Confidentiality Policy

Oftentimes, during conducting business as an organization, Unicamp has access to personal and private information about campers, staff members, volunteers, event renters, etc. Unicamp of Ontario wants to ensure that this information is well-protected.

Definition of Personal data: 'Personal information' is defined slightly differently under Ontario and federal Canadian privacy laws, but generally means information about an identifiable individual (in some statutes, specified as recorded information). Examples include race, ethnicity, age, sex, family status, criminal or employment history, address, telephone numbers, and opinions of the individual.

Private Information must be protected because it may be:

- Legally binding (e.g. sensitive customer data.)
- Personal or sensitive information
- Constitute information about business processes and charitable organization procedures that may be under review to ensure compliance

Unicamp Data Security
The confidential information employees use every day must be protected from disclosure to those who could misuse it. Whether staff members work with paper records, at a computer terminal, or spend most of their day on the phone, employees are part of the Unicamp's information security systems.

Confidentiality Measures

Unicamp of Ontario will take measures to ensure that confidential information is well protected. We'll:

- Store and lock paper documents
- Shred paper documents after the prescribed length of time
- Safeguard electronic information
- Keep records of staff authorization to access certain confidential information

End of Employment: When staff members / volunteers leave Unicamp of Ontario, they're obliged to return any confidential files and delete them from their personal devices. The password for electronically stored files is to be changed when a Camp Director or Executive Director leaves their role.

We should never:

- Use confidential information for any personal benefit or profit
- Disclose confidential information to anyone outside of our organization
- Replicate confidential documents and files and store them on insecure devices

There are many facets to Unicamp's organization. Unicamp's protocols apply to all groups and individuals involved.

- Governance: Members, Delegates, Board Members
- Staff: Senior Staff, Middle Management, Junior Staff, Volunteers
- Campers: Seasonal and Occasional Campers, Children in Childcare, Program Participants
- Children's and Youth Programming: Kid's Campers, LITs, CITs, Jouth, Junior Volunteers
- Adult Programming: Facilitators, Participants
- Events: Event Renters, Participants

Onsite Incidents (Governance, Staff, Campers, Children's Programming, Events)

- Incident reports are to be stored electronically in a password protected folder accessible to the Camp Director and Executive Director.
- When collecting information for the incident report, all notes to be stored electronically in a password protected folder **or** (if a hard copy) locked in the Administration Building onsite.
- All incidents and accidents are to be reported, if required by law, contract, or regulation, to the Children's Aid Society (see Policy on Providing a Safe Environment and Child Protection) and/or Public Health and/or the Insuring Organization.
- Incident reports may be shared with the Ministry of Labour, Immigration, Training and Skills Development and Unicamp's Health and Safety Representative or Committee (when applicable) if staff members have been injured.
- Incident reports may be shared with staff within the organization if required for the express purposes of maintaining or improving the health and safety of persons at camp, camp property, or Unicamp as an organization.

- Incident reports may be shared, if required, with our Insuring Organization for the purpose addressing legal or insurance matters.
- Incident reports may be shared with the Board of Directors should that be required to maintain the safe operation of Unicamp or to address a concern brought to the board if the sharing of the report does not jeopardize our duty to maintain confidentiality.
- Incident reports are not to be shared via email or stored outside a password protected electronic Incident Report folder.
- The Camp Director and Executive Director are responsible for these reports and for sharing them in a manner which maintains the security and confidentiality of the information therein.
- Incident reports are to be kept indefinitely.

Accommodation Requests (Staff, Campers, Children's and Youth Programming)

- Completed accommodation (accessibility) requests are to be stored electronically in a password-protected folder.
- The Camp Director and Executive Director are those with access to this folder and its contents.
- Accommodation requests may be shared with staff within the organization if required for the express purposes of maintaining or improving the health and safety of persons at camp, camp property, or Unicamp as an organization.
- Accommodation Requests are to be stored for three years unless another request is made by the same individual that supersedes the first.

Unicamp Staff Personal Data

- Unicamp of Ontario establishes a personnel file for each employee that includes information relevant to their employment.
- The personnel file may include such information as the employee's name and address, date of birth (if a student and under 18 years of age), date of hire, hours worked, pay periods, gross and net salary, deductions, vacation, leaves of absence, termination date, job application, resume, records of training, documentation of performance appraisals and salary increases, and other records required to maintain the employment relationship.
- All employees are entitled to access personal information collected about them in the course of their employment.
- Employees may not add anything to or remove anything from their personnel file. If an employee believes that personal information in his/her file is inaccurate, they may request a correction.
- Personnel files are the property of Unicamp of Ontario and access will be restricted to authorized individuals within the organization (Executive Director, Camp Director, and Administrator performing payroll).

Consent: Individuals must provide informed consent when Unicamp acquires their personal information.

Right to information: Individuals have the right to access personal information held by Unicamp, challenge its accuracy, and have it amended as appropriate.

Unicamp must obtain the knowledge and consent of the individual for the collection, use, or disclosure of personal information, except where inappropriate. Some situations where consent might be inappropriate include legal, medical, or security reasons that make it impractical to seek consent, obtaining personal information for fraud or law enforcement purposes, or where the individual lacks mental capacity. Individuals under PIPEDA also have the right to access personal information held by an organization, challenge its accuracy, and have it amended as appropriate.

5.2. Contract with the data subject

To comply with identifying purposes requirements under PIPEDA, organisations are to identify and document why personal information that is needed and notify individuals of the purposes for collection. Under the consent principle, organisations are to obtain the knowledge and consent of the individual for the collection, use, or disclosure of personal information, except where inappropriate. Under the limiting collection principle, organisations are not to collect personal information indiscriminately or deceive individuals about the reasons for collection.

5.3. Legal obligations

Ontario's privacy legislation does not explicitly provide for the concept of a 'data controller.' Instead, the legislation governs how institutions and regulated entities can collect, use, and disclose personal information. Under FIPPA and the MFIPPA, no person can collect personal information on behalf of an institution unless the collection is expressly authorised by statute, used for law enforcement purposes, or necessary to the proper administration of a lawfully authorised activity. Personal information must be collected directly from the individual, except in limited circumstances. Notice must be provided to individuals when personal information is collected on behalf of the institution, informing the individual of the legal authority for the collection, principal use for the information, and contact information of a public official who can answer the individual's questions about the collection.

Personal information that is collected under FIPPA and the MFIPPA can only be used or disclosed for the purposes for which it was collected, subject to certain circumstances, for example with the individual's consent, for the purpose of complying with other laws, and compassionate circumstances. Institutions must ensure that personal information records are accurate and retain personal information for at least one year after its use, subject to certain

exceptions. Institutions must also ensure the security and confidentiality of personal information records and the transfer and destruction of personal information must also meet security requirements.

Under PHIPA, HICs are generally required to obtain an individual's consent to collect, use, or disclose personal health information, unless PHIPA allows otherwise. A HIC must ensure that personal health information is accurate and protected against theft, loss, and unauthorised use and disclosure. In addition, HICs must ensure that records of personal health information are transferred and disposed of in a secure manner. Notably, the Fiscal Act creates a new obligation for HICs that use electronic means to collect, use, disclose, modify, retain, or dispose of personal health information to maintain, audit, and monitor an electronic audit log (Section 10.1 of PHIPA). In addition, section 34 of PHIPA is also amended to allow prescribed persons, and health information custodians that are providing health care to a person, to collect or use the person's health number, with the person's consent, for certain verification and linking purposes. Section 39, is amended to permit the disclosure of personal health information for purposes related to the Immunization of School Pupils Act 2017.

Part X of the CYFSA requires service providers to have an individual's consent to collect, use, or disclose personal information unless otherwise authorised. Service providers have to ensure that the personal information is accurate and take reasonable steps to protect personal information in their custody or control against theft, loss, or unauthorised collection, use, or disclosure.

Regulations under PIPEDA provide that consent is not required for the collection, use, and disclosure of certain publicly available information, e.g. published information and court decisions, although some restrictions apply. In general terms, for the exemption to apply, the collection, use, or disclosure must be related to the purpose for which the information is publicly available.

Employment

Canadian privacy statutes governing the private sector generally allow for the collection, use, and disclosure of employee personal information without consent if solely for the purposes reasonably required to establish, manage, or terminate an employment relationship between the organisation and that individual.

While the statutes allow for the collection of personal information without consent within the bounds of reasonableness, they nonetheless require the employer to be transparent. Accordingly, organisations must generally notify employees that such data collection is occurring and explain the purpose(s) for the collection (such as employee safety).

In addition to the data protection statutes that can apply to employee personal information, workplace privacy issues have long been addressed in the labour and employment context by

arbitrators and the courts. A significant body of law has been built up in that context in respect of privacy-based limitations on management rights, for example drug and alcohol testing, workplace surveillance, and investigations.

6. PRINCIPLES

Schedule 1 of PIPEDA provides a code that organisations must follow for the protection of personal information. The code consists of 10 principles for the protection of personal information, which are as follows:

- accountability;
- identifying purposes;
- consent;
- limiting collection;
- limiting use, disclosure, and retention;
- accuracy;
- safeguards;
- openness;
- individual access; and
- challenging compliance.

When an organisation transfers personal information to a third party service provider who acts on behalf of the transferring organisation, the transferring organisation remains accountable for the protection of that personal information and ensuring compliance with the applicable legislation. In particular, the transferring organisation is responsible for ensuring that the third party service provider appropriately safeguards the data, and would also be required under the notice and openness/transparency provisions to reference the use of third party service providers in and outside of Canada in their privacy policies and procedures.

Canada has, through PIPEDA, chosen an organisation-to-organisation approach that is not based on the concept of adequacy. PIPEDA does not prohibit organisations in Canada from transferring personal information to an organisation in another jurisdiction for processing. However, under PIPEDA, organisations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement. The OPC can investigate complaints and audit the personal information handling practices of organisations.

To comply with accountability requirements under PIPEDA, organisations are required to appoint an individual responsible for the organisation's compliance with PIPEDA and develop personal information policies and practices. Further, under the accountability principle, an organisation is responsible for personal information in its possession or custody, including

information that has been transferred to a third party for processing. However, a data controller is not explicitly defined in PIPEDA.

However, FIPPA and the MFIPPA use the term 'head,' which refers to the official at an institution accountable and responsible for overseeing the administration of the privacy laws, ensuring compliance with the privacy laws, and making decisions regarding the privacy laws. Under FIPPA, the head for Ontario ministries is the Minister presiding over the ministry, the chair of the board of the hospital for public hospitals, the superintendent for private hospitals, and the person designated in the regulations for other institutions. Under the MFIPPA, institutions can designate a head by by-law or in writing as applicable. Under both FIPPA and the MFIPPA, the head of an institution can delegate its powers or duties to another officer of the institution in writing.

Furthermore, HICs under PHIPA that are not natural persons are to designate a contact person who will, among other things, facilitate the custodian's compliance with PHIPA, respond to public inquiries about the custodian's information practices, and respond to requests from individuals to access or correct personal health information.

Under the accountability principle in PIPEDA, organisations are to designate an individual to be accountable for the organisation's compliance with PIPEDA.

privacy breaches may occur when personal information is collected, retained, used, disclosed, or disposed of in ways that do not comply with the legislation. Individuals may make complaints to the OIPC about privacy breaches. Institutions can also self-report privacy breaches and incidents to the OIPC, but it is not required under FIPPA or the MFIPPA. However, institutions are encouraged to alert appropriate staff, contain the breach, notify those affected by the breach, investigate the breach, and notify the OIPC of significant breaches. The OIPC can investigate privacy breaches formally or informally.

However, there is mandatory reporting of privacy breaches under the CYFSA and PHIPA. Under PHIPA, a HIC is required to notify the OIPC of a privacy breach in prescribed circumstances, which include the use or disclosure without authority, stolen information, a pattern of similar breaches, disciplinary action for breaches, and significant breaches. Further, HICs are required to submit annual reports to the OIPC setting out the number of times personal health information was stolen, lost, used without authority, and disclosed without authority in the previous calendar year.

Under the CYFSA, service providers are required to notify the OIPC of privacy breaches under certain circumstances, including the use or disclosure without authority, stolen information, a pattern of similar breaches, breaches that lead to disciplinary action against an employee, and significant breaches. Similar to PHIPA, service providers under the CYFSA must submit annual reports to the OIPC setting out the number of times personal information was stolen, lost, used

without authority, disclosed without authority, and used in a manner outside the scope of its information practices.

Organisations under PIPEDA are required to report breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals to the OPC. Organisations are also required to notify individuals about those breaches and keep records of those breaches for a period of at least 24 months. A breach of a security safeguard is defined as the loss of, unauthorised access to, or unauthorised disclosure of personal information resulting from a breach of the organisations' security safeguards or from a failure to establish safeguards. Significant harm includes but is not limited to bodily harm, humiliation, damage to reputation, financial loss, and identity theft. Section 10(1) of PIPEDA provides that the factors relevant to determining whether a security breach creates a real risk of significant harm includes the sensitivity of the personal information, the probability of misuse of the personal information, and any other prescribed factor.

7.7. Data retention

To limit use, disclosure, and retention under PIPEDA, organisations are to only disclose personal information for the purpose for which it was collected (unless the individual consents), keep personal information for a reasonable time to allow the individual to access it but only as long as needed, and destroy information that is no longer required for an identified purpose or legal requirement. Under the accuracy principle, organisations are to minimise the possibility of using incorrect personal information. Under the safeguard principle, organisations are to protect personal information against loss or theft and safeguard it against unauthorised access or disclosure.

Data Retention for Employee Information:

- Records of each employee’s name, address and employment start date must be kept for three years after the employee ceases to be employed by the organization
- The date of birth of any students under 18 must be recorded and kept until they turn 21 or for three years after he/she ceases to be employed by the organization, whichever happens first
- All documents relating to an employee’s leave (including pregnancy, family medical, personal emergency, declared emergency, reservist or organ donor leave) must be kept for three years after the day the leave expired

- If you employ homeworkers, you must keep a register showing each homeworker’s name, address and wage rate. This information can be deleted from the register three years after the homeworker ceases to be employed by you

7.8. Children's data

While there are no regulations related to the processing of children's data and age of consent, the OPC has identified the following tips for services aimed to children and youth:

- limit, or avoid altogether, the collection of personal information;
- be careful about 'inadvertent' collection;
- have an appropriate retention schedule for inactive accounts;
- speak to the specific services being provided to youth;
- make sure users can understand the ask, or know, to engage their parents/guardians;
- consider the user experience;
- make clear who is agreeing to terms and conditions;
- ensure there are proper defaults for the age of users;
- know what is happening on the organisation's own website; and
- prevention is preferable to monitoring.

DATA SUBJECT RIGHTS

8.1. Right to be informed

As noted above, individuals generally must be given notice under FIPPA and the MFIPPA when an institution subject to FIPPA or the MFIPPA collects personal information.

8.2. Right to access

Individuals also have the right under FIPPA and the MFIPPA to access any personal information about themselves that is in the custody or under the control of an applicable institution or any other personal information about themselves that is reasonably retrievable by the institution.

8.3. Right to rectification

Individuals who are given access to their personal information can request correction of errors or omissions, request that a statement of disagreement be attached to information reflecting corrections that were requested but not made, and require that any person to whom the

information has been disclosed within the year before a correction is requested or a statement of disagreement is required be notified of the correction or statement of disagreement.

8.4. Right to erasure

Canada has yet to recognise 'a right to be forgotten' or to enact erasure laws. However, injured parties can use the complaint procedure under PIPEDA.

8.5. Right to object/opt-out

Not applicable.

8.6. Right to data portability

Not applicable.

8.7. Right not to be subject to automated decision-making

Not applicable.

8.8. Other rights

Individuals can make complaints to the OIPC when they believe that an institution has not complied with the privacy rules on personal information. Individuals are encouraged to first resolve the complaint with the institution directly, but they can file a complaint with the OIPC if they believe the institution has not adequately addressed their concerns. The OIPC will investigate and encourage settlement or adjudicate as appropriate and necessary.

- INTRODUCTION
- +1. GOVERNING TEXTS
- +2. SCOPE OF APPLICATION
- +3. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY
- 4. KEY DEFINITIONS
- +5. LEGAL BASES
- 6. PRINCIPLES
- +7. CONTROLLER AND PROCESSOR OBLIGATIONS
- +8. DATA SUBJECT RIGHTS

Part X of the Child, Youth and Family Services Act, 2017, S.O. 2017, c. 14, Sched. 1 ('CYFSA').
Collection, use and disclosure of personal information — requirement for consent
286 A service provider shall not collect personal information about an individual for the purpose of providing a service or use or disclose that information unless,

(a) the service provider has the individual's consent under this Act and the collection, use or disclosure, to the best of the service provider's knowledge, is necessary for a lawful purpose; or

(b) the collection, use or disclosure without the individual's consent is permitted or required by this Act.

Collection, use and disclosure of information other than personal information

287 (1) A service provider shall not collect personal information for the purposes of providing a service or use or disclose that personal information if other information will serve the purpose of the collection, use or disclosure.

Collection, use and disclosure of personal information limited to what is reasonably necessary

(2) For the purposes of providing a service, a service provider shall not collect, use or disclose more personal information than is reasonably necessary to provide the service.

Exception

(3) This section does not apply to personal information that a service provider is required by law to collect, use or disclose.

Indirect collection of personal information

With consent

288 (1) A service provider may collect personal information indirectly for the purpose of providing a service if the individual to whom the information relates consents to the collection being made indirectly.

Without consent

(2) A service provider may collect personal information indirectly for the purpose of providing a service and without the consent of the individual to whom the information relates if,

(a) the information to be collected is reasonably necessary to provide a service or to assess, reduce or eliminate a risk of serious harm to a person or group of persons and it is not reasonably possible to collect personal information directly from the individual,

(i) that can reasonably be relied on as accurate and complete, or

(ii) in a timely manner;

(b) the information is to be collected by a society from another society or from a child welfare authority outside of Ontario and the information is reasonably necessary to assess, reduce or eliminate a risk of harm to a child;

(c) the information is to be collected by a society and the information is reasonably necessary for a prescribed purpose related to a society's functions under subsection 35 (1);

(d) the indirect collection of information is authorized by the Commissioner; or

(e) subject to the requirements and restrictions, if any, that are prescribed, the indirect collection of information is permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada.

Direct collection without consent

289 A service provider may collect personal information directly from the individual to whom the information relates, even if the individual is not capable, if,

(a) the collection is reasonably necessary for the provision of a service and it is not reasonably possible to obtain consent in a timely manner;

(b) the collection is reasonably necessary to assess, reduce or eliminate a risk of serious harm to a person or group of persons; or

(c) the service provider is a society and the information is reasonably necessary to assess, reduce or eliminate a risk of harm to a child.

Notice to individual re use or disclosure of information

290 Where a service provider collects personal information directly from an individual, the service provider shall give the individual notice that the information may be used or disclosed in accordance with this Part.

Permitted use

291 (1) A service provider may use personal information collected for the purpose of providing a service,

(a) for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose, including providing the information to an officer, employee, consultant or agent of the service provider, but not if the information was collected with the consent of the individual or under clause 288 (2) (a) and the individual expressly instructs otherwise;

(b) if the service provider believes on reasonable grounds that the use is reasonably necessary to assess, reduce or eliminate a risk of serious harm to a person or group of persons;

(c) for a purpose for which this Act, another Act or an Act of Canada permits or requires a person to disclose it to the service provider;

(d) for planning, managing or delivering services that the service provider provides or funds, in whole or in part, allocating resources to any of them, evaluating or monitoring any of them or detecting, monitoring or preventing fraud or any unauthorized receipt of services or benefits related to any of them;

(e) for the purpose of risk management and error management activities;

(f) for the purpose of activities to improve or maintain the quality of a service;

(g) for the purpose of disposing of the information or modifying the information in order to conceal the identity of the individual;

(h) for the purpose of seeking the individual's consent, or the consent of the individual's substitute-decision maker, when the personal information used by the service provider for this purpose is limited to the name and contact information of the individual and the name and contact information of the substitute decision-maker, where applicable;

(i) for the purpose of a proceeding or contemplated proceeding in which the service provider or an officer, employee, agent or former officer, employee or agent of the service provider is, or is expected to be, a party or witness, if the information relates to or is a matter in issue in the proceeding or contemplated proceeding;

(j) for research conducted by the service provider, subject to the requirements and restrictions, if any, that may be prescribed; or

(k) subject to the requirements and restrictions, if any, that are prescribed, if permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada.

Exception

(2) Despite clause (1) (a), where the individual to whom the personal information relates expressly instructs otherwise,

(a) a society may nonetheless use that personal information,

(i) if it is reasonably necessary to assess, reduce or eliminate a risk of harm to a child, or

(ii) for a prescribed purpose related to a society's functions under subsection 35 (1); and

(b) a service provider may nonetheless use that personal information if it is reasonably necessary to assess, reduce or eliminate a risk of serious harm to a person or group of persons.

Disclosure without consent

292 (1) A service provider may, without the consent of the individual, disclose personal information about an individual that has been collected for the purpose of providing a service,

(a) to a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or to allow the agency to determine whether to undertake such an investigation;

(b) to a proposed litigation guardian or legal representative of the individual for the purpose of having the person appointed as such;

(c) to a litigation guardian or legal representative who is authorized under the Rules of Civil Procedure, or by a court order, to commence, defend or continue a proceeding on behalf of the individual or to represent the individual in a proceeding;

(d) for the purpose of contacting a relative, member of the extended family, friend or potential substitute decision-maker of the individual, if the individual is injured, incapacitated or otherwise not capable;

(e) for the purpose of contacting a relative, member of the extended family or friend of the individual if the individual is deceased;

(f) subject to section 294, for the purpose of complying with,

(i) a summons, order or similar requirement issued in a proceeding by a person having jurisdiction to compel the production of information, or

(ii) a procedural rule that relates to the production of information in a proceeding;

(g) if the service provider 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; or

(h) if permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada, subject to the requirements and restrictions, if any, that are prescribed.

To assess, etc. risk of harm to a child

(2) A society may disclose to another society or to a child welfare authority outside Ontario personal information that has been collected for the purpose of providing a service if the information is reasonably necessary to assess, reduce or eliminate a risk of harm to a child.

For a prescribed purpose related to society's functions

(3) A society may disclose personal information that has been collected for the purpose of providing a service if the information is reasonably necessary for a prescribed purpose related to a society's functions under subsection 35 (1).

Definition

(4) In this section,

"law enforcement" has the same meaning as in subsection 2 (1) of the Freedom of Information and Protection of Privacy Act.

Disclosure for planning and managing services, etc.

Disclosure to prescribed entity

293 (1) A service provider may disclose personal information collected by the service provider under the authority of this Act to a prescribed entity for the purposes of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of services, the allocation of resources to or planning for those services, including their delivery, if the prescribed entity meets the requirements under subsection (5).

Disclosure to other person or entity

(2) A service provider may, subject to the prescribed requirements and restrictions, disclose personal information collected by the service provider under the authority of this Act to a person or entity that is not a prescribed entity for the purposes described in subsection (1) and a person or entity to whom a service provider discloses personal information under this subsection shall comply with any prescribed requirements and restrictions with respect to the use, security, disclosure, return or disposal of the information.

Minister may require disclosure

(3) The Minister may require a service provider to disclose information, including personal information, to a prescribed entity, if the prescribed entity meets the requirements under subsection (5), or to a person or entity that is not a prescribed entity, for the purposes described in subsection (1) and a person or entity, including a prescribed entity, to whom a service provider discloses information under this subsection shall comply with any prescribed requirements and restrictions with respect to the use, security, disclosure, return or disposal of the information.

Exception

(4) Subsections (1), (2) and (3) do not apply to prescribed information in prescribed circumstances.

Requirements for prescribed entity

(5) A service provider may disclose personal information to a prescribed entity under subsection (1) or (3) if,

(a) the prescribed entity has in place practices and procedures to protect the privacy of the individuals whose personal information it receives and to maintain the confidentiality of the information; and

(b) the Commissioner has approved the practices and procedures.

Exception

(6) Despite clause (5) (b), a service provider may disclose personal information to a prescribed entity under subsection (1) or (3) before the first anniversary of the day this section comes into force even if the Commissioner has not approved its practices and procedures.

Review of practices and procedures by Commissioner

(7) The Commissioner shall review the practices and procedures of each prescribed entity every three years after they were first approved and advise the service provider whether the prescribed entity continues to meet the requirements of subsection (5).

Prescribed entity or other person or entity may collect personal information

(8) A prescribed entity or a person or entity that is not a prescribed entity is authorized to collect the personal information that a service provider may disclose to it under subsection (1), (2) or (3).

Use and disclosure of personal information by prescribed entity, other person or entity

(9) Subject to the exceptions and additional requirements, if any, that are prescribed, a prescribed entity or a person or entity that is not a prescribed entity that receives personal information under subsection (1), (2) or (3) shall not use the information except for the purposes for which it received the information and shall not disclose the information except as required by law.

Deemed compliance

(10) For the purpose of clause 42 (1) (e) of the Freedom of Information and Protection of Privacy Act, clause 32 (e) of the Municipal Freedom of Information and Protection of Privacy Act or clause 43 (1) (h) of the Personal Health Information Protection Act, 2004, a disclosure of personal information by an institution or a health information custodian, within the meaning of those Acts, under this section is deemed to be for the purposes of complying with this Act.

Records of mental disorders

Definitions

294 (1) In this section,

"court" includes the Divisional Court; ("tribunal")

"record of a mental disorder" means a record or a part of a record made about an individual concerning a substantial disorder of the individual's emotional processes, thought or cognition which grossly impairs the individual's capacity to make reasoned judgments. ("dossier relatif à un trouble mental")

Disclosure pursuant to summons, etc.

(2) A service provider shall disclose, transmit or permit the examination of a record of a mental disorder pursuant to a summons, order, direction, notice or similar requirement in respect of a

matter in issue or that may be in issue in a court or other body unless a physician states in writing that the physician believes that to do so,

(a) is likely to detrimentally affect the treatment or recovery of the individual to whom the record relates; or

(b) is likely to result in,

(i) injury to the mental condition of another individual, or

(ii) bodily harm to another individual.

Court or body to determine whether to disclose

(3) Where the disclosure, transmittal or examination of a record of a mental disorder is required by a court or body before which a matter is in issue, the court or body shall determine whether the record referred to in the physician's statement should be disclosed, transmitted or examined.

Hearing

(4) Before making a determination under subsection (3), the court or body shall give notice to the physician and, if the court or body holds a hearing to determine whether the record should be disclosed, transmitted or examined, it shall be held in the absence of the public.

Matters to be considered

(5) In making a determination under subsection (3), the court or body shall consider whether or not the disclosure, transmittal or examination of the record of a mental disorder referred to in the physician's statement is likely to have a result described in clause (2) (a) or (b) and, for that purpose, the court or body may examine the record.

Order

(6) The court or body shall not order that the record of a mental disorder referred to in the physician's statement be disclosed, transmitted or examined if the court or body is satisfied that a result described in clause (2) (a) or (b) is likely, unless satisfied that to do so is essential in the interests of justice.

Conflict

(7) Subsections (2) to (6) apply despite anything in the Personal Health Information Protection Act, 2004.

Return of record to service provider

(8) Where a record of a mental disorder is ordered to be disclosed, transmitted or examined under this section, the clerk of the court or body in which it is admitted in evidence or, if not so admitted, the person to whom the record is transmitted, shall return the record to the service provider as soon as possible after the determination of the matter in issue in respect of which the record was required.

Consent

Elements of consent for collection, use and disclosure of personal information

295 (1) If this Act or any other Act requires the consent of an individual to the collection, use or disclosure of personal information by a service provider, the consent,

(a) must be a consent of the individual;

(b) must be knowledgeable;

(c) must relate to the information; and

(d) must not be obtained through deception or coercion.

Implied consent for collection and use

(2) A consent to the collection and use of personal information 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.

Consent may be written or oral

(3) A consent may be written or oral, but an oral consent may be relied on only if the service provider that obtains the consent makes a written record that sets out the following information:

1. The name of the individual who gave the consent.
2. The information to which the consent relates.
3. The manner in which the notice of purposes required by subsection (5) was provided to the individual.

Knowledgeable consent

(4) A consent to the collection, use or disclosure of personal information is knowledgeable if it is reasonable in the circumstances to believe that the individual to whom the information relates knows,

(a) the purposes of the collection, use or disclosure; and

(b) that the individual may give, withhold or withdraw consent.

Notice of purposes

(5) Unless it is not reasonable in the circumstances, an individual is deemed to know the purposes of the collection, use or disclosure of personal information about the individual if the service provider,

(a) posts a notice describing the purposes where it is likely to come to the individual's attention;

(b) makes such a notice readily available to the individual;

(c) gives the individual a copy of such notice; or

(d) otherwise communicates the content of such notice to the individual.

Transition

(6) A consent that an individual gives, before the day that subsection (1) comes into force, to a collection, use or disclosure of personal information is a valid consent if it meets the requirements of this section for consent.

Withdrawal of consent

296 A consent may be withdrawn by the individual who gave the consent by providing notice to the service provider, but the withdrawal of the consent shall not have retroactive effect.

Conditional consent

297 If an individual places a condition on their consent to the collection, use or disclosure of personal information, the condition is not effective to the extent that it purports to prohibit or restrict the making of any record of personal information by a service provider that is required by law or by established standards of professional or institutional practice.

Presumption of consent's validity
298 A service provider that has obtained an individual's consent to the collection, use or disclosure of personal information about the individual or who has received a copy of a document purporting to be a record of the individual's consent, may presume that the consent fulfils the requirements of this Act and that the individual has not withdrawn it, unless it is not reasonable to do so.

Integrity and Protection of Personal Information
Steps to ensure accuracy, etc. of personal information
Personal information used by service provider
306 (1) A service provider that uses personal information for the purpose of providing a service shall take reasonable steps to ensure that the information is as accurate, complete and up-to-date as is necessary for the purposes for which it uses the information.
Personal information disclosed by service provider
(2) A service provider that discloses personal information that has been collected for the purpose of providing a service shall,

(a) take reasonable steps to ensure that the information is as accurate, complete and up-to-date as is necessary for the purposes of the disclosure that are known to the service provider at the time of the disclosure; or

(b) clearly set out for the recipient of the disclosure the limitations, if any, on the accuracy, completeness or up-to-date character of the information.

Record of disclosed personal information
(3) A service provider that discloses personal information that has been collected for the purpose of providing a service shall record the disclosures made under the prescribed provisions in the prescribed manner.
Steps to ensure collection of personal information is authorized
307 A service provider shall take reasonable steps to ensure that personal information is not collected without authority.
Steps to ensure security of personal information
308 (1) A service provider shall take reasonable steps to ensure that personal information that has been collected for the purpose of providing a service and that is in the service provider's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.
Notice of theft, loss, etc. to individual
(2) Subject to any prescribed exceptions and additional requirements, if personal information that has been collected for the purpose of providing a service and that is in a service provider's custody or control is stolen or lost or if it is used or disclosed without authority, the service provider shall,

(a) notify the individual to whom the information relates at the first reasonable opportunity of the theft, loss or unauthorized use or disclosure; and

(b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under section 316.

Notice to Commissioner and Minister

(3) If the circumstances surrounding the theft, loss or unauthorized use or disclosure meet the prescribed requirements, the service provider shall notify the Commissioner and the Minister of the theft, loss or unauthorized use or disclosure.

Handling of records

309 (1) A service provider,

(a) shall take reasonable steps to ensure that the records of personal information collected for the purpose of providing a service that are in its custody or control are retained, transferred and disposed of in a secure manner; and

(b) shall comply with any prescribed requirements in respect of the retention, transfer and disposal of those records.

Retention of records subject to access request

(2) Despite subsection (1), a service provider that has custody or control of personal information that is subject to a request for access under section 312 shall retain the information for as long as necessary to allow the individual to exhaust any recourse under this Act that they may have with respect to the request.

Disclosure to successor

310 (1) A service provider may disclose personal information about an individual to a potential successor of the service provider, for the purpose of allowing the potential successor to assess and evaluate the operations of the service provider, if the potential successor first enters into an agreement with the service provider to keep the information confidential and secure and not to retain any of the information longer than is necessary for the purpose of the assessment or evaluation.

Transfer to successor

(2) A service provider may transfer records of personal information about an individual to the service provider's successor if the service provider makes reasonable efforts to give notice to the individual before transferring the records or, if that is not reasonably possible, as soon as possible after transferring the records.

Definitions

(3) In this section,

"potential successor" and "successor" mean a potential successor or a successor that is a service provider or that will be a service provider if it becomes a successor.

Written public statement by service provider

311 (1) A service provider shall, in a manner that is practical in the circumstances, make available to the public a written statement in plain, easy-to-understand language that,

(a) provides a general description of the service provider's information practices;

(b) describes how to contact the service provider;

(c) describes how an individual may obtain access to or request correction of a record of personal information about the individual that is in the custody or control of the service provider; and

(d) describes how to make a complaint to the service provider and to the Commissioner under this Part.

Use or disclosure contrary to service provider's information practices

(2) If a service provider uses or discloses personal information about an individual, without the individual's consent, in a manner that is outside the scope of the service provider's description of its information practices under clause (1) (a), the service provider shall,

(a) inform the individual of the uses and disclosures at the first reasonable opportunity, unless the individual does not have a right of access under section 312 to a record of the information;

(b) make a note of the uses and disclosures; and

(c) keep the note as part of the record of personal information about the individual that it has in its custody or under its control or in a form that is linked to that record.

Individual's Access to Personal Information

Individual's right of access

312 (1) An individual has a right of access to a record of personal information about the individual that is in a service provider's custody or control and that relates to the provision of a service to the individual unless,

(a) the record or the information in the record is subject to a legal privilege that restricts its disclosure to the individual;

(b) another Act, an Act of Canada or a court order prohibits its disclosure to the individual;

(c) the information in the record was collected or created primarily in anticipation of or for use in a proceeding, and the proceeding, together with all appeals or processes resulting from it, has not been concluded; or

(d) granting the access could reasonably be expected to,

(i) result in a risk of serious harm to the individual or another individual,

(ii) lead to the identification of an individual who was required by law to provide information in the record to the service provider, or

(iii) lead to the identification of an individual who provided information in the record to the service provider explicitly or implicitly in confidence if the service provider considers it appropriate in the circumstances that the identity of the individual be kept confidential.

Right of access to part of record not restricted

(2) Despite subsection (1), an individual has a right of access to that part of a record of personal information about the individual that can reasonably be severed from the part of the record to which the individual does not have a right of access under any of clauses (1) (a) to (d).

Right of access to part of record not dedicated to provision of service

(3) Despite subsection (1), if a record is not a record dedicated primarily to the provision of a service to the individual requesting access, the individual has a right of access only to the personal information about the individual in the record that can reasonably be severed from the record.

Consultation regarding harm

(4) Before deciding to refuse to grant an individual access to a record of personal information under subclause (1) (d) (i), a service provider may consult with a member of the College of Physicians and Surgeons of Ontario, a member of the College of Psychologists of Ontario or a member of the Ontario College of Social Workers and Social Service Workers.

Informal access

(5) Nothing in this Part prevents a service provider from granting an individual access to a record of personal information to which the individual has a right of access, if the individual makes an oral request for access or does not make a request for access under section 313.

Service provider may communicate with individual

(6) Nothing in this Part prevents a service provider from communicating with an individual or the individual's substitute decision-maker with respect to a record of personal information to which the individual has a right of access.

Request for access

313 (1) An individual may exercise a right of access to a record of personal information by making a written request for access to the service provider that has custody or control of the information.

Details required

(2) The request must contain sufficient detail to enable the service provider to identify and locate the record with reasonable efforts.

Service provider must assist individual making request

(3) If the request does not contain sufficient detail to enable the service provider to identify and locate the record with reasonable efforts, the service provider shall offer assistance to the person requesting access in reformulating the request to comply with subsection (2).

Response of service provider

314 (1) A service provider that receives a request from an individual for access to a record of personal information shall,

(a) make the record available to the individual for examination and, at the request of the individual, provide a copy of the record to the individual and if reasonably practical, an explanation of the purpose and nature of the record and any term, code or abbreviation used in the record;

(b) give a written notice to the individual stating that, after a reasonable search, the service provider has concluded that the record does not exist, cannot be found, or is not a record to which this Part applies;

(c) if the service provider refuses the request, in whole or in part, under any provision of this Part other than clause 312 (1) (c) or (d), give a written notice to the individual stating that the

service provider is refusing the request, in whole or in part, providing a reason for the refusal and stating that the individual is entitled to make a complaint about the refusal to the Commissioner under section 316; or

(d) subject to subsection (2), if the service provider refuses the request, in whole or in part, under clause 312 (1) (c) or (d), give a written notice to the individual stating that the individual is entitled to make a complaint about the refusal to the Commissioner under section 316 and that the service provider is refusing,

(i) the request, in whole or in part, while citing which of clauses 312 (1) (c) and (d) apply,

(ii) the request, in whole or in part, under one or both of clauses 312 (1) (c) and (d), while not citing which of those provisions apply, or

(iii) to confirm or deny the existence of any record subject to clauses 312 (1) (c) and (d).

Exception

(2) A service provider shall not act under subclause (1) (d) (i) where doing so would reasonably be expected in the circumstances known to the person making the decision on behalf of the service provider to reveal to the individual, directly or indirectly, information to which the individual does not have a right of access.

Time for response

(3) As soon as possible, but no later than 30 days after receiving the request, the service provider shall, by written notice to the individual, give the response required by subsection (1) or extend the deadline for responding by not more than 90 days if,

(a) responding to the request within 30 days would unreasonably interfere with the operations of the service provider because the information consists of numerous pieces of information or locating the information would necessitate a lengthy search; or

(b) the time required to undertake an assessment under subsection 312 (1) necessary to respond to the request within 30 days after receiving it would make it not reasonably practical to respond within that time.

Extension of time — notice and response

(4) A service provider that extends the time limit under subsection (3) shall,

(a) give the individual written notice of the extension setting out the length of the extension and the reason for it; and

(b) respond as required by subsection (1) as soon as possible but no later than the expiry of the time limit as extended.

Expedited access

(5) Despite subsections (3) and (4), if the individual provides the service provider with evidence satisfactory to the service provider that the individual requires access to the requested record of personal information within a specified time period, the service provider shall respond within that time period if the service provider is reasonably able to do so.

Frivolous or vexatious requests

(6) A service provider that believes on reasonable grounds that a request for access to a record of personal information is frivolous or vexatious or is made in bad faith may refuse to grant the

individual access to the requested record and, in that case, shall provide the individual with a notice that sets out the reasons for the refusal and that states that the individual is entitled to make a complaint about the refusal to the Commissioner under section 316.

Deemed refusal

(7) A service provider that does not respond to a request for access within the time required is deemed to have refused the request.

Right to complain

(8) If the service provider refuses or is deemed to have refused the request, in whole or in part,

(a) the individual is entitled to make a complaint about the refusal to the Commissioner under section 316; and

(b) in the complaint, the burden of proof in respect of the refusal lies on the service provider.

Identity of individual

(9) A service provider shall not make a record of personal information or a part of it available to an individual or provide a copy of it to an individual under clause (1) (a) without first taking reasonable steps to be satisfied as to the individual's identity.

No fee for access

(10) A service provider shall not charge a fee for providing access to a record under this section, except in the prescribed circumstances.

Corrections to Records

Correction to record

Interpretation

315 (1) In this section, a reference to a correction to a record or to correct a record includes the addition of, or adding, information to make the record complete. 2017, c. 14, Sched. 1, s. 315 (1).

Written request

(2) If a service provider has granted an individual access to a record of personal information and if the individual believes that the record is inaccurate or incomplete, the individual may request in writing that the service provider correct the record. 2017, c. 14, Sched. 1, s. 315 (2).

Informal request

(3) If the individual makes an oral request that the service provider correct the record, nothing in this section prevents the service provider from making the requested correction. 2017, c. 14, Sched. 1, s. 315 (3).

Time for response

(4) As soon as possible, but no later than 30 days after receiving a request for a correction under subsection (2), the service provider shall, by written notice to the individual, grant or refuse the individual's request or extend the deadline for responding by not more than 90 days if,

(a) responding to the request within 30 days would unreasonably interfere with the operations of the service provider; or

(b) the time required to undertake the consultations necessary to respond to the request within 30 days would make it not reasonably practical to respond within that time. 2017, c. 14, Sched. 1, s. 315 (4).

Extension of time

(5) A service provider that extends the time limit under subsection (4) shall by written notice to the individual,

(a) set out the length of the extension and the reason for it; and

(b) grant or refuse the individual's request as soon as possible in the circumstances but no later than the expiry of the time limit as extended. 2017, c. 14, Sched. 1, s. 315 (5).

Frivolous or vexatious requests

(6) A service provider that believes on reasonable grounds that a request for a correction is frivolous or vexatious or is made in bad faith may refuse to grant the request and, in that case, shall provide the individual with a notice that sets out the reasons for the refusal and that states that the individual is entitled to make a complaint about the refusal to the Commissioner under section 316. 2017, c. 14, Sched. 1, s. 315 (6).

Deemed refusal

(7) A service provider that does not respond to a request for a correction within the time required is deemed to have refused the request. 2017, c. 14, Sched. 1, s. 315 (7).

Right to complain

(8) If the service provider refuses or is deemed to have refused the request, in whole or in part,

(a) the individual is entitled to make a complaint about the refusal to the Commissioner under section 316; and

(b) in the complaint, the burden of proof in respect of the refusal lies on the service provider. 2017, c. 14, Sched. 1, s. 315 (8).

Duty to correct

(9) The service provider shall grant a request for a correction if the individual demonstrates, to the service provider's satisfaction, that the record is inaccurate or incomplete and gives the service provider the information necessary to enable the service provider to correct the record. 2017, c. 14, Sched. 1, s. 315 (9).

Exceptions

(10) Despite subsection (9), a service provider is not required to correct a record of personal information if,

(a) it consists of a record that was not originally created by the service provider and the service provider does not have sufficient knowledge, expertise or authority to correct the record; or

(b) it consists of a professional opinion or observation that was made in good faith about the individual. 2017, c. 14, Sched. 1, s. 315 (10).

Manner of making the correction

(11) Upon granting a request for a correction, the service provider shall,

(a) make the requested correction by,

(i) recording the correct information in the record and,

(A) striking out the incorrect information in a manner that does not obliterate the record, or

(B) if that is not possible, labelling the information as incorrect, severing the incorrect information from the record, storing it separately from the record and maintaining a link in the record that enables a person to trace the incorrect information, or

(ii) if it is not possible to make the requested correction in the manner set out in subclause (i), ensuring that there is a practical system in place to inform a person who accesses the record that the information in the record is incorrect and to direct the person to the correct information;

(b) give notice to the individual of what has been done under clause (a); and

(c) at the request of the individual, give written notice of the requested correction, to the extent reasonably possible, to the persons to whom the service provider has disclosed the information with respect to which the individual requested the correction of the record, unless the correction cannot reasonably be expected to have an effect on the ongoing provision of services. 2017, c. 14, Sched. 1, s. 315 (11); 2019, c. 15, Sched. 5, s. 3.

Notice of refusal

(12) A notice of refusal under subsection (4) or (5) must give the reasons for the refusal and inform the individual that the individual is entitled to,

(a) prepare a concise statement of disagreement that sets out the correction that the service provider has refused to make;

(b) require that the service provider attach the statement of disagreement as part of the records that it holds of the individual's personal information and disclose the statement of disagreement whenever the service provider discloses information to which the statement relates;

(c) require that the service provider make all reasonable efforts to disclose the statement of disagreement to any person who would have been notified under clause (11) (c) if the service provider had granted the requested correction; and

(d) make a complaint about the refusal to the Commissioner under section 316. 2017, c. 14, Sched. 1, s. 315 (12).

Rights of individual

(13) If a service provider refuses a request for a correction, in whole or in part, or is deemed to have refused the request, the individual is entitled to take any of the actions described in subsection (12). 2017, c. 14, Sched. 1, s. 315 (13).

Service provider's duty

(14) If the individual takes an action described in clause (12) (b) or (c), the service provider shall comply with the requirements described in the applicable clause. 2017, c. 14, Sched. 1, s. 315 (14).

No fee for correction

(15) A service provider shall not charge a fee for correcting a record under this section, or for complying with subsection (14). 2017, c. 14, Sched. 1, s. 315 (15).

Section Amendments with date in force (d/m/y)

2019, c. 15, Sched. 5, s. 3 - 01/01/2020

****Notice of Confidentiality : By submitting this request, the Camper understands the Executive Director and Camp Director will have access to this information. Should any other Unicamp Staff or Board Members need to be informed of this information, the camper will be notified in advance.****

2021 Resort Rules (Schedule A of License of Occupation)

Primrose Park, is a seasonal family campground. Our goal to provide a beautiful, safe and secure environment for all of our campers to enjoy. Our Resort Rules are written in order to achieve this goal.

Privacy

Ontario law prohibits the sharing of any occupant's personal information.

1. **We will not provide any personal information without written permission from the primary occupant on the license of occupation, unless by request by any authority of the law.**

2. **If more than one person will be paying bills or dealing with the office in regards to your site, make sure the office has them listed as occupants of the site.**

3. **Anyone not listed on the contract will not be given any information about the status of accounts, etc.**

Medication Info/Storage:

1. All documentation must be kept in a secure and confidential manner. *Medication Administration Records* are to be kept in an organized binder, locked up with the centralized medication, while an individual is on site (OCA, HC.2.7., 2017).
    1.1. Once a participant or staff member is no longer on site, records should be digitized and kept for the time period recommended by the Canadian Medical Protective Association (CMPA) (OCA, HC.2.7., 2017).
        1.1.1. "The CMPA recommends to its members that they retain their medical records for at least 10 years from the date of last entry or, in the case of minors, 10 years from the time the patient would have reached the age of majority (either age 18 or 19 years)," (OCA, HC.2.7., 2017).

Employee Privacy and Confidentiality of Information

The [COMPANY] takes all reasonable steps to preserve the confidentiality of all personal information it collects to manage its business and maintain the employment relationship

and is dedicated to protecting the personal security and privacy of all employees and customers.

The [COMPANY] may collect the following types of personal information upon commencement of the employment relationship and thereafter to the extent required to administer the employment relationship:

- **Name, date of birth, gender, marital status, beneficiaries, identification numbers including social insurance number and other identifying information;**
- **Background information, including education, training, work history and reference information including results from criminal reference checks;**
- **Contact information, such as personal address and phone numbers, email address and emergency contact information;**
- **Health and medical information**
- **Work history, experience, training and performance information**

This type of information is collected for the purposes including, but not limited to, the administration of payroll, benefits and pension plans, collecting employment equity information in accordance with applicable legislation, adhering to various reporting such as income tax reporting, conducting pre-employment screening and verifying credentials and experience relevant to employment.

Employees are responsible for keeping any information they handle confidential, ensuring it is used only for the purpose for which it was collected and is not disclosed or used. Failure to do so may result in disciplinary action up to and including termination of employment.

Personnel File Access

The Company maintains a personnel file on each employee. The personnel file may include such information as the employee's job application, resume, records of training, documentation of performance appraisals and salary increases, and other records required to maintain the employment relationship.

All employees are entitled to access personal information collected about them in the course of their employment.

Employees may not add anything to or remove anything from their personnel file. If an employee believes that personal information in his/her file is inaccurate, he/she may request a correction.

Personnel files are the property of the Company and access will be restricted to authorized individuals within the Company.

Employees have been entrusted with one of [COMPANY NAME] most valuable assets – information – and they have the responsibility to protect it and to see that it is used only for its intended business purpose. We use information on a daily basis that could be useful to competitors and others who would misuse it.

Confidential information appears in many forms, such as:

- **Computer records**
- **Word processing documents**
- **Letters and memos**
- **Paper reports**
- **Electronic Data Storage**
- **Conversation**

The confidential information employees use every day must be protected from disclosure to competitors and those who would misuse it. Whether employees work with paper records, at a computer terminal, or spend most of their day on the phone, employees are part of the [COMPANY NAME] information security systems.

Employees must always remember these rules when handling confidential information:

- **Do not disclose to anyone outside the [COMPANY NAME] any information relating to the [COMPANY NAME] that has not been disclosed to the public, without appropriate management approval or as required by law, at any time during or after the termination of the employment relationship. This information must not even be shared with other employees unless they have a business need to know about it.**

- **Routinely take precautions to keep confidential information from being disclosed. This includes making sure such information is not displayed on employees' desks or in their work area where it can be seen by anyone. Employees should also avoid transmitting information via a computer or by fax in ways that might make it available to unauthorized people.**

- **Require third-party recipients of restricted Company information to keep such information confidential.**

- **Do not reveal [COMPANY NAME] trade secrets or the trade secrets of a previous Company or accept improperly obtained proprietary information about another Company.**

- **Respect the confidentiality of private information concerning our employees and proprietary information from customers, suppliers and other third parties that comes to our attention under an understanding of confidentiality. We must respect the proprietary nature of such information and not use or disclose it without proper written authority.**

6.2 Abuse of Power in the Event of Verbal, Emotional, Intellectual, Spiritual, Physical, and/or Sexual Abuse

6.2.1 The "Congregational Covenant of Good Relations" (January 2011) of the First Unitarian Church of Victoria, Victoria B.C, contains guidelines regarding respect between people associated with the congregation.

6.2.2 The members of the First Unitarian Church of Victoria, through their Board of Trustees, in consultation and with the approval of the Minister will suggest three trusted people, any one of whom may be approached, to listen to concerns arising as a result of any experience of abusive behavior by people associated with the congregation. These three people will be available in a counselling / consulting capacity for these special conversations. These three people will be invited to be involved.

6.2.3 These appointments will be reviewed by the Board of Trustees on an annual basis before the Annual General Meeting.

6.2.4 Each and every person associated with the First Unitarian Church of Victoria has the right to confidentiality regarding any of these special conversations except under the following conditions:

Page 20

6.2.4.1 If neglect or abuse of a child is suspected

6.2.4.2 If there is a court order to produce documentation (see below.)

6.2.4.3 If there is a signed and witnessed Release and Exchange of Information which states, in part, the understanding "that any information will not be sent through "public" communication corridors (for example: cordless phone, cell phone, FAX, email, etc.) The requested information will be relayed by private "ear to ear" telephone conversation (for example, not on "speaker" phone); and/or by letter correspondence sent by Canada Post designated PRIVATE AND CONFIDENTIAL.

6.2.4.4 This correspondence is not to be available to others, except to the named person(s) and if necessary her/his appointed staff in the course of carrying out their assigned duties relating to the situation and is considered null and void 30 days from the witnessed date of signing.

6.2.5 Formal written notation describing the situation(s) will be made in collaboration with those involved in the conversations. These notes will be filed in a double-locked secured location determined as safe by the Board of Trustees. These documents will be released only as described in section 6.2.4. Reporting of events will be guided by the Confidentiality exceptions as described in 6.2.

6.5 Human Resources

6.5.1 All relations with staff shall be guided by the following principles:

a) Full conformity with relevant Provincial and Federal legislation on employment including the Employment Standards Act of British Columbia.

b) Fundamental fairness, equity, and natural justice.

c) Fair and equitable wages

d) Respect for confidentiality and privacy where appropriate.

6.7 Records: Security and Disposal
6.7.1 All Church records, including financial statements, correspondence, reports, and committee documents are considered property of the Church and not of any particular member, committee, or office holder.
6.7.2 The Church Administrator, in conjunction with the Treasurer, shall be accountable for the security of all Church records.
6.7.3 Confidential records are only available to

a) President
b) Treasurer
c) Church Administrator
d) Minister
e) Persons specifically identified by the President or the Treasurer.

6.7.4 Church records shall be kept for the following periods:
a) minutes of Board and General Meetings—10 years
b) minutes of Council and Committee Meetings—3 years
c) Church Correspondence—5 years
d) Financial records—7 years.
e) Staff Contracts—7 years

6.7.5 Any destruction of Church records before the time periods defined in Section 6.7.4 have lapsed must be specifically approved by the Board.
6.7.6 When the time periods defined in Section 6.7.4 have lapsed, the Church Administrator shall turn the expired Church records over to the Archives Committee.
6.7.7 Those expired Church records that the Archives Committee does not want shall be destroyed by the Church Administrator in the following manner:

a) Financial records involving members' pledges and contributions, personnel records and contracts, confidential files, and files deemed sensitive by the Church Administrator shall be shredded and sent to paper recycling
b) The remainder shall be sent to paper recycling.

The Charter Review Committee members will continue to uphold the privacy rights of all who participated in the community research (anonymity and confidentiality).

We will not share nor discuss the research findings presented solely to the committee for decision-making purposes. We may discuss these findings with other members of the committee.

Committee members will delete the preliminary reports they received. This refers to any reports of research findings except those made public. Committee members with copies of raw data for verification checks will delete these files and will not share information gained from viewing the raw data that is not in the public reports.

Committee members may share the public reports, in pdf format, with others and speak about the findings and conclusions in the public reports.

When speaking to others about the work to update the charitable purposes, committee members will be mindful of their leadership role and responsibility. This includes conducting ourselves in an ethical and professional way when discussing the work of the committee and the community engagement process and results. We seek to serve as trustworthy caretakers of this knowledge and to act and speak in the best interest of Unicamp about the work of updating the charitable purposes. We may speak candidly with other committee members with the same level of knowledge about the work.

Copies of the raw data and preliminary reports (not released to the public) will be securely stored by the Executive Director for a period of approximately 5 years and the Principal Researcher for a period of approximately 1 year. Secure storage of electronic documents refers to password protection or encryption that prevents anyone but the designated person from access. Secure storage of paper copies refers to a secure locked location that prevents anyone but the designated person from access.

Unicamp Research Data and Retention

The raw data (focus group transcripts and survey responses) do not contain any names or identifying information except for the type of focus group (Board, family camp etc.). The data will be stored securely in accordance with Unicamp's policies for the storage of sensitive information. Copies of the raw data and preliminary reports (not released to the public) will be securely stored by the Executive Director for a period of approximately 5 years and by the Principal Researcher for a period of approximately 1 year. Secure storage of electronic documents refers to password protection or encryption that prevents anyone but the

designated person from access. Secure storage of paper copies refers to a secure locked location that prevents anyone but the designated person from access. Public reports will be accessible from the Unicamp website.

Resource:
https://www.cno.org/globalassets/docs/prac/41069_privacy.pdf

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

https://secureprivacy.ai/blog/what-is-pipeda#:~:text=There%20are%20several%20exemptions%20to,literary%20purposes%2C%20and%20employee%20personal