

INFORMATION TECHNOLOGY AND PRIVACY POLICIES

PRIVACY AND CONFIDENTIALITY POLICY

Date of Origin: August 19, 2022

Date of Last Revision: N/A

Approval Date: August 19, 2022

Approved by: Executive Director

POLICY

The Child Witness Centre values the trust of our clients, volunteers, donors, staff members, supporters, and all others who work with us. We recognize that maintaining trust requires that we be transparent and accountable in how we manage personal information. The Child Witness Centre adheres to all applicable privacy legislation and aims to go above the basic standards of legislation.

The Child Witness Centre strives for a privacy program that operates within a culture of privacy; however, legal compliance should be one result of a successful program, not the only goal. A culture of privacy provides a shared understanding of how personal data can and should be used to support broader strategic objectives. This improves the ability of the privacy program to ensure alignment across our teams, increasing their understanding of and desire to support the achievement of privacy goals.

SCOPE

This policy applies to all employees, sub-contractors, third-party vendors, and volunteers in service of clients, and/or donors.

RATIONALE

In conducting our various programs and activities, including raising funds to support our work, we frequently collect, use and disclose personal information. Anyone from whom we collect such information can expect that it will be carefully protected and that any use of or other dealing with this information is subject to consent. Our privacy practices are designed to achieve this.

This policy is intended to outline our practices and procedures that are in place to protect confidentiality and privacy and refers to consistent standards and obligations that employees, volunteers and contractors need to be aware of in regard to the personal and confidential information under the custody and control of the Child Witness Centre.

WHAT IS PERSONAL INFORMATION?

Under the Personal Information Protection and Electronic Documents Act (PIPEDA), personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- age, name, ID numbers, income, ethnic origin, or blood type;
- opinions, evaluations, comments, social status, or disciplinary actions; and
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).

Employee information such as name, title or contact information is not considered personal information and generally is made available to the public.

As an organization we collect various personal information data, this information helps us to contact clients, process transactions, and help us make informed decisions about our programs. In some situations, we de-identify information for statistical purposes so information is not able to be traced back to individuals. This may include summary information on individuals preferred languages to allow us to plan for multi-lingual materials, form example.

PROCEDURES

OVERVIEW

The Child Witness Centre adheres to the 10 fair information principles to protect personal information, which are set out in Schedule 1 of PIPEDA. The principles are:

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

In addition to these principles, PIPEDA states that any collection, use or disclosure of personal information must only be for purposes that a reasonable person would consider appropriate in the circumstances.

The following purposes would be considered inappropriate by a reasonable person:

- collecting, using or disclosing personal information in ways that are otherwise unlawful;
- profiling or categorizing individuals in a way that leads to unfair, unethical or discriminatory treatment contrary to human rights law;
- collecting, using or disclosing personal information for purposes that are known or likely to cause significant harm to the individual;
- publishing personal information with the intent of charging people for its removal;
- requiring passwords to social media accounts for the purpose of employee screening; and
- conducting surveillance on an individual using their own device's audio or video functions.

FUNDRAISING AND CANADA'S ANTI-SPAM LEGISLATION

Canada's Anti-Spam Legislation (CASL) provisions, such as those relating to sending commercial electronic messages (CEMs) and installing computer programs, applies to activities of non-profit organizations. However, there is an exemption under section 3(g) of the Governor-in-Council Regulations for CEMs sent by or on behalf of a registered charity, as defined under the INCOME TAX ACT, where the primary purpose of the CEM is to raise funds for the charity.

The "primary purpose" of a CEM means the main reason or main purpose of the CEM. There could be a secondary or additional purpose to the message, but the principal purpose of the CEM must be to raise funds for the charity.

Examples

Where the primary purpose **is** raising funds (CASL may not apply):

Example 1: A CEM, sent by or on behalf of the Child Witness Centre, which promotes an event and/or the sale of tickets for an event – such as a dinner, golf tournament, theatrical production or concert or other fundraising event – where the proceeds from ticket sales flow to the registered charity.

Example 2: The Child Witness Centre sends, by email, a newsletter which provides information about the agency's activities or an upcoming campaign, but which also contains a section which solicits donations for the purpose of raising funds for the charity and mentions corporate sponsors who supported the charity (but does not encourage the recipient to participate in a commercial activity with that sponsor). While this message may be considered a CEM under CASL, the primary purpose of the message may be viewed as raising funds; therefore, the exemption in the GIC Regulations could apply.

Where the primary purpose **is not** raising funds (CASL may apply):

Example: The Child Witness Centre sends, by email, a newsletter which provides information about the charity's activities or about a particular social issue. If this email also advertises the corporate sponsors of a charity's event and encourages the email recipient to participate in a commercial activity with that sponsor, then the primary purpose of the message may not be to raise funds for the charity and section 6 of the CASL may apply without any exemption.

The Child Witness Centre strives to maintain the trust and respect of its donors and at no time will we sell donors information or share information for any other purpose than the reason for which the individual has consented for use of the information. Furthermore, all electronic communications are intended to serve the donor by providing them insights into the agency, how funds are utilized and event notification. Donors may unsubscribe to newsletter directly or ask to be removed from mailing lists at any time. This can also be done by emailing our Marketing, Events and Communication Coordinator directly.

CONSENT AND CASL

The Child Witness Centre may rely on implied consent when it comes to electronic communication to donors and other stakeholders. This may include having an existing business relationship based on a previous commercial transaction with our organization; or having an existing non-business relationship based on, for example, membership, or if the recipient participated as a volunteer for your charitable organization; or where a person makes their email address publicly available by publishing it on a website. Typically, individuals who have provided a donation to our agency will be added to our electronic mailing list, unless otherwise requested not to be and will receive our development team updates and newsletters. Individuals may opt-out at any time, and we will ensure this has been completed within 10 business days.

ACCOUNTABILITY

The Child Witness Centre is accountable for all personal information in its possession, custody and control, all of which will be kept private and secure. However, the Child Witness Centre may be required to release/make available information to a number of sources, including parents/guardians, child protection, police services and legal counsel, in the following circumstances:

- if the CWC receives a warrant/subpoena to release and produce client records to a criminal, civil or family court of law;
- suspicions of child abuse;
- concerns for child safety and wellbeing or child maltreatment and
- if any staff at CWC is made aware of a risk of serious harm to the client or others.

All employees, contractors, volunteers, students and other third parties who have dealings with the Child Witness Centre must be aware of and follow the privacy policies and procedures put in

place to conform to principles embodied in its privacy code. In short, employees, contractors, volunteers, students and other third parties who have dealings with our agency must ensure that any personal information held in their possession is kept private.

IDENTIFYING PURPOSE

The Child Witness Centre will identify, document, and share the purposes for collecting personal information. The Child Witness Centre will explain to its clients, donors, volunteers, and employees the purpose for collecting their information and will obtain consent again, should a new purpose for collecting the information arise. Depending on how the information is collected, this may be done orally or in writing.

OBTAIN VALID AND INFORMED CONSENT

The Child Witness Centre believes it is important for individuals who are providing their personal information are doing so in a meaningful and informed manner.

Prior to receiving consent to collect personal information the Child Witness Centre will inform and educate individuals on:

- what personal information is being collected, with sufficient precision for individuals to meaningfully understand what they are consenting to;
- with which parties' personal information is being shared;
- for what purposes personal information is being collected, used or disclosed, in sufficient detail for individuals to meaningfully understand what they are consenting to; and
- what are the risks of harm and other consequences.
- In most cases consent will be expressly sought and documented. The Child Witness Centre will consider whether the consent is implied or express by assessing and determining if:
 - the information being collected, used or disclosed is sensitive;
 - the collection, use or disclosure is outside of the reasonable expectations of the individual; and/or,
 - the collection, use or disclosure creates a meaningful residual risk of significant harm.

In rare occasions implied consent may apply in strictly defined circumstances.

In general, all information will be collected, used and disclosed with an individual's consent; however, the Child Witness Centre may collect, use or disclose personal information without consent in a life-threatening situation, or where otherwise required or permitted by law. The Child Witness Centre will explain to the individual the consequences of a withdrawal of consent.

Consent can only be required for collections, uses or disclosures that are necessary to fulfil an explicitly specified and legitimate purpose. For non-integral collections, uses and disclosures, individuals must be given a choice.

In the case where a client chooses not to provide the agency with consent to collect, use or disclose personal information, the Child Witness Centre may have insufficient information to provide services to the client. In some cases, the refusal to provide consent may limit the services and benefits that the agency is able to offer the individual.

Individuals can withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice, and you must inform individuals of the implications of withdrawal.

FULFILLING OUR RESPONSIBILITIES

The Child Witness Centre will endeavour to meet the responsibilities of obtaining consent by making privacy information readily available in complete form, while giving emphasis or bringing attention to four key elements:

- what personal information is being collected, with sufficient precision for individuals to meaningfully understand what they are consenting to;
- with which parties personal information is being shared;
- for what purposes personal information is being collected, used or disclosed, in sufficient detail for individuals to meaningfully understand what they are consenting to; and
- what are the risks of harm and other consequences.

In addition, the Child Witness Centre will:

- provide information in manageable and easily accessible ways.
- make available to individuals in a clear and easily accessible choice for any collection, use or disclosure that is not necessary to provide the product or service.
- consider the perspective of your clients, to ensure consent processes are user-friendly and generally understandable.
- obtain consent when making significant changes to privacy practices, including use of data for new purposes or disclosures to new third parties.
- obtain consent from a substitute decision maker for any individual unable to provide meaningful consent themselves (the OPC takes the position that, in all but exceptional circumstances, this includes anyone under the age of 13), and ensure that the consent process for youth able to provide consent themselves reasonably considers their level of maturity.

LIMITING COLLECTION

The Child Witness Centre will only collect information that is necessary to fulfill a legitimate identified purpose such as for the provision of service, processing a donation or payroll processing in the case of employee personal information.

Whenever possible, information will be collected directly from the individual requesting services from the agency; however, information may also be collected indirectly (e.g., referral sources and other third parties) provided consent is obtained from the individual and/or the parent/guardian and when reasonable and appropriate.

The purposes for which personal information is collected, used and disclosed will be identified in advance of collection.

Collecting less information also reduces the risk and/or impact of loss or inappropriate access, use or disclosure.

We collect, use and share personal information to:

- Provide services through our Child Witness Program and Child and Youth Advocacy Program;
- Plan and manage services, including making referrals to appropriate services;
- Aid a law enforcement agency in an investigation;
- Seek consent (or consent of a substitute decision-maker) where appropriate;
- Receive payment or process, monitor, verify or reimburse claims for payment as related to our mandate;
- Detect, monitor or prevent fraud or any unauthorized receipt of services or financial benefits;
- Conduct risk management, error management and quality improvement activities;
- Conduct service recipient surveying;
- Conduct research (subject to certain rules);
- Compile statistics;
- Report to the government as required by law;
- Process payroll and benefits and other employee relation processes;
- Process donations;
- Allow for the analysis, administration and management of our programs;
- Comply with legal and regulatory requirements; and
- Fulfill other purposes permitted or required by law.

LIMIT USE, DISCLOSURE AND RETENTION

Unless someone consents otherwise—or unless doing so is required by law—the Child Witness Centre may use or disclose personal information only for the identified purposes for which it was collected. The agency will keep personal information only as long as it is needed to serve those purposes or as required by law. We will obtain fresh consent if we intend to use or disclose personal information for a new purpose. Exceptions to this rule include:

- if the agency receives a warrant/subpoena to release and produce records to a criminal, civil or family court of law;
- we have suspicions of child abuse, safety or maltreatment and are obligated to report the matter to child protection services;
- if any staff member is made aware of a risk of serious harm to a client or others.

For detailed descriptions of retention and destruction policies and practices please see Records Storage, Retention and Destruction Policy for more information on specific timelines for maintaining and destroying records.

FULFILLING RESPONSIBILITIES

In order to meet our obligations regarding limiting the use, disclosure and retention of personal information the Child Witness Centre will:

- document any new purpose for the use of personal information and seek consent with effected individuals.
- limit and monitor employee access to personal information, and take appropriate action when information is accessed without authorization.
- dispose of personal information that does not have a specific purpose or no longer fulfills its intended purpose. The agency will dispose of information in a way that prevents a privacy breach, such as by securely shredding paper files or effectively deleting electronic records. If information is to be retained purely for statistical purposes, employ effective techniques that would render it anonymous.
- ensure all personal information is fully deleted before disposing of electronic devices such as computers, photocopiers and cellphones.
- ensure your employees receive appropriate training on their roles and responsibilities in protecting personal information.

ACCURACY

The Child Witness Centre is committed to ensuring that personal information collected is accurate and up to date. There are some reasons why personal information may be inaccurate:

- the personal information may have been incorrect when it was collected. For example, an individual indicating their address is a "street" rather than an "avenue."
- the personal information may have been captured incorrectly, such as when a staff member enters in a phone number into a client database. Names and numbers are also often transposed.

- the personal information may have become out-of-date over time, such as when people change addresses or phone numbers, or when they get married or divorced.
- the personal information may have been incorrectly associated, such as when one person's information is associated with another person who has the same name.

All avenues should be explored in verifying the accuracy and completeness of the personal information held by the Child Witness Centre. Incomplete and inaccurate information can result in privacy breaches, delay in service and misleading documentation. Employees will:

- conduct periodic checks, directly with the individual the information is about or using other authorized avenues, to ensure the information is still current and valid;
- ensure thorough reviews of applications to ensure all questions are answered completely. Confirm information if it is ambiguous;
- comply with an individual's right to rectify information that is incorrect and will consider any challenges to the accuracy of the information;
- will clearly identify any matters of opinion, and where appropriate whose opinion it is and any underlying facts about the matter; and
- material errors/corrections will be documented.

In general, the Child Witness Centre is responsible for ensuring the accuracy of information is collected, however in some cases the responsibility remains with the client, employee, or other stakeholder. For example, if an employee moves house, it is their responsibility to update the employer so that the Child Witness Centre has a correct record of address. If an employee comes to know that a client has recently moved, it is the responsibility of the employee to check the client record and amend accordingly.

SAFEGUARDS

Appropriate steps must be taken to safeguard personal information to protect all personal information (regardless of how it is stored) against loss, theft, or any unauthorized access, disclosure, copying, use or modification. The Child Witness Centre will take measures, including physical, administrative, and technical safeguards, to protect personal information from loss, misuse, unauthorized access, disclosure, alteration or destruction. The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution and format of the information and the method of storage. More sensitive information will be safeguarded by a higher level of protection.

The Child Witness Centre will employ a variety of measures to maintain the security of personal information, this includes; physical measures (e.g., locked filing cabinets, restricting access to offices, and alarm systems); up-to-date technological tools (e.g., passwords, encryption, firewalls and security patches); and organizational controls (e.g., security clearances, limiting access, staff training and agreements).

Specifically:

- all employees, contractors, fee for service staff, students and volunteers are required to sign a confidentiality agreement at the beginning of employment or involvement with the Child Witness Centre, and annually thereafter. All third party contractors retained by the Child Witness Centre will also be required to adhere to the agency's Privacy and Confidentiality Policies;
- all confidential information paper files will be stored in secure cabinets, which will be locked outside of business hours or when not in use; access to confidential client information will be limited to those who need to know the information or as otherwise permitted or required by law;
- employees, contractors, and students are only to access, process and transmit confidential information and/or client records using authorized hardware, software and other equipment;
- information stored in the agency's computer network is protected through the use of usernames and passwords; dual and/or multi-factor authentication will be utilized whenever possible. Information is limited to a need-to-know user access.
- email and text communication is only initiated with the informed consent of clients and procedures are in place to minimize risk;
- care is used when transporting confidential documents to prevent unauthorized parties from gaining access to personal information during the process;
- precautions are taken so that conversations regarding client information are not inadvertently overheard by others; appointment books and/or confidential information on electronic devices are to be closed when not in use; and
- employees will receive regular training on information security and privacy.

Appropriate steps shall always be taken to safeguard personal information. However, individuals will be notified at the first reasonable opportunity if information is stolen, lost or accessed by an unauthorized person or if personal information is used and/or disclosed without consent in a manner that is not in line with the privacy policies or procedures of the agency. The Child Witness Centre has a duty to report qualifying breaches in privacy to the Office of the Privacy Commissioner of Canada.

OPENNESS

The Child Witness Centre endeavours to provide detailed personal information management practices that are clear and easy to understand. Our privacy statement will be posted on our agency website and reviewed at least annually. Individuals often find privacy policies difficult to understand, yet they feel compelled to give their consent to obtain the services they want. Individuals should not be expected to decipher complex legal language to make informed decisions on whether to provide consent. The Child Witness Centre Chief Privacy Officer is the Executive Director. Questions, concerns, or complaints should be directed to their attention.

FULFILLING OUR RESPONSIBILITIES

The Child Witness Centre will:

- comply with guidelines on obtaining meaningful and informed consent.
- ensure our staff members are familiar with the agency's procedures for responding to people's inquiries about their personal information.
- provide, in easy-to-understand terms: the name and contact information of the person who is accountable for the agency's privacy policies and practices and with whom access requests should be sent, how an individual can gain access to their personal information; how an individual can make a complaint; and a description of what personal information we disclose to other organizations, including any third parties, and why.

ACCESS

Individuals have a right to access the personal information that the Child Witness Centre holds about them. They also have the right to challenge the accuracy and completeness of the information, and have that information amended as appropriate.

The Child Witness Centre will:

- when asked, advise people about the personal information about them our organization holds.
- explain where the information was obtained.
- explain how that information is or has been used and to whom it has been disclosed.
- give people access to their information at minimal or no cost or explain your reasons for not providing access. Providing access can take different forms. For example, we may provide a written or electronic copy of the information or allow the individual to view the information or listen to a recording of the information.
- correct or amend personal information in cases where accuracy and completeness is deficient.
- note any disputes on the file and advise third parties where appropriate.

Individuals who request client information, e.g., past client records, must provide photo identification prior to release of information. We will not release records to individuals who are not the individual for whom the record is being requested, e.g., parent, spouse without a subpoena/warrant. In rare circumstances individuals may be refused access to information, in these exceptional circumstances the individual will be provided in writing the reason for the refusal and their options for recourse, such as filing a complaint with the OPC.

CHALLENGING COMPLIANCE

The Child Witness Centre welcomes feedback and critique regarding our compliance with the fair information principles and Canada's Anti-Spam Legislation. Individuals with concerns, comments or complaints should address these matters with the Chief Privacy Officer of the organization. As an organization we will:

- provide recourse through a simple complaint handling and investigation policy and procedure.

- tell complainants about their avenues of recourse. These include our organization's own complaint procedures, along with those related to industry associations, regulatory bodies and the OPC.
- investigate all complaints receive and provide feedback to complainant.
- improve any information-handling practices and policies that are found to be problematic.

TRAINING AND ADHERENCE TO POLICY

Each staff member and volunteer will receive training on privacy and information security at the time of onboarding and on an annual, or more frequently basis thereafter. Employees and volunteers are required to sign an oath of confidentiality confirming their understanding and agreement to maintain privacy and confidentiality regarding client and business information.

Employees or volunteers who have breached this policy are subject to performance management measures, up to and including termination if they are found to have been callous in their handling of client information and have breached privacy procedures.

Third party vendors must also comply with our policy and ensure their company has in place appropriate training for their staff members, auditing and evaluation of privacy programs. The CWC may request confirmation that privacy programs are in place for our vendors. Failing to maintain privacy on behalf of our client could result in the cancellation of contracts and agreements.

PRIVACY OFFICER

The Child Witness Centre has an appointed a Privacy Officer to facilitate compliance with this policy, and other policies that relate to privacy/confidentiality, as well as any relevant legislation.

The Privacy Officer will also be responsible for receiving complaints and taking appropriate action. Staff that receive requests for information, must notify the Privacy Officer.

The Chief Privacy Officer is the Executive Director and may be contacted at 519-744-0904 (ext. 212).

If an individual is not satisfied with the response of the Chief Privacy Officer, a complaint may be directed to the Privacy Commissioner for Ontario, for issues with respect to the handling of personal information.

The Privacy Commissioner can be contacted:

Toll-free: 1-800-282-1376

Phone: (819) 994-5444

TTY: (819) 994-6591

REFERENCES AND RELATED FORMS, POLICIES AND PROCEDURES

IP - Records Retention, Storage and Destruction Policy

SS – Feedback and Complaints Policy

Personal Information Protection and Electronic Documents Act, 2015 (PIPEDA)

Canada's Anti-Spam Legislation (CASL)