**Privacy Policy and Protection of Personal Data**
Adopted by the Board of Directors on: December 27, 2024, Montreal

---

## Table of Contents

## Introduction

Protecting privacy and ensuring the confidentiality of personal data is a priority for CCBI. We are committed to safeguarding the privacy of all individuals who provide personal information and upholding their rights regarding data protection. CCBI takes this responsibility seriously, earning the trust of those we serve by holding ourselves accountable to high professional and ethical standards. Transparency, honesty, and accountability are at the core of our work, ensuring that we consistently earn and maintain that trust.

In this spirit, CCBI has developed the **Privacy Policy and Protection of Personal Data**, which outlines the principles and procedures our organization adheres to in order to ensure the confidentiality and security of the data we collect, use, and retain. This policy draws on best practices in data protection, Canadian and international regulations, and our commitment to ethics and transparency.

The policy describes the types of personal information CCBI collects, how it is used, the circumstances under which it may be disclosed to third parties, and the security measures taken to protect it. We encourage you to read this policy carefully to understand how we protect personal information and to adhere to these principles and procedures in your work.

It is important to note that this policy also complies with **Law 25 (2024)**, which establishes additional requirements for personal data protection. CCBI ensures adherence to all provisions of this law to provide the highest level of protection for the personal data it processes.

Feel free to contact management if you have any questions or concerns about this policy or its application to your work.

## Designated Data Protection Officer

The management of CCBI assumes responsibility for data protection and confidentiality within the organization. As the designated data protection officer, management oversees the implementation and compliance with policies, procedures, and principles related to the confidentiality and security of personal information. Management is also responsible for addressing questions, concerns, and requests from members of the organization and affected individuals regarding data protection.

---

## Principles

1. **Accountability:** Every member of the organization is responsible for protecting the personal information they handle by adhering to this privacy policy and following management's guidelines.
2. **Data Minimization:** Personal information should only be collected to the extent necessary for carrying out responsibilities and in accordance with identified purposes.
3. **Non-Disclosure:** Personal information must not be disclosed to unauthorized third parties within or outside the organization without the explicit consent of the individual concerned or prior authorization from management.
4. **Confidentiality:** Internal records and sensitive information must not be discussed with unauthorized individuals to preserve the privacy and confidentiality of affected persons.
5. **Data Security:** Appropriate security measures must be implemented to protect personal information from unauthorized access, disclosure, alteration, or destruction.
6. **Notification:** Any breach of confidentiality or situation potentially compromising the security of personal information must be reported immediately to management.
7. **Respect for Rights:** The rights of individuals regarding privacy, including access, correction, and deletion of personal information, must be respected in accordance with the organization's privacy policy.

## Collection and Use of Personal Information

Our social enterprise collects only the personal information necessary to fulfill its business and social objectives, such as tax preparation, distributing funds, development and impact assessment of programming, T4A processing and managing partnerships. The personal information collected may include but is not limited to:

- Full legal name
- Mailing address
- Email address
- Phone number
- Date of birth
- Financial information (e.g., bank statements, tax details)
- Social insurance number
- Other relevant information as needed (e.g., demographics, program pertinence)

This information is collected lawfully and fairly and is used solely for the purposes for which it was collected. Whenever possible, personal information is collected directly from the individual concerned unless explicit consent is given to obtain it from another source.

CCBI uses the personal information collected for the following purposes:

- Filing Tax returns
- Processing T4As
- Managing collaborator, sponsor, and partner records
- Processing funds and prizes
- Organizing programs and training sessions
- Communicating about our activities and services
- Complying with legal and funder regulatory obligations
- Evaluating and improving programs and services

CCBI is committed to obtaining consent from individuals before collecting, using, or disclosing their personal information, except as permitted or required by law. Consent can be expressed (e.g., signing a form) or implied (e.g., voluntarily providing information).

Individuals have the right to withdraw their consent at any time, subject to legal or contractual restrictions and reasonable notice. If consent is withdrawn, CCBI will inform the individual of the consequences, including the potential impact on services and benefits.

## Data Destruction

CCBI recognizes the importance of prudent and respectful data management. Once personal information is no longer required to achieve its purposes, it is securely and permanently destroyed.

Destruction is carried out following industry best practices to ensure information cannot be recovered.

---

## Confidentiality Clause

All employees, board members, and partners of CCBI are bound by a strict confidentiality agreement. This agreement prohibits unauthorized access, use, or disclosure of personal information obtained during their duties with the organization. Non-compliance with this clause will result in disciplinary action, up to and including termination of contracts or agreements.

---

## Disclosure of Personal Information

CCBI will not disclose personal information to third parties unless required by law or with the explicit consent of the individual. Exceptions include legal obligations, emergencies involving threats to life or property, and other limited situations defined by applicable laws.

---

## Personal Information Security

The organization implements security measures to protect personal data from loss, theft, or unauthorized access. Measures include:

- Physical and Technical Barriers: Protection of premises where personal information is stored, use of firewalls, antivirus software, and data encryption.
- Backup and Recovery Procedures: Safeguards against accidental loss of personal information through backup and data recovery systems.
- Access Management: Implementation of procedures to ensure that only authorized individuals can access personal information.

- Staff Awareness: Training staff on the importance of confidentiality and establishing policies and procedures to ensure the protection of personal information.
- Incident Management: Establishment of procedures to handle emergencies and security incidents.
- Vendor Management: Procedures to ensure that vendors with access to personal information comply with appropriate privacy practices.
- Physical Measures: Secure storage of personal information and restricted access to areas where personal information is kept.

CCBI strives to maintain up-to-date security measures and regularly assesses risks to the confidentiality of information. In the event of a security incident, CCBI will take appropriate measures to contain the incident, evaluate its impact, and inform affected individuals in accordance with applicable legal requirements.

It is important to note that, while CCBI endeavors to protect personal information, no method of electronic transmission or storage is completely foolproof. Therefore, CCBI cannot guarantee absolute security of personal information but is committed to making every effort to ensure its protection. We pledge to regularly update these measures to adapt to advancements in technology and evolving security threats.

## Access, Correction, and Updates to Personal Information

Individuals have the right to access their personal information held by CCBI and request corrections or updates if the information is inaccurate or incomplete.

Requests for access or correction can be made by contacting the organization's designated Data Protection Officer. To ensure security, individuals may be required to verify their identity before accessing or modifying their records.

CCBI commits to responding to access and correction requests promptly, usually within 30 days. In cases where access is denied, the organization will provide an explanation, except where prohibited by law.

## Use of Cookies and Similar Technologies

CCBI's website may use cookies and similar technologies to enhance user experience, gather usage data, and improve online services.

Cookies are small files stored on a user's device when visiting the website. They may collect information such as browser type, pages visited, and session duration.

Users can manage their cookie preferences by adjusting their browser settings to block or delete cookies. However, disabling cookies may affect the functionality of certain website features.

By using the website, users consent to the use of cookies in accordance with this policy.

---

## Links to Other Websites

CCBI's website may contain links to third-party websites for informational purposes. These external websites operate independently and are not governed by this Privacy Policy.

CCBI is not responsible for the privacy practices or content of these third-party sites. Users are encouraged to review the privacy policies of any external websites they visit.

---

## Changes to This Privacy Policy

CCBI reserves the right to amend this Privacy Policy at any time to reflect changes in regulations, organizational practices, or other circumstances.

When changes are made, the updated policy will be posted on the organization's website with a revised adoption date.

Significant changes will be communicated to affected individuals directly, where feasible, and their continued use of CCBI's services will constitute acceptance of the updated policy.

## Contact Us

For questions, concerns, or requests related to this Privacy Policy or the organization's data protection practices, please contact:

**CCBI Data Protection Officer**
info@ccbi.ca
1988 Sainte catherine est #201, Montréal, Qc H2K 2H7

---

## Conclusion

CCBI remains committed to protecting the privacy and personal information of individuals interacting with the organization. This Privacy Policy serves as a cornerstone of that commitment, outlining the principles and procedures we follow to ensure responsible and ethical data management.

Your trust is vital to our mission, and we pledge to uphold the highest standards of data protection and confidentiality in all our activities.

# Annexes

## Annexe 1. Procedure for Managing Data Security Incidents

CCBI takes data security incidents seriously and follows a defined procedure to address them:

1. **Identification:** Employees or contractors must immediately report any suspected or confirmed data breaches to management.
2. **Containment:** Immediate actions will be taken to prevent further unauthorized access or damage, such as disabling compromised accounts or isolating affected systems.
3. **Investigation:** A thorough review will determine the scope and cause of the breach.
4. **Notification:** If personal information is involved, affected individuals and relevant authorities will be notified as required by law.
5. **Mitigation:** Corrective actions will be implemented to prevent future incidents, such as revising protocols or enhancing security measures.

---

**Annexe 2. Procedures for Managing Data Collection and Destruction**

**1. Tax Return Information**

- **Data Collected:** Income, expenses, statements, credits, deductions, supporting documents, and other financial details required for tax preparation.
- **Collection Methods:** Directly from clients through intake forms, interviews, and digital submissions.
- **Storage:** Secure, encrypted databases with access limited to authorized personnel.
- **Destruction:** No paper documents are accepted, electronic records are securely deleted after statutory retention periods.

---

**2. Program Participants and Impact Assessments**

- **Data Collected::** Participant registration details, demographic data, impact assessment data and program feedback.
- **Collection Methods:** Online registration forms, interviews, group and individual surveys.
- **Storage:** Secure membership database with layered access controls. Restricted access database, organized by program to facilitate anonymization during analysis.
- **Destruction:** Data is anonymized or securely deleted when no longer needed for evaluation or reporting purposes.

---

**3. Membership Registration and Updates**

- **Data Collected:** Member registration information, demographic data, preferences, updates, and participation details for special offers/events.
- **Collection Methods:** Membership forms submitted online.
- **Storage:** Secure membership database with layered access controls.
- **Destruction:** Member data is securely deleted or anonymized upon cancellation or after prolonged inactivity, per organizational policies.

---

**4. Suppliers**

- **Data Collected:** Supplier contracts, contact details, and tax information (e.g., NAS for T4A issuance).
- **Collection Methods:** Vendor registration forms and contractual agreements.
- **Storage:** Financial systems and team directories with administrative access only.
- **Destruction:** Records are archived or securely deleted following the fulfillment of contractual and regulatory obligations following statutory retention periods for financial supporting documents.

---

**5. Employees and Board Members**

- **Data Collected:** Legal names, SINs, birthdates, addresses for employment, partnership agreements, governance records, and other legal documentation.
- **Collection Methods:** Onboarding processes, forms, and applications.
- **Storage:** Human resources systems with restricted access.
- **Destruction:** Records are securely destroyed following statutory retention periods in accordance with labor laws.

---

**6. Financial Contributions and Records**

- **Data Collected:** Donor and sponsor contact information.
- **Collection Methods:** Donation forms, online payment systems, or third-party platforms.
- **Storage:** Secure management systems compliant with applicable regulations.
- **Destruction:** Data is securely deleted after statutory retention periods.

---

**7. Partners and Collaborators**

- **Data Collected:** Contact information, partnership agreements, and shared resources.
- **Collection Methods:** Partnership agreements.
- **Storage:** Document management systems with shared but restricted access.
- **Destruction:** Information is removed from shared systems and securely deleted upon partnership termination.