Privacy policy

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.
Last review data	Q3 2024
Scheduled review date	Q3 2026
Lawfulness, fairness and transparency	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 and retain 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 we 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 it is no longer needed. **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 limitation(s)	Nil noted
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 a 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: o In a secure office that has the ability to be locked o On a computer that is password protected with that password being changed every four months o In a database or equivalent system that is password protected with that password being changed every four months
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 information about a person - whether de-identified or not - with that person's express permission. For 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 responsibility	CCDR will: • Assign an Organisational Data Privacy Officer (DPO) 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 (LPO) 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. It is the responsibility of the DSO and LPO to ensure that: • Passwords are changed on schedule of 4, 8 and 12 months • Staff and volunteers are provided with new passwords via Zoho Vault or as deemed appropriate by the DSA considering their level of access It is the responsibility of all employees and volunteers to ensure that: • Passwords are not stored in any Keychain applications • Passwords are never stored or shared electronically outside a vault • When a new password is provided, it is stored in Zoho Vault and not written down
Account and password protected data registry	The DSO will keep a password protected registry of all accounts, applications and password-protected data repositories used by the CCDR. Staff will be provided with this list according to their delegation that will be placed on the organisational intranet.
Communicating change of passwords	The DSO will inform staff via the intranet of the time and date that a password will be changed. The DSO will provide the LPO with new passwords via a vault. These will be provided to staff according to their delegation.
Password creation	All passwords at each level should: • Contain at least 8 alphanumeric characters • Contain both upper and lower case letters • Contain at least one number (for example, 0-9) • Contain at least one special character for example ! $ % ^ & * ?

	• Not include a name or date of birth or other easily identifiable information

Annex 1: Data classification levels

Level	Description	Examples
Level I	Information that can be made publicly available	Information that is available on CCDR website No identifiable information (including names, addresses and emails)
Level II	Information that is restricted to CCDR employees	Information that is not available on CCDR website No identifiable information (including names, addresses and emails)
Level III	Identifiable personal information	Information that may include individual names, addresses and emails however not email or contact lists
Level IV	De-identified personal information	Research and evaluation data that has been deidentified
Level V	Sensitive or commercial-in-confidence materials	Information restricted to Chief Executive and Deputy Chief Executive delegations Other access on a need-only basis Includes identifiable data For human resources, this level should not hold any financial information (salary level, bank details, pension fund etc).
Level VI	Sensitive materials (research)	Includes identifiable study data Access on a need-only basis, such as study interviews and transcripts before deidentification
Level VII	Financial and confidential human resources	Information restricted to Chief Executive
Level VIII	Data Security Officer (DSO)	Information restricted to Data Security Officer