Record management policy

Last review date	Quarter 3, 2024
Scheduled review date	Quarter 3, 2026
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. Record management is an important way of protecting people's privacy.
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 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 limitation(s)	CCDR must comply with local governance requirements. The organisation: • must keep certain written financial and operational records • can keep the records filed in the relevant electronic file • must keep the records for seven years • must keep records in the local language or English, or in a form that can be easily translated to English
Purpose	CCDR receives funding from charitable donations, grants and fee-for-service projects. As a registered charity it is an important part of our accountability and responsibility to maintain accurate records of our work. As an organisation that has staff working in various locations, it is also important to maintain reliable records which individuals can easily create and retrieve. Finally, record management is a very important part of managing compliance to ethics, privacy and regulations and should be taken seriously.
Policy	Records management is everyone's responsibility. Records are an important and unique source of evidence and information about CCDR's activities. They provide specific information about our business.

	Managing information and records effectively makes your job easier and helps your colleagues. If you regularly make records and keep them in the right places, it will be easier to: • locate emails, documents or information when needed • reuse valuable work that you or someone has done in the past • determine the most recent version of a document • produce evidence as to why a particular decision was made • protect yourself, our clients, and CCDR from litigation against privacy, ethics or regulatory claims Some general rules in maintain records and the privacy of records are: **ALL COMPUTERS MUST BE PASSWORD PROTECTED** **ALL COMPUTERS MUST BE LOCKED WHEN NOT IN USE** **STAFF MAY ONLY ACCESS FILES ON CCDR-ISSUED COMPUTERS** **SYNC MUST NOT BE ACCESSED ON ANY PERSONAL COMPUTER UNLESS PERMISSION IS GRANTED BY THE DSO** **PASSWORDS AT ANY LEVEL MUST NOT BE SHARED IN ANY CIRCUMSTANCE, INCLUDING BETWEEN STAFF MEMBERS.** **LAPTOPS MUST NOT BE USED IN PUBLIC SPACES OR ON WIFI NETWORKS OUTSIDE THE STAFF MEMBER'S HOME/FAMILY NETWORK** Levels of access will be provided dependent on a staff member's need to access the information to complete their work. It should be noted that while there are levels of data, all documents, data and information should as a general rule be treated as confidential. A detailed file structure is maintained on the organisations intranet.
Policy Implementation and assignment of responsibility	Records are an essential tool of good business and efficient administration. All work conducted while under contract with CCDR is considered work product. All information created, sent and received in the course of your job is potentially a record. Records provide evidence of CCDR's business. Whether something is a record depends on the information it contains and the context. Records can be in paper, digital or other formats. Not all information you're working on needs to be saved as a record. If you're not sure, ask yourself these questions • Did I write, send or use this in the course of my work and does that information need to be prepared in a document that can be saved and shared? • Am I (or is someone else) required to act on this? • Will this information be needed in the future?

	If you answered yes to any of these questions, you should make or keep a record and filed accordingly, keeping in mind the access levels of various files (Please refer to the organisation's intranet).
Protecting privacy	An important rule to remember is that: No lists of names and contact details should be kept outside the file 'LISTS AND REGISTERS' unless permission is granted by the DSO No lists should be created that contain any personal details. If a list is needed, you need to make a request to your supervisor to determine the appropriate place for storing and securing this information.
Naming and using files	Files should be saved using the following format: DOCUMENT NAME_ YYYYMMDD • Words should be separated by an underscore after the date • Document names should be in capital letters • There is no circumstance where anyone should create separate or duplicate versions of the one document • Close all documents when you are not working on them
Creating files outside the file structure	CCDR has a file structure so that, if audited for compliance with privacy and ethics policies, we will have confidence that all files have been stored in an appropriate place. Most folders will have a 'OTHER' folder. This and the 'AA_WORKING FILES' is where you can create files (but remember – no lists) while you are working on new projects or projects where no structured file is available. Once the project is set or complete, you will need determine what records need to be kept, what the level of security needed for long-term storage is, and then provide this information to the Data Security Officer (DSO) for approval. The name of the DSO is maintained on the organisation's intranet.
Clear desk policy	CCDR is in general, a paperless organisation. We need to work collaboratively online, so as a general rule, if you need to make notes rather than writing them down on a piece of paper, it is better to type them into a document and store these as needed in your personal working file on Sync. All employees must clear their desks at the end of each workday, and this is also good practice when working from home. This not only includes documents and notes, but any post-it notes, businesses cards, and removable media (e.g. USB memory sticks) and be reminded that these are all considered work product. Following a clean desk policy will help reduce the risk of information theft, fraud, or a security breach caused by sensitive information being left unattended and visible in plain view.