



CENTRE FOR DEVELOPMENT IN SOCIAL JUSTICE (CDSJ)

DATA PROTECTION, PRIVACY, AND CONFIDENTIALITY POLICY



CENTRE FOR DEVELOPMENT
— IN SOCIAL JUSTICE —
A People-Centered Development

1. Title

This instrument shall be known as the **CDSJ Data Protection, Privacy, and Confidentiality Policy**.

2. Effective Date

This Policy takes effect on the date of approval by the competent governance authority of CDSJ and remains in force until amended or repealed.

3. Purpose

This Policy sets the rules for how CDSJ collects, receives, records, stores, uses, shares, transfers, secures, retains, accesses, corrects, and disposes of personal information, confidential information, and other protected data in the course of its governance, employment, programmes, research, partnerships, safeguarding, complaints handling, communications, and administration.

This Policy is adopted because CDSJ handles highly sensitive information, including staff records, community data, safeguarding information, case-related information, research data, donor records, financial records, and partner information. If such information is mishandled, the organisation can expose individuals to stigma, retaliation, financial harm, identity misuse, safety risk, reputational harm, and loss of trust. This Policy is designed in a way that reflects the practical logic of modern personal data protection law, including the lawful processing approach found in South Africa's POPIA, which sets out conditions including accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation.

4. Application

This Policy applies to:

- a. all CDSJ employees, whether permanent, fixed-term, temporary, probationary, or part-time;
- b. all governance members;
- c. all consultants, interns, volunteers, associates, and other non-employee personnel who access or process CDSJ information;
- d. all CDSJ offices, branches, projects, and future country operations;
- e. all physical and electronic records containing personal information or confidential information; and
- f. all systems, devices, applications, platforms, shared drives, cloud services, email accounts, and other data environments used for CDSJ work.

This Policy applies whether the information is collected directly from the person, received from a partner, generated through operations, or obtained through a lawful third-party source.

5. Policy Statement

CDSJ shall process personal information and confidential information lawfully, fairly, securely, and only for legitimate organisational purposes.

CDSJ shall:

- a. collect only information it has a lawful and legitimate reason to process;
- b. process information for a defined and proper purpose;
- c. keep information accurate and reasonably up to date;
- d. protect information against loss, unauthorised access, destruction, misuse, or disclosure;
- e. respect the privacy and dignity of the people whose information it holds;

- f. respond appropriately to requests for access, correction, or lawful inquiry; and
- g. report and manage security compromises in a timely and accountable manner.

POPIA's conditions for lawful processing include accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation, and this Policy adopts that same practical structure as an internal governance standard.

6. Guiding Rules

All implementation of this Policy must follow these rules:

- a. information must be processed only where there is a clear and lawful basis;
- b. collection must be relevant and not excessive for the purpose;
- c. people should not be misled about why their information is being collected;
- d. especially sensitive information must receive heightened protection;
- e. access to information must be limited to those with a legitimate need-to-know role;
- f. security must be proportionate to the sensitivity of the information; and
- g. confidentiality is a continuing duty and does not end merely because a task is complete.

7. Definitions

For purposes of this Policy:

Personal Information means information relating to an identifiable, living natural person, and where applicable an identifiable juristic person, including contact details, identity details, employment details, financial details, health-related information, location-linked information, images, recordings, case information, or any other information that can identify or be linked to a person.

Special Personal Information means particularly sensitive personal information requiring heightened protection, including health information, biometric information, information relating to children, and any other especially protected category recognised by law or policy.

Confidential Information means information which CDSJ is obliged or expected to protect from unauthorised disclosure because of privacy, legal duty, professional sensitivity, organisational risk, safeguarding need, employment sensitivity, donor restriction, or legitimate institutional interest.

Processing means any operation involving information, including collection, receipt, recording, storage, use, updating, sharing, transfer, analysis, publication, retention, archiving, or destruction.

Data Subject means the person to whom the personal information relates.

Security Compromise means a breach or compromise affecting the confidentiality, integrity, or availability of personal information, including unauthorised access, disclosure, alteration, loss, or destruction. The South African Information Regulator has explained that security compromises include accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal information, and has stated that all such compromises must be reported, without a low-risk exception.

8. Categories of Information Covered

This Policy covers, among other things:

- a. employee and applicant records;
- b. payroll, banking, and remuneration records;
- c. grievance, disciplinary, safeguarding, child protection, and PSEAH records;
- d. health-related and wellness-related information;

- e. programme participant, beneficiary, and community contact information;
- f. case documentation, referral information, and support records;
- g. research and monitoring information;
- h. images, audio, video, and attendance records;
- i. donor, partner, supplier, and contractual records;
- j. governance and legal records; and
- k. usernames, credentials, access records, and system-generated information where linked to persons.

9. Lawful and Legitimate Processing Basis

CDSJ may process personal information only where there is a legitimate and lawful basis to do so.

Lawful bases may include:

- a. the information is necessary for employment administration;
- b. the information is necessary for contractual performance or pre-contract steps;
- c. the information is necessary for legal compliance;
- d. the information is necessary for a legitimate organisational purpose that does not override the rights and dignity of the data subject;
- e. the information is processed with valid consent where consent is the appropriate basis; or
- f. the information is necessary to protect safety, provide support, or respond to a legitimate safeguarding, welfare, or operational concern.

No employee or unit may collect personal information merely because it might be useful one day.

10. Accountability

CDSJ is responsible for ensuring that personal information processed by or for the organisation is handled in compliance with this Policy.

This means CDSJ must:

- a. assign responsibility for implementation;
- b. ensure that staff understand their obligations;
- c. maintain systems for secure handling;
- d. review information practices where risk is visible; and
- e. act when a breach, weakness, or misuse is identified.

This reflects the accountability condition recognised in POPIA.

11. Processing Limitation and Data Minimisation

CDSJ shall limit personal information processing to what is relevant, adequate, and not excessive for the purpose.

Accordingly:

- a. only information needed for the defined purpose should be collected;
- b. intrusive data collection must be avoided unless clearly justified;
- c. duplicate collection should be avoided where the information already exists lawfully in CDSJ systems; and
- d. managers and staff must not ask for sensitive information merely out of curiosity or convenience.

This reflects the processing limitation condition recognised in POPIA.

12. Purpose Specification

Before collecting personal information, CDSJ must be able to identify the purpose for which the information is needed.

The purpose must be:

- a. specific enough to explain why the information is needed;
- b. lawful and organisationally legitimate; and
- c. communicated appropriately to the person where required.

Information collected for one clear purpose may not automatically be used for a different and unrelated purpose. This reflects the purpose specification and further processing limitation approach recognised in POPIA.

13. Further Processing and Secondary Use

Where CDSJ wishes to use information for a new purpose beyond the original reason for collection, it must consider whether the new use is:

- a. compatible with the original purpose;
- b. permitted by law or policy;
- c. supported by a valid consent where needed; or
- d. otherwise justified by a legitimate and documented basis.

If the new use is materially different and not obviously compatible, the new processing must not proceed without proper legal or policy basis.

14. Information Quality and Accuracy

CDSJ shall take reasonable steps to ensure that personal information is accurate, complete where necessary, not misleading, and updated where the purpose requires current information.

This means:

- a. staff records must be updated when material details change;
- b. programme and case data should be reviewed for obvious inaccuracy;
- c. decisions should not be based on known inaccurate information; and
- d. where an inaccuracy is identified, it must be corrected, clarified, or flagged appropriately.

This reflects the information quality condition recognised in POPIA.

15. Openness and Transparency

Where CDSJ collects personal information directly from a person, it should, where appropriate, make clear:

- a. what information is being collected;
- b. why it is being collected;
- c. who is collecting it;
- d. whether provision is mandatory or voluntary where relevant;
- e. how it may be used or shared; and
- f. what rights or contact routes are available for questions or concerns.

This does not require an overly formal notice in every small interaction, but it does require honesty and clarity appropriate to the context. This reflects the openness condition recognised in POPIA.

16. Consent

Where consent is used as the lawful basis for processing, it must be:

- a. informed;
- b. voluntary;
- c. specific enough for the purpose; and
- d. capable of being evidenced where the context requires it.

Consent must not be relied on where the real basis is something else, such as employment necessity, legal duty, or safeguarding need. In employment settings especially, managers must be careful not to treat coerced agreement as valid consent.

17. Special Personal Information and Child Information

Special personal information and information relating to children require heightened protection.

CDSJ may process such information only where:

- a. there is a clear lawful and policy basis;
- b. the purpose is legitimate and necessary;
- c. access is tightly restricted;
- d. additional care is taken in storage, sharing, and retention; and
- e. any consent, authorisation, or protective control required by law or policy is in place.

POPIA prohibits processing of special personal information and children's personal information unless permitted circumstances apply.

18. Confidentiality Obligations

All personnel covered by this Policy must protect confidential information and may disclose it only where:

- a. disclosure is required for authorised work purposes;
- b. the recipient has a legitimate need to know;
- c. disclosure is required by law;
- d. disclosure is necessary for safeguarding, safety, or emergency response; or
- e. valid consent or authorisation allows it.

Confidentiality applies to verbal discussions, documents, emails, messaging platforms, case notes, images, and all other forms of information.

19. Access Control

Access to information must be limited according to role and need.

19.1 Open Internal Information

Some internal information may be broadly accessible within CDSJ because it is low-risk and operationally necessary.

19.2 Restricted Information

Personnel files, finance records, legal records, complaints records, supplier records, and similar materials must be restricted to authorised roles.

19.3 Highly Restricted Information

Safeguarding files, child protection files, sexual harassment files, PSEAH files, disciplinary files, health-related information, and other highly sensitive records must be accessible only to specifically authorised persons. Curiosity, status, or informal seniority is not a lawful basis for access.

20. Storage and Security Safeguards

CDSJ must take reasonable technical and organisational steps to secure personal information and confidential information against loss, damage, unauthorised access, or misuse.

This includes, where applicable:

- a. password-controlled systems;
- b. restricted folder access;
- c. secure storage of physical files;
- d. controlled sharing of highly sensitive records;
- e. secure backup practices; and
- f. proper disposal of data and documents.

This reflects the security safeguards condition recognised in POPIA.

21. Email, Messaging, and Digital Sharing of Information

Personal information and confidential information must not be shared through email, messaging platforms, shared drives, or file transfer methods in a careless or excessive manner.

The following rules apply:

- a. only the minimum necessary information should be shared;
- b. highly sensitive records should not be circulated broadly;
- c. recipients must be checked carefully;
- d. open group chats must not be used for highly sensitive personal information unless there is an approved and secure need; and
- e. screenshots, downloads, or exports of confidential information must not be created casually.

22. Cross-Border and External Sharing

Where CDSJ shares personal information with a partner, donor, consultant, service provider, or other third party, the responsible office must ensure that:

- a. there is a legitimate purpose for the sharing;
- b. the amount shared is limited to what is needed;
- c. the recipient is expected to protect the information appropriately; and
- d. any law, contract, consent, or policy condition relevant to the sharing is respected.

Cross-border sharing requires particular caution where the information is sensitive or where legal protections may differ.

23. Data Subject Participation, Access, and Correction

A person whose personal information is held by CDSJ may, subject to law and legitimate organisational limitations, request:

- a. confirmation of whether CDSJ holds their personal information;
- b. access to their information where appropriate;

- c. correction of inaccurate information; or
- d. clarification of how their information is being used.

Requests must be handled through an authorised internal route and in a manner that respects privacy, confidentiality, legal duty, and records management requirements. This reflects the data subject participation condition recognised in POPIA.

24. Record Retention and Disposal

Personal information must not be kept longer than is reasonably necessary for the purpose, legal obligation, operational accountability, or retention period applicable to the record type.

Retention and disposal must follow:

- a. this Policy;
- b. the Records Management and Document Retention Policy;
- c. any donor or legal requirement; and
- d. any litigation hold, safeguarding hold, audit hold, or investigation hold that applies.

When disposal is permitted, it must be done securely.

25. Security Compromises and Data Breaches

25.1 Immediate Reporting

Any person who becomes aware of a possible data breach, security compromise, unauthorised access, accidental disclosure, lost device, or suspicious information security event must report it immediately and not later than the same working day where possible.

25.2 Immediate Containment

The responsible office must take immediate steps to contain the issue where possible, such as:

- a. restricting access;
- b. recalling communication;
- c. disabling credentials;
- d. recovering devices or files; or
- e. escalating to the relevant technical or management authority.

25.3 Assessment and Notification

CDSJ must assess the compromise promptly and determine what internal and external notification is required. South Africa's Information Regulator has stated that all security compromises must be reported and that there is no low-risk threshold that removes the duty to report, and that notification should occur as soon as it is reasonably sure a compromise has occurred.

25.4 Record of Incident

A breach or compromise record must be maintained showing:

- a. what happened;
- b. when it happened or was discovered;
- c. what information was affected;
- d. immediate action taken; and
- e. follow-up action required.

26. Confidentiality in Employment, Grievance, Safeguarding, and Case Contexts

Where information relates to:

- a. staff employment matters;
- b. disciplinary or grievance processes;
- c. safeguarding or child protection concerns;
- d. sexual harassment or PSEAH matters;
- e. legal disputes; or
- f. health or psychosocial support,

the information must be handled with heightened sensitivity and shared only with those directly involved in lawful handling of the matter.

27. Public Use of Images, Stories, and Personal Details

No personal information, image, story, quote, or identifying detail may be used publicly by CDSJ unless:

- a. there is a lawful and legitimate basis to do so;
- b. the use is consistent with dignity and protection;
- c. any required consent or authorisation is in place; and
- d. the use does not expose the person to avoidable harm.

This rule is especially strict where the information relates to children, survivors, complainants, vulnerable persons, or high-risk communities.

28. Third-Party Service Providers and Processors

Where CDSJ uses an external service provider or processor to handle information on its behalf, CDSJ must ensure that the relationship includes reasonable confidentiality and security expectations.

Relevant arrangements should address:

- a. the purpose of processing;
- b. limits on use;
- c. confidentiality;
- d. security;
- e. return or destruction where appropriate; and
- f. incident notification expectations.

29. Training and Awareness

CDSJ should provide orientation and periodic awareness on privacy, confidentiality, and data handling appropriate to staff roles.

This may include:

- a. induction on confidentiality rules;
- b. handling of personnel and case information;
- c. breach reporting;
- d. safe storage and sharing practices; and
- e. role-specific guidance for high-risk information environments.

30. Misuse and Non-Compliance

The following are breaches of this Policy:

- a. unauthorised access to personal information;
- b. careless or excessive disclosure;
- c. storage of sensitive information in insecure locations;
- d. failure to report a known breach or compromise;
- e. use of information for unofficial or personal purposes;
- f. inaccurate or misleading record handling where correction was required; or
- g. destruction or concealment of information outside approved process.

Any such breach may result in corrective action, disciplinary action, governance review, contractual consequence, or legal response depending on seriousness.

31. Country Operations Clause

This Policy applies across all CDSJ operations.

Where a country of operation requires additional privacy notices, regulator notifications, cross-border transfer controls, local registration, sector-specific consent rules, or stronger personal information protections, CDSJ shall issue a country annex. The annex may add requirements but may not reduce the minimum privacy, confidentiality, and security standards in this Policy unless mandatory local law requires a different arrangement.

32. Related Instruments

This Policy shall be read together with:

- the Constitution of CDSJ;
- the CDSJ Policy Framework;
- the Board Governance and Oversight Charter;
- Human Resources Policy;
- Records Management and Document Retention Policy;
- Safeguarding Policy;
- Child Protection Policy;
- Sexual Harassment Policy;
- PSEAH Policy;
- Grievance and Complaints Handling Policy;
- Financial Management Policy;
- Email, Internet, Computer Use, and Cybersecurity Policy;
- Media, Communications, and Branding Policy; and
- any approved confidentiality undertakings, breach forms, access request forms, or country annexes.

33. Review

This Policy must be reviewed at least once every three years, or earlier if required by legal change, major breach, audit finding, regulator guidance, governance direction, or country expansion.

34. Approval

Approved by: Adv. Motlatsi J Mofolo
Approving Authority: Director and Boards Ex-Officio
Date of Approval: 10 February 2026
Effective Date: 1st March 2026

Version: 1.0



**CENTRE FOR DEVELOPMENT
IN SOCIAL JUSTICE**
A People-Centered Development