CARE International UK
Data Protection Policy

Information Commissioner Officer's Data Protection Registration No. Z6664020 (CARE International UK) and No. Z8127893 (CI Enterprises)

Data Controller: CARE International UK

89 Albert Embankment
London, SE1 7TP
020 7091 6000

1. Aims of this policy

CARE International UK (CIUK) is committed to protecting personal data. For CIUK, personal data can be related to relationships we hold with supporters and donors, as well as data on job candidates, employees or beneficiaries of CARE International's poverty-fighting work. CIUK needs to keep certain information to carry out our day-to-day work – enabling our mission by fundraising, through campaign actions, monitoring our programme impact and by providing evaluation reports to funders and supporters.

The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 1998. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

CIUK does not sell or exchange personal data with other organisations for marketing purposes.

2. Definitions

In line with the Data Protection Act Principles (1998) CIUK will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary

- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not to be transferred outside the European Economic Area (EEA)

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper-based personal data as well as that kept electronically.

The Personal Data Guardianship Code outlines five key principles of good data governance on which best practice is based. CIUK will seek to abide by this code in relation to all the personal data it processes, i.e.

- **Accountability:** Those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who have used this data.
- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

Definitions of roles:

- **Data Controller**: an organisation or person that determines the purposes for which, and the manner in which, any personal data are, or are to be, processed.
- **Data Protection Officer:** an individual within the organisation responsible for ensuring compliance with this policy (and the Data Protection Act 1998), who is the point of contact for information requests, as well as reporting any breaches to the Information Commissioner's Office (ICO).

3. Types of information processed

CIUK processes the following personal information:

3.1 Candidates and employees

- Information on applicants for posts, including references, is kept for six months.
- Employee payroll and performance information – contact details, bank account number, payroll information, supervision and appraisal notes are all kept for the duration of employment and six years thereafter.

- Ethnic origin is held electronically and this information is not shared outside of the Human Resources team.
- Employee contact details including email, telephone and family details (eg next of kin) are all kept for the duration of employment and six years thereafter.
- Users – contact details (in many voluntary organisations, detailed case notes may be held).

NB: Personal sensitive data such as ethnic origin, political opinions, religious beliefs, membership of a trade union, physical or mental health, criminal convictions are not held.

3.2 Supporters, donors, trustees, enquirers and complainants

- Personal data including address, email address and telephone number(s).
- Bank account details for direct debits (where applicable).
- For event participants, information including, but not limited to, medical information and emergency contacts.

Additional information, which is collected through our websites, is outlined in our privacy policies:

http://www.careinternational.org.uk/privacy-policy

https://www.lendwithcare.org/info/terms/privacy

3.3 How data is kept

Personal data is kept electronically and in paper form.

Groups of people within the organisation who will process personal information are employed staff and volunteers.

Externally we instruct suppliers to process data, keeping in-line with the data protection principle of data transfers. This enables the mailing of communications to individuals. In these instances CIUK remains responsible for this personal data in line with the Data Protection Act.

Data used externally for research purposes will be made anonymous. This can be academia or market research companies who are employed to analyse our performance and ensure we continue to learn and improve our programme and fundraising practices.

4 Notification

The needs we have for processing personal data are recorded on the public register maintained by the Information Commissioner. We notify and renew our notification on an annual basis as the law requires.

If there are any interim changes, these will be notified to the Information Commissioner within 28 days.

The name of the Data Protection Officer within our organisation as specified in our notification to the Information Commissioner is Leigh Wetherall.

5 Responsibilities

Under the Data Protection Guardianship Code, overall responsibility for personal data in a not-for-profit organisation resides with the governing body. In the case of CIUK, this is the Board of Trustees.

The governing body delegates tasks to the Data Protection Working Group at CIUK. The Group is responsible for:

- understanding and communicating obligations under the Act
- identifying potential problem areas or risks
- producing clear and effective procedures
- notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes.

All employed staff and volunteers who process personal information must ensure they not only understand, but also act in line with this policy and the Data Protection Principles.

6 Policy implementation

To meet our responsibilities employees, contractors, suppliers, volunteers and trustees will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised.

We will ensure that:

- Everyone managing and handling personal information is trained to do so;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures;
- Queries about handling personal information will be dealt with swiftly and politely and in line with the Information Commissioner's guidelines.

7 Training CIUK employees

At CIUK we have a data protection working group including representatives from IT, Finance, HR, Fundraising and Programmes & Policy. This group is chaired by a member of the Senior Management Team. The group is responsible for:

- internal policies
- training of staff
- awareness raising
- ensuring systems are robust
- identifying and mitigating risks
- carrying out internal audits
- reporting on any breaches.

Training and awareness-raising about the Data Protection Act and how it is followed at CIUK takes the following forms:

- On induction: each new employee, volunteer or board member will be introduced to this policy during their HR induction on the first day of employment/volunteering. In addition a presentation is made by the Data Protection Officer to all new staff at a quarterly induction.
- General awareness of data protection will be promoted internally through posters placed in key areas e.g. tea stations, meeting rooms, photocopy/print machines.
- All employees, volunteers and board members will sign a Data Protection Policy statement, declaring they understand their responsibility in protecting personal data.
- Refresher training will be provided by the Data Protection Working Group on an annual basis.

Any suppliers who handle personal data on our behalf will be checked for compliance with the Data Protection Act and contracts will include clauses related this. Suppliers are responsible for training their staff on data protection, although this policy will be shared with them.

8 Gathering and checking information

Before personal information is collected, we will consider the Data Protection Act principles to ensure we adhere to them.

We will take the following measures to ensure that personal information kept is accurate and safe:

- Using lockable cupboards with restricted access to keys.
- Setting up computer systems to allow restricted access to database systems.

- Not allowing personal data to be taken off site as hard copy, on laptop or on memory stick unless the portable device is password protected and encrypted. A portable device policy is available.
- Back-up of data on computers.
- Encrypted and password protected attachments for sensitive personal information sent by email. Preferably data transfers will be by secure FTP (file transfer protocol).
- Paper-based information is destroyed by a confidential waste supplier (www.shredit.co.uk)

If an employee makes an unauthorised disclosure of personal data to a third party this will result in disciplinary proceedings. The Board of Trustees are accountable for compliance of this policy. Any unauthorised disclosure made by a volunteer may result in the termination of the volunteering agreement. Any unauthorised disclosure by a supplier will break the terms of contract and legal proceedings will be instigated.

Personal sensitive information will not be used apart from the exact purpose for which permission was given.

9 Subject Access Requests

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to the CIUK Supporter Care team:

CARE International UK, 9th Floor, 89 Albert Embankment, London, SE11 7TP

supportercare@careinternational.org

The following information will be required before access is granted: full name and address.

We may also require proof of identity before access is granted. The following forms of ID will be required: copy of a passport, driving license or utilities bill.

Queries about handling personal information will be dealt with swiftly and politely.

We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 40 days required by the Act from receiving the written request.

10 Reviewing this policy

This policy will be reviewed annually to ensure it remains up to date and compliant with the law.

11 Declaration (for internal use only)

I confirm I have read and understood CIUK's Data Protection Policy and will act in accordance with it.

I am connected with this organisation in my capacity as a

- ☐ Employee
- ☐ Volunteer
- ☐ Trustee/committee member

Signature:

Print name:

Date:

Please return this form to Jacqueline Salvage, HR Officer, CARE International UK. Jacqueline is a member of CIUK's Data Protection Working Group.

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7 Consent

You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8 Children

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9 Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11 Data Protection Officers

You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

12 International

If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

ico.
Information Commissioner's Office

ico.org.uk