POLICIES and PROCEDURES

"All children and youth achieve their greatest potential within caring, responsive families and communities."
PINT Vision Statement

SECTION: ORGANIZATIONAL POLICIES
SUB-SECTION: INFORMATION MANAGEMENT
PRIVACY AND PROTECTION OF PERSONAL INFORMATION
CROSS-REFERENCE(S): To consider for cross-references: HR-17 CONFIDENTIALITY / DUTY TO RESPECT PRIVACY HR-18 PERSONAL HEALTH INFORMATION PROTECTION ACT (PHIPA) POLICY S-135 AUTHORIZATION FOR SERVICE AND CONSENTS Breach of Privacy of Information Use of Client Information in Public Relations Activities Programs and Services – Confidentiality of Client Information Confidentiality Policies Complaints Policy

POLICY NUMBER: INFO-18	DATE APPROVED: 2023-11-28
DATE REVIEWED: 2023-08-31	APPROVED BY: BOARD OF DIRECTORS

RATIONALE:

- To establish procedures for the collection, use and disclosure of personal information (PI) and personal health information (PHI) in the custody or under the control of Point in Time Centre for Children Youth and Families (PinT); and

- To ensure that PinT meets the requirements of the *Personal Health Information Protection Act, 2004* (Ontario) (PHIPA), *Child, Youth and Family Services Act, 2017* (CYFSA) and *Personal Information Protection and Electronic Documents Act* (PIPEDA), as applicable.

POLICY STATEMENT:

PinT is a health information custodian for the purposes of PHIPA and a service provider for the purposes of Part X (Personal Information) of the CYFSA and is responsible for the PHI and PI, respectively, within its custody or control. PinT has established and monitors information practices that comply with PHIPA and CYFSA.

PinT only collects PI and PHI that is necessary to operate its programs, services and activities. Records are held and disposed of securely, in accordance with the Records Retention schedule, and access is limited on a need-to-know basis.

PinT values the trust of those we work with, and of the public, and recognizes that maintaining this trust requires that we be transparent and accountable in how we treat the information that is shared with us.

PinT collects and uses PI and PHI in connection with various projects and activities. Anyone from whom PI and/or PHI is collected should expect that it will be carefully protected and that any further use or disclosure beyond the purposes for which it was collected will be subject to consent.

Even where privacy laws are not directly applicable to PinT activities, PinT adopts the ten privacy principles set out in the CSA Model Code for the Protection of Privacy (Schedule 1 to PIPEDA), which form the foundation for this policy.

SCOPE:

This policy applies to PinT clients, donors, staff, volunteers, and Board members and describes the principles PinT will use to protect the privacy of PI and/or PHI.

DEFINITIONS:

"Capable" means able to understand the information that is relevant to deciding whether to consent to the collection, use or disclosure of PI or PHI and able to appreciate the reasonably foreseeable consequences of giving, withholding, or withdrawing the consent.

"Information practices" means the policy or practices respecting the collection, use, modification, disclosure, retention or disposal of personal information or personal health information and the administrative, technical and physical safeguards and practices that PinT maintains with respect to the information.

"***Personal Health Information***" or ***"PHI"*** as defined by PHIPA eans identifying information about an individual if that information relates to a person's physical or mental health, or relates to the provision of health care to the individual, including the identification of a person as a provider of health care; is a plan of service for an individual; relates to an individual's eligibility for health care.

Personal Information or **"PI"** – as defined by CYFSA, means recorded information about an identifiable individual. Any information that can be used to distinguish, identify, or contact a specific individual. This information can include an individual's opinions or views, as well as facts about, or related to, the individual. Personal information does not include business contact information or publicly available information.

"Substitute decision-maker" means a person who is authorized to consent, withhold or withdraw consent on behalf of an individual.

POLICY PRINCIPLES:

Principle 1 - Accountability

PinT is responsible for PI and PHI in its custody or control, including any PI or PHI being handled or processed by a third party on PinT's behalf. Accountability for PinT's compliance with this policy is the responsibility of the Chief Privacy Officer (Executive Director) or designate.

PinT has taken steps to give effect to this Policy, including:

- Informing staff and stakeholders of its information practices;
- Training staff and volunteers to understand and follow its information practices;
- Establishing policies and procedures to receive and respond to questions and complaints;
- Overseeing compliance with its information practices, which may include performing privacy audits.

PinT has implemented additional information practices to meet its privacy obligations. They include:

- HR-17 Confidentiality / Duty to Respect Privacy
- S-135 Authorization for Service and Consents
- Breach of Privacy of Information
- Use of Client Information in Public Relations Activities
- Programs and Services – Confidentiality of Client Information
- Confidentiality Policies
- Complaints Policy

Principle 2 - Identifying Purposes

At or before the time PI and/or PHI is collected, PinT will identify the purposes for which PI and PHI are collected. The primary purposes for which PinT collects PI and PHI include:

Clients:

- To inform treatment, academic and child development goals
- For public relations activities (see Policy: Use of Client Information for Public Relations Activities);
- For special internal events such as graduation;
- To maintain a network of alumni; and
- To inform program and service planning including the efforts in engagement, diversity, equity and inclusion, and the self-assessment of the agency to gain accreditation status

Management/Operational Responsibilities:

- To complete quality assurance tasks;
- To complete a self-assessment of the organization for accreditation purposes;
- To comply with the requirements of the accreditation process (site visits and file audits);
- To maintain professional supervision of programs, services and employees; and
- To comply with financial audit requirements.

Donors:

- To establish a relationship and to communicate;
- To understand donor identity and identify how we may improve our services to meet donor needs;
- To reach our fundraising goals;
- To process donations;
- To provide donors with information about PinT;
- To respond to donor requests for information; and
- To recognize individual donations publicly with the donor's consent.

Staff and Volunteers:

- To recruit, hire, train, recognize and retain highly qualified and motivated individuals;
- To establish and maintain harmonious employer-staff relations;

- To administer PinT policies and procedures;
- To manage and promote the philanthropic activities of PinT; and
- To meet legal, regulatory or contractual requirements.

Depending on the way in which the information is collected, PinT may specify the purposes orally, electronically and/or through notice to the client.

When PI and PHI collected is to be used for a purpose not previously identified, the purpose will be identified prior to its use. Unless required by law, consent of the individual is required before the information can be used for that purpose.

Persons who collect PI and PHI will be able to explain to individuals the purposes for which the information is being collected.

Principle 3 - Consent

PinT will only collect, use or disclose PI or PHI about an individual for the purpose of providing a service or treatment with the individual's consent, where such collection, use or disclosure is for a lawful purpose or where the collection, use or disclosure is permitted or required by law.

The knowledge and consent of the individual are required for the collection, use and disclosure of PI and PHI. In order to be knowledgeable, it must be reasonable in the circumstances to believe that the individual knows the purposes of the collection, use or disclosure and knows that they may give or withhold consent. PinT will make reasonable efforts to make sure that individuals are knowledgeable about how their PI or PHI will be collected, used or disclosed at the time of collection, which may include the use of written notice.

Consent for the collection and use of PI may be implied if the collection is made directly from the individual to whom the information relates and is collected for the purpose of providing a service. A consent may be written or oral, but an oral consent may only be relied on if the service provider who obtains it documents the name of the individual who provided consent, the information to which the consent relates and the manner in which notice was provided.

Where a client is incapable of consenting to the collection, use or disclosure of PI or PHI, for example, where the individual is seriously ill or mentally incapacitated, consent may be given by the person's substitute decision maker.

An individual may withdraw consent at any time, subject to legal restrictions and reasonable notice. Withdrawal of consent will not have a retroactive effect. Pin T will inform the individual of the implications of such a withdrawal. A request to withdraw consent can be made to a Manager using the *Consent to Release Information Form*.

<u>Documentation of Consent to Disclose Personal Information:</u>

If applicable, when releasing or sharing personal information, PinT documents the individual's express consent on the Consent to Release Information Form, including:

- Their name;
- Organization and staff person's name;
- Name of person or organization to which the information is being released;
- Specific information being released;
- Date of consent; and
- Any limits on the consent (for example: time period for consent, special conditions).

Use and Disclosure of PI or PHI without Consent

PinT may use PI or PHI without consent of the individual, in certain circumstances, as permitted or required by law. For example, PinT may use PI or PHI where it believes on reasonable grounds that this is necessary to assess, reduce or eliminate a risk of serious harm to a person or group of persons; for planning, managing or delivering services or for purposes of risk management or quality improvement.

PinT may disclose PI or PHI without the knowledge and consent of the individual in circumstances where such disclosure is permitted or required by law. For example, PinT may disclose PI or PHI to comply with a court order, subpoena or warrant; to law enforcement to aid in an investigation or to assist the activities of an investigative body; or where it believes on reasonable grounds that the disclosure is necessary to assess, reduce or eliminate a risk of serious harm to a person or group of persons.

PinT will comply with PHIPA and CYFSA as it relates to the use and disclosure of PHI and PI, respectively.

Principle 4 - Limiting Collection

PinT limits the amount and type of PI and PHI collected to that which is reasonably necessary in order to provide services and for the purposes identified by PinT. PinT will not collect PI or PHI if other information will serve the purpose.

PinT only collects PI and PHI for lawful purposes and takes reasonable steps to ensure that PI and PHI is not collected without authority.

Principle 5 - Limiting Use, Disclosure and Retention

PI and PHI will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as permitted or required by law. PinT shall not use or disclose more PHI than is reasonably necessary to meet the purpose.

PI and PHI is retained only for as long as necessary for the fulfillment of the purpose of the information, subject to legislative retention periods and organizational need.

PI and PHI that is no longer required to fulfill the identified purpose will be destroyed, erased, or made anonymous in a secure manner.

Principle 6 - Ensuring Accuracy

PinT takes reasonable steps to ensure that PI and PHI is as accurate, complete, and up to date as is necessary for the purposes for which it uses the information. Limitations on the accuracy and completeness of PI and PHI disclosed will be clearly set out for the recipient where possible.

When an individual successfully demonstrates the inaccuracy or incompleteness of PI or PHI, PinT will amend the information as required. Depending on the nature of the information, amendment may involve the correction to the record, or addition of information. Where appropriate, the amended information will be transmitted to any third parties that have been provided access to the information in question. When a correction request is not resolved to the satisfaction of the individual, the individual may provide a statement of disagreement which will be filed on the client record.

Principle 7 - Ensuring Safeguards

PinT protects PHI and PHI with security safeguards appropriate to the sensitivity of the information.

- Security safeguards are used to protect PI and PHI against loss or theft as well as unauthorized access, disclosure, copying, use, or modification. PinT protects PI and PHI regardless of the format and ensures that records of PI and PHI are retained, transferred and disposed of in a secure manner.
- The nature of safeguards 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.
- The methods of protection may include:
    - Physical security, for example, secure locks on filing cabinets and restricted access to offices
    - Organizational security, for example, confidentiality agreements and limiting access to PI and PHI to those who are authorized to use or handle such information in order to perform their current job duties (i.e. on a "need-to-know" basis).
    - Technological security, for example, requirement for strong passwords, password access, personal identification numbers and use of strong encryption
- PinT notifies the individual at the first reasonable opportunity if PI or PHI in its custody or control has been stolen, lost or if it is used or disclosed without authority, and complies with legislative reporting requirements, as applicable.

<u>Website and Electronic Commerce</u>

- PinT does not automatically gather PI such as client name, phone number, e-mail or address through its website. This information is only obtained if it is supplied voluntarily, through contacting us via e-mail, or by asking to receive electronic newsletters or other information;
- Any PI provided to PinT will not be sold to any third party;
- PinT uses software that receives and records the Internet Protocol (IP) address of the computer that has contacted our website. PinT makes no attempt to link these addresses with the identity of individuals contacting our site.
- The information is used to improve the content of and/or measure the level of interest in our site and is not shared with other organizations;
- Whenever we enable "cookies" to facilitate our transactions, we will first inform the client;
- If individuals choose to participate in an online forum or discussion group, we may ask that they volunteer PI such as name and e-mail address for the purposes of effective administration of the forum or discussion group; and
- We will not disclose PI to anyone outside of PinT without prior consent.

Principle 8 - Openness

PinT is transparent about its information practices and makes information about its policies and practices relating to the management of PI and PHI readily available to individuals. The information is made available in a manner that is accessible and easy to understand.

Principle 9 - Individual Access

Individuals have the right to access their own record of PI or PHI, subject to limited exceptions. An individual may make a request for access in writing and must provide sufficient detail to identify and locate the record with reasonable efforts. Where access has been granted, the individual may challenge the accuracy and completeness of the information and have it amended, as appropriate.

In certain situations, PinT may not be able to provide access to all PI and PHI it holds about an individual. Exceptions to access requirements will be in accordance with the law. The reasons for denying access will be provided to the individual, and they will be notified of the right to challenge this decision.

PinT will respond to the individual's access request within 30 days, subject to the ability to extend the deadline in accordance with privacy law.

Principle 10 - Challenging Compliance

Individuals may challenge our compliance with this policy. We have policies and procedures to receive, investigate, and respond to complaints and questions. Individuals may direct their questions to the PinT Privacy Officer who will:

- Receive and respond to complaints or inquiries about PinT policies and practices related to the handling of PI or PHI.
- Inform individuals who make inquiries or complaints of the existence of relevant complaint procedures.
- Investigate all complaints. If a complaint is found to be justified, PinT shall take appropriate measures, including, if necessary, amending its policies and practices.

Individuals may also make a complaint to the Information and Privacy Commissioner/Ontario at 2 Bloor St., E., Suite 1400, Toronto, Ontario M4W 1A8 or www.ipc.on.ca, or commissioner@ipc.on.ca .