Data Management Policy

This policy was agreed by trustees on: 1.09.2021

It will be reviewed annually and updated as necessary.
The next review is due by:
1.09.2023

Community Action for Refugees and Asylum Seekers
25 Blakenham Road
London
SW17 8NE

0208 767 5378
www.caras.org.uk
charity number: 1124376
company number: 6462487

CARAS Data Management Policy

Introduction

The organisation has access to sensitive and personal data about staff, volunteers and beneficiaries all of which must be treated with respect and held in accordance with Data Protection Act 2018 and UK GDPR.

In line with the key principles of the act, all data will be:

- Fairly, lawfully and transparently processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Secure and only accessible to relevant people within the organisation
- Available to be accessed by the subject
- Not transferred to a country outside of the UK, unless the receiving country has equivalent levels of protection for personal data.

CARAS data management responsibilities

The CARAS Trustee Board, CARAS staff and any others who have access to personal information on behalf of CARAS must comply with the principles of the Act and UK GDPR.

The CARAS Trustee Board has overall responsibility for making sure that CARAS meets the terms of the Data Protection Act and UK GDPR.

CARAS management is responsible for ensuring staff are trained and up to date.

CARAS staff have a responsibility to make sure that they, and all volunteers contributing to their project, have a full understanding of the CARAS data protection policy and process information in line with the terms of the Act and UK GDPR.

Heads of Service have responsibility for overseeing that volunteers with access to sensitive information comply with the Data Protection Act. The Volunteer Development Lead has responsibility for ensuring that data relating to volunteers also complies with the Act and UK GDPR

All project staff have responsibility for overseeing that information relating to beneficiaries complies with the Data Protection Act and UK GDPR.

CARAS general practices

CARAS does not work with any vulnerable adults (as defined by law). For people under 18, consent must be obtained from a parent or legal guardian. During face-to-face activities we allow over 16s to drop-in and join us and subsequently conduct a formal intake with guardians.

A privacy policy containing relevant details of this Data Management Policy is available to all on our website.

Explicit consent, as referred to in this policy, for the processing of group member and volunteer personal data is obtained through intake forms on which the rights of the subject are highlighted. Photographic consent for publicity is obtained via a form for each event at which photography takes place. Consent to receive the CARAS newsletter and bulletin is obtained either through a signup form on the website, an opt-in box when making a donation, or an opt-in box in the volunteer agreement.

Adhering to the Data Protection Act or UK GDPR

Failure to adhere to the Act or UK GDPR is unlawful and can result in action being taken against CARAS. The ICO has the right to impose fines of up to £500,000 for serious breaches.

Principle 1 - Data must be fairly, lawfully and transparently processed

Staff and volunteers must:

- have legitimate grounds for collecting and using any personal data, or explicit consent from the person involved
- not use the data in ways that have unjustified adverse effects on the individuals concerned
- be transparent about how they intend to use the data. Consent for handling personal details will be sought explicitly at the time of collection from both volunteers and beneficiaries
- handle people's personal data only in ways they would reasonably expect
- not buy or sell any data
- Not do anything unlawful with the data

- If the lawful basis for processing data is other than 'legitimate interest' or explicit consent, that basis must be noted along with the data. Further details are in the staff handbook.

Principle 2 - Data must be processed for limited purposes

Staff and volunteers must:

- be clear from the outset about why they are collecting personal data and what they intend to do with it
- comply with fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data

Principle 3 - Data collected should be adequate, relevant and not excessive

Staff and volunteers must ensure:

- they hold personal data about an individual that is sufficient for the purpose it is held for in relation to that individual; and
- they do not hold more information than is needed for that purpose.

The minimum amount of personal data needed to properly fulfil the purpose should be identified. This much information should be held, but no more. This is part of the practice known as "data minimisation".

Principle 4 - Data should be accurate and up-to-date

Staff must:

- take reasonable steps to ensure the accuracy of any personal data obtained
- ensure that the source of any personal data shared by a third party brought to the attention of the person concerned
- carefully consider any challenges to the accuracy of information
- regularly review the accuracy of information stored in the electronic database

- update personal details on the database as soon as they are made aware of any changes

Principle 5 - Data should not be keep for longer than necessary

- there will be a twice annual review of the 'active' beneficiary and volunteer data; this will occur in June and December each year to ensure that active clients' cases should not be closed
- All personal information on ex-volunteers will be archived immediately they inform CARAS that they are leaving. It will be permanently deleted after 3 years since separation from CARAS.
- Once a beneficiary file is closed, the data will be kept for 5 years and then securely destroyed. This is to ensure that CARAS has information that could be useful if the case reopens and for reporting purposes
- Where data is stored in additional locations for one-off purposes such as events or trips this will be deleted immediately after the date of the event has passed
- If it is required that volunteers have access to beneficiary information, e.g. for help in calling beneficiaries prior to or during an event, the staff member coordinating is responsible for ensuring this information is not retained by the volunteer

Principle 6 - Data should be stored securely and only accessible to relevant people within the organisation

Electronic data

- Electronic records containing personal data relating to beneficiaries should be stored on the Lamplight database only
- Electronic records containing personal data relating to volunteers should be stored on Lamplight only
- Volunteers will only have access to Lamplight during activities from CARAS devices
- Staff, volunteer and beneficiary data will be accessed only when necessary for service provision
- Personal passwords for Lamplight will be kept secret by the individual and changed regularly
- Accounts must be properly logged out of after each use

- Emails containing personal and sensitive data will refer to a beneficiary using their initials only. An email with personal info would only ever be shared with a social worker or solicitor, only with the person's permission except where there is a safeguarding concern.
- Electronic files will be stored on encrypted hardware
- All electronic devices will be given full virus and privacy protection, which is to be updated on a regular basis

Physical Records

- No paper documents containing personal or sensitive data relating to staff, volunteers and clients are retained by CARAS. Beneficiaries are responsible for their own documents and these will not be stored in the office. Where copies are necessary, these will be scanned and stored in Lamplight, with originals returned to the beneficiary
-
- An up-to-date record of who has access to the database must be kept by the system administrators CARAS operates a clear desk policy. No documents relating to beneficiaries or volunteers should be left on desks overnight
- CARAS staff have their own password protected user accounts. No documents relating to beneficiaries or volunteers should be left on shared accounts.
- All physical documents containing personal or sensitive data will be securely disposed of
- Other
- No personal or sensitive information will be given out without previously confirming the identity of the person being spoken to. Information will only be passed to third parties with given consent from the data subject
-

Principle 7 - Data must be available to be accessed by the subject

- Anyone has the right to access personal information CARAS holds about them, whether in electronic or paper form. Staff, beneficiaries, volunteers and any other data subject will be made aware of this when data is collected
- requests to view personal information can be written or verbal

- CARAS must respond to requests to view personal information within 10 working days
- A person may correct the information held about them if erroneous, ask for it to be deleted or limit its use.

Principle 8 - Personal information must not be transferred to other countries without adequate protection

- If it is necessary to transfer data outside of the UK, CARAS will follow the ICO guidelines
- Before transferring data CARAS will carefully consider the necessity of it to achieving their aims
- When transferring data provisions relating to the other 7 principles will be enforced.

Subject Access Requests

When a subject access request is made to CARAS we aim to provide all data within 28 days. A search will be conducted to find all the subject's data held in Lamplight, in email accounts, in computer or cloud storage, and on paper. If we anticipate this taking longer than 28 days we will respond to the request with an explanation of why it is particularly difficult to retrieve and extend the deadline for the request by a further 28 days. When all a subject's data is disclosed to them we will ensure no other sensitive data is included with it. The data will be provided via encrypted digital file transfer.

Data Breaches

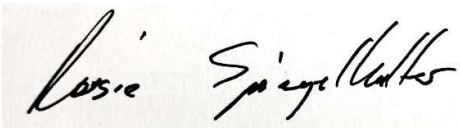
In order to lower the risk of data breach CARAS will check and update storage and security systems regularly. Staff and volunteers should report a breach immediately, however minor the risk. CARAS will act quickly to understand the nature of the breach, inform affected persons and learn how to avoid a repeat of the breach. Developments to this policy and to staff training should follow.

- CARAS will inform affected persons within 14 days by email or letter. If the rules require the breach to be reported to the ICO then this will be performed within 72 hours (0303 123 1113).

Review

This policy will be reviewed annually, or if the law changes.

This policy is agreed by the board of Trustees, and signed on behalf of them by:



Chair or Trustees

1.09.2021
Date