CONFIDENTIALITY AND DATA PROTECTION POLICY Icon for Child and Adult Nurturing (I-CAN) Social Enterprise

ICAN
Icon for Child and Adult Nurturing

Confidentiality and Data Protection Policy

1. Purpose

This policy outlines how ICAN ensures the protection, lawful handling, and confidentiality of personal and sensitive data collected, processed, or shared in the course of its activities. It aims to ensure that all ICAN personnel and partners understand their responsibilities regarding data protection, confidentiality, and safeguarding when working with individuals, communities, or organizations in connection with ICAN's mental health, education, and community development programs.

2. Scope

This policy applies to **all individuals and organizations working for or on behalf of ICAN**, including but not limited to:

- Full-time, part-time, or contractual employees
- Volunteers, interns, visiting fellows, and students
- Partner organizations and collaborating institutions
- Consultants and independent trainers
- External service providers with access to ICAN data

The policy applies to **all forms of information**, including:

- Personal information of clients, participants, or beneficiaries (adults and children
- Staff and volunteer data
- Organizational, financial, and program-related data
- Photographs, audio-visual material, and digital records collected during programs
- Information stored or processed on any medium — paper, digital devices, mobile phones, tablets, laptops, or cloud-based platforms
- There are **no exclusions** from compliance with this policy.

3. Principles of Data Protection

ICAN adheres to the following key principles in line with national and international data protection standards:

1. **Lawfulness, Fairness, and Transparency** – Data will be processed lawfully and transparently, with informed consent obtained from participants whenever required.
2. **Purpose Limitation** – Information will be collected only for specified, explicit, and legitimate purposes and will not be used for unrelated activities
3. **Data Minimization** – Only data strictly necessary for the stated purpose will be collected
4. **Accuracy** – ICAN will ensure that personal information is accurate and kept up to date.
5. **Storage Limitation** – Data will not be retained for longer than necessary and will be disposed of securely when no longer needed.
6. **Integrity and Confidentiality** – Information will be handled securely to prevent unauthorized access, alteration, or disclosure.
7. **Accountability** – All ICAN representatives and partner entities must ensure compliance with this policy.

4. Roles and Responsibilities

ICAN Board of Directors – Holds overall accountability for ensuring compliance with this policy.

Director (Data Controller) – Responsible for ensuring that systems, processes, and staff comply with data protection and confidentiality standards.

Project Leads / Coordinators – Ensure that all staff, volunteers, and partners under their supervision follow the confidentiality and data protection requirements.

Staff, Interns, and Volunteers – Must safeguard all personal and organizational information they access and report any data breaches or risks immediately.

Partner Organizations / Third Parties – Are required to sign a **Data Sharing and Confidentiality Agreement** (MOU) with ICAN, confirming adherence to equivalent standards of data protection.

5. Data Collection and Use

- Personal information shall only be collected where necessary for ICAN's operations, training, evaluation, or reporting requirements.
- Sensitive information related to mental health, trauma, or personal wellbeing will be collected and used strictly for support or training or intervention purposes with informed consent.
- All digital and paper-based forms must clearly state the purpose of data collection and obtain consent where applicable.

- Data collected for research or program evaluation will be anonymized whenever possible.

6. Data Storage and Security

- All records, whether paper-based or electronic, must be stored securely and accessible only to authorized personnel.
- Electronic data must be password-protected and stored on secure devices or approved cloud storage with encryption.
- Paper records containing personal data should be kept in locked cabinets when not in use.
- Data should not be transferred to personal email accounts, USB drives, or unapproved online platforms.

7. Data Accuracy

ICAN will take reasonable steps to ensure that personal data remains accurate and current. Staff may periodically contact participants or partners to confirm or update records.

8. Data Retention and Disposal

Information will be retained only as long as necessary for program, reporting, or legal requirements.
Upon expiry of the retention period, data will be securely destroyed — through shredding (for paper records) or permanent deletion (for digital files).

9. Third-Party and Partner Data Handling

Where ICAN partners with external organizations or individuals (e.g., volunteers, interns, training facilitators, or collaborative agencies), the following conditions apply:

A **Confidentiality and Data Sharing Agreement (MOU)** must be signed prior to accessing or collecting data.

All third parties must ensure that any data collected on behalf of ICAN is securely transmitted, stored, and disposed of in compliance with this policy.

No third party may use ICAN data for personal, promotional, or commercial purposes.

10. Breach Management

Any suspected or confirmed breach of data protection or confidentiality must be reported immediately to the **Director of ICAN**.
An internal review will be conducted to determine the cause, impact, and corrective actions. Breaches may lead to disciplinary action, termination of contracts, or legal consequences.

11. Training and Awareness

All ICAN staff, interns, and volunteers will receive orientation on confidentiality, safeguarding, and data protection protocols as part of their induction.
Refresher training will be conducted annually or when policies are updated.

12. Compliance and Monitoring

Regular internal reviews and audits will be conducted to ensure adherence to this policy. ICAN may engage external auditors or partner organizations for compliance verification.
The **Audit and Compliance Committee** will oversee the effectiveness of data protection measures and report findings to the Board.

13. Policy Review

This policy will be reviewed annually or earlier if significant changes occur in legislation, operational procedures, or ICAN’s program scope.