Centre for Community-Driven Research Internal Policy

Privacy

Introduction

The Centre for Community-Driven Research (CCDR) is committed to protecting the privacy of personal information which the organisation collects, holds and administers. Personal information is information which directly or indirectly identifies a person.

This policy follows the data protection principles under the General Data Protection Regulation including:

Lawfulness, fairness and transparency - CCDR must process personal data lawfully, fairly and in a transparent manner in relation to the data subject.

Purpose limitation - CCDR must only collect personal data for a specific, explicit and legitimate purpose. CCDR must clearly state what this purpose is, and only collect data for as long as necessary to complete that purpose.

Data minimisation - CCDR must ensure that personal data processed is adequate, relevant and limited to what is necessary in relation to the processing purpose.

Accuracy - CCDR must take every reasonable step to update or remove data that is inaccurate or incomplete. Individuals have the right to request that you erase or rectify erroneous data that relates to them, and CCDR must do so within a month.

Storage limitation - CCDR must delete personal data when you no longer need it. The timescales in most cases aren't set. They will depend on your business' circumstances and the reasons why we collect this data.

Integrity and confidentiality - CCDR must keep personal data safe and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Purpose

The purpose of this document is to provide a framework for CCDR in dealing with privacy considerations.

Policy

CCDR collects and administers a range of personal information for the purposes of research, evaluation and community engagement. The organisation is committed to protecting the privacy of personal information it collects, holds, is custodian for, and administers.

CCDR recognises the essential right of individuals to have their information administered in ways which they would reasonably expect – protected on one hand and made accessible to them on the other. These privacy values are reflected in and supported by our core values and philosophies.

CCDR is bound by laws which impose specific obligations when it comes to handling information. The organisation has adopted the following principles contained as minimum standards in relation to handling personal information.

CCDR will:

- Collect only information which the organisation requires for its primary function;
- Ensure that stakeholders are informed as to why we collect the information and how we administer the information gathered;
- Store personal information securely, protecting it from unauthorised access;
- Only provide access to personal information to staff that have the need for this information to perform their duties;
- Where information is in an identifiable or re-identifiable form, provide stakeholders with access to their own information, and the right to seek its correction;
- Not retain or have access to personal identifying information where there is not an operational, governance or compliance need to do so.

Collection

CCDR will:

- Only collect information that is necessary for the performance and primary function of CCDR.
- Notify stakeholders about why we collect the information and how it is administered.
- Notify stakeholders that this information is accessible to them.
- Not retain or have access to personal identifying information where there is not an operational, governance or compliance need to do so.

Use and Disclosure

CCDR will:

- Only use or disclose information for the primary purpose for which it was collected or a directly related secondary purpose.
- For other uses, CCDR will obtain consent from the affected person.

Data Quality

CCDR will:

- Take reasonable steps to ensure the information the organisation collects are accurate, complete, up to date, and relevant to the functions we perform.

Data Security and Retention

CCDR will:

- Safeguard the information we collect and store against misuse, loss, unauthorised access and modification.
- Personal information will be stored securely using the following measures:
    - In a secure office that has the ability to be locked
    - On a computer that is password protected with that password being changed every four months
    - In a database or equivalent system that is password protected with that password being changed every four months
- Only destroy records in accordance with the organisation's Records Management Policy.

Staff access to personal and confidential information

CCDR can:

- Only provide access to personal information to staff that have the need for this information to perform their duties

Openness

CCDR will:

- Ensure stakeholders are aware of CCDR's Privacy Policy and its purposes.
- Make this information freely available in relevant publications and on the organisation's website.

Access and Correction

CCDR will:

- Ensure individuals have a right to seek access to information held about them and to correct it if it is inaccurate, incomplete, misleading or not up to date. This is only applicable where the information held by CCDR is in a identifiable or re-identifiable form.

Anonymity

CCDR will:

- Give stakeholders the option of not identifying themselves when completing evaluation forms, research interviews, questionnaires or opinion surveys.

Making information available to other organisations

CCDR can:

- Only release personal information about a person with that person's express permission. For identifiable personal information to be released, the person concerned must sign a release form.
- Only release identifiable information to third parties where it is requested by the person concerned.

Policy Implementation and assignment of privacy officer(s)

CCDR will:

- Assign an Organisational Data Privacy Officer responsible for the implementation of this policy, for monitoring changes in Privacy legislation, and for advising on the need to review or revise this policy as and when the need arises.
- Assign a Local Data Privacy Officer for each CCDR office location. The role of the privacy officer will be to conduct privacy and confidentiality policy compliance checks and manage the printing and delivery of sensitive documents to local staff.
- Assign privacy levels to staff members for each project that they work on and only provide access to information to staff that have the need for this information to perform their duties.

Level	
Level I	Identifiable raw data associated with research and/or evaluation
Level II	De-identified raw data associated with research and/or evaluation
Level III	Identifiable personal information associated with stakeholder engagement and non-research or evaluation programs
Level IV	No access to identifiable personal information