually obtain consent to process personal and sensitive data when a new employee signs an employment contract or during induction programs. Data subjects have the right to withdraw consent for non-operational functions at any time.

12.6 The Privacy and Electronic Communications Regulations (PECR) is also covered by this section of this Policy in relation to understanding consent.

## 13. COMPLAINTS

13.1 All complaints made with regard to Carers’ Support East Kent’s processing of personal data may be lodged by a data subject directly with the responsible individual by emailing them directly, or in writing, providing details of the complaint. The data subject must be provided with the Privacy Notice General at this stage.

13.2 All complaints in relation to how a complaint has been handled and any appeals following the submission of a complaint shall be dealt with by the responsible individual and in accordance with the Data Protection and UK GDPR Complaints Policy.

## 14. DATA SECURITY

14.1 All staff, volunteers and trustees of Carers’ Support East Kent are personally responsible for keeping secure any personal data held by Carers’ Support East Kent for which they are responsible. Under no circumstances may any personal data be disclosed to any third party unless Carers’ Support East Kent has provided express authorisation and has entered into a data processing agreement with the third party.

14.2 Access to personal data shall only be granted to those who need it and only according to the principles of Carers’ Support East Kent’s Security Access Policy.

14.3 All personal data must be stored: -

- In a locked room, the access to which is controlled; and/or
- In a locked cabinet, drawer, locked briefcase or locker; and/or

- If in electronic format and stored on a computer, encrypted according to the corporate requirements set out in the Security Access Policy; and/or
- If in electronic format and stored on removable media, encrypted as per Security Access Policy.

14.4 Before being granted access to any organisational data, all staff, volunteers, and trustees must be made aware of the Security Access Policy and a deadline set by which to read this.

14.5 Computer screens and terminals must not be visible to anyone other than staff, volunteers, trustees and contractors of Carers' Support East Kent with the requisite authorisation.

14.6 Manual records may only be accessed by authorised persons working for or on behalf of Carers' Support East Kent. Such records may only be removed from the business premises for the explicit purpose of providing the support services. Manual records must be securely handled out of the line of sight of the public. Manual records should be archived when access is no longer needed on a day-to-day basis.

14.7 All deletion of personal data must be carried out in accordance with the Data and Document Retention Policy. Manual records which have passed their retention date must be shredded and disposed of as 'confidential waste' and any removable or portable computer media such as hard drives and USB sticks must be destroyed.

14.8 Personal data that is processed 'off-site' must be processed by authorised staff, volunteers, trustees and contractors of Carers' Support East Kent, due to the increased risk of its loss, damage or theft.

## 15. DISCLOSURE OF DATA

15.1 Carers' Support East Kent will take appropriate steps to ensure that no personal data is disclosed to unauthorised third parties. This includes friends and family members of the data subject, governmental bodies and, in special circumstances, even the Police. All staff are required to complete Data Protection / UK GDPR training in order to learn how to exercise due caution when requested to disclose personal data to a third party.

15.2 Disclosure may be permitted by the Data Protection Act 2018 / UK GDPR without the consent of the data subject under certain circumstances, namely in the interests of:

- Safeguarding and National Security
- Crime prevention and detection which includes the apprehension and prosecution of offenders.
- Assessing or collecting a tax duty
- Discharging various regulatory functions, including health and safety

- Preventing serious harm occurring to a third party
- Protecting the vital interests of the data subject i.e., only in a life and death situation.

15.3 The responsible individual is responsible for advising on all requests for the disclosure of data for these reasons above, and authorisation by the responsible individual shall only be granted with the support of appropriate documentation and verification.

## 16. DATA RETENTION AND DISPOSAL

16.1 Carers' Support East Kent will not retain personal data for longer than is necessary and once an employee has left the organisation it may no longer be necessary to retain all the personal data held in relation to that individual.

16.2 Some data will be kept for longer than other data, in line with data retention and disposal procedures in the Data and Document Retention Policy.

16.3 Personal data must be disposed of securely to ensure that the data subject's information is protected at all times.

## 17. POLICY ENFORCEMENT

17.1 Carers' Support East Kent's IT and internet resources — including computers, smart phones, and internet connections — are provided for legitimate business use. We reserve the right to monitor how social networks are used and accessed through these resources. Any such examinations or monitoring will only be carried out by authorised persons.

17.2 All data relating to social networks written, sent or received through Carers' Support East Kent's computer systems are part of official records. Carers' Support East Kent can be legally compelled to share that information to law enforcement agencies or other parties.

17.3 Breaches of this Policy will be managed through the Disciplinary Procedure. If there is a possibility that the breach could amount to a criminal offence, the matter shall be referred to the relevant authorities.

## 18. AWARENESS OF THIS POLICY

Awareness in relation to this policy is incorporated in the Induction Program for all staff, trustees and volunteers.

**APPENDIX 1**

## ICO Consent Checklist

### Asking for consent

□ We have checked that consent is the most appropriate lawful basis for processing.
□ We have made the request for consent prominent and separate from our terms and conditions.
□ We ask people to positively opt in.
□ We don't use pre-ticked boxes or any other type of default consent.
□ We use clear, plain language that is easy to understand.
□ We specify why we want the data and what we're going to do with it.
□ We give separate distinct ('granular') options to consent separately to different purposes and types of processing.
□ We name our organisation and any third-party controllers who will be relying on the consent.
□ We tell individuals they can withdraw their consent.
□ We ensure that individuals can refuse to consent without detriment.
□ We avoid making consent a precondition of a service.
□ If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

### Recording consent

□ We keep a record of when and how we got consent from the individual.
□ We keep a record of exactly what they were told at the time.

### Managing consent

□ We regularly review consents to check that the relationship, the processing, and the purposes have not changed.
□ We have processes in place to refresh consent at appropriate intervals, including any parental consents.
□ We consider using privacy dashboards or other preference-management tools as a matter of good practice.
□ We make it easy for individuals to withdraw their consent at any time and publicise how to do so.
□ We act on withdrawals of consent as soon as we can.
□ We don't penalise individuals who wish to withdraw consent.