Policy and Process:	**A - 170 - Privacy Policy – SOLUS**
Effective Date:	August 1, 2018
Approved By:	Chief Operating Officer
Responsibility:	Director of Corporate Services
Review Frequency:	Every four years
Last Review Date:	**January 1, 2025,** May 1, 2023, July 13, 2021, October 15, 2020
Scope:	All Directors, Coordinators, managers, employees, and associates
Authorizing Signature:	

1. POLICY:

SOLUS Support Services (SOLUS) respects the privacy and confidentiality rights of clients and staff and has policies and procedures in place regarding the collection, use, storage and disclosure of personal information and/or personal health information. We are committed to maintaining the privacy, security, and accuracy of the personal and personal health information that we collect, use, and disclose in accordance with applicable legislation. This privacy policy is a statement of principles and guidelines concerning the protection of personal information of our clients, staff and other individuals.

SOLUS Support Services requires written consent from our clients and staff before collecting, using, or disclosing personal information and personal health information. These consents specifically state with whom the information and the type of information that will be shared.

It is expected that all SOLUS staff will adhere to the Privacy Principles outlined in this policy and will maintain professional and ethical standards with respect to the privacy of individuals; and will always use the strictest confidentiality measures regarding information acquired by them through their involvement with SOLUS subject to legal obligations.

All SOLUS staff will sign and uphold the Confidentiality Agreement and act in accordance with this policy, the Code and Rules of Conduct, and all related policies and directives.

Clients may refuse or withdraw consent to certain of the identified purposes at any time by contacting us. If a client refuses or withdraws consent, SOLUS may not be able to provide or to continue to provide certain services.

GUIDING PRIVACY PRINCIPLES:

The following ten privacy principles guide our commitment to your privacy:

SOLUS Support Services Inc. (SOLUS) is committed to protecting the confidentiality of personal information in its custody and control. Anyone who collects, uses, or discloses Personal Information on SOLUS behalf is required to follow these 10 information practices:

Principle 1: Accountability for Personal Information

SOLUS is responsible for the personal and personal health information in its custody or control and has designated an individual to act as its Chief Privacy Officer (CPO). The CPO is accountable for SOLUS's compliance with its Privacy Policy and related legislation.

SOLUS demonstrates its commitment to privacy and the confidentiality of Personal Information by:

- Implementing policies and procedures to protect personal information.
- Educating anyone who collects, uses, or discloses Personal Information on SOLUS's behalf about their responsibilities under SOLUS's privacy policies.
- Implementing policies and procedures through the Privacy Office to:
    - Receive and respond to complaints
    - Field inquiries on privacy related matters, and
    - Make material on SOLUS's privacy policies and procedures available.
- Reviewing this Privacy Policy on an annual basis.

Principle 2: Identifying Purposes for Which Personal Information is Being Collected

SOLUS will identify to the individual from whom it collects Personal Information (and explain as necessary) the purposes for the collection.

SOLUS collects Personal Information for purposes related to direct client service care, administration and management of SOLUS programs and services, client billing, administration, research, teaching, statistical reporting, payroll and as permitted or required by law.

When Personal Information that has been collected is to be used for a purpose not previously identified, the new purpose will be identified. Unless the new purpose is permitted or required by law, consent is required before the information can be used for that purpose.

Principle 3: Consent for the Collection, Use, and Disclosure of Personal Information

Knowledge and consent (express or implied) is required for the collection, use or disclosure of personal information by SOLUS, except as otherwise required or permitted by law.

An individual may withdraw consent at any time, but the withdrawal cannot be retroactive. The withdrawal may also be subject to legal or contractual restrictions and reasonable notice.

Principle 4: Limiting Collection of Personal Information

SOLUS limits the amount and type of personal information it collects to that which is necessary to fulfill the purposes identified. Information is collected directly from the individual unless the law permits or requires collection from third parties.

Principle 5: Limiting Use, Disclosure, and Retention of Personal Information

SOLUS uses and discloses personal information for purposes related to direct client services, administration, research, teaching, statistical reporting, client billing and administration.

Personal information will be retained in accordance with SOLUS policy, and as required by law. Otherwise, it will be destroyed, erased, or made anonymous.

Principle 6: Accuracy of Personal Information

To the extent reasonably possible, personal information will be as accurate, complete, and up to date as is necessary for the purposes for which it is to be used. SOLUS does not routinely update personal information unless this is necessary to fulfill the purposes for which the information was collected.

Principle 7: Safeguards for Personal Information

SOLUS has implemented security safeguards for the personal information it holds, which include:

• Physical measures (such as locked filing cabinets).

• Organizational measures (such as permitting access on a "need-to-know" basis only), and

• Technological measures (such as the use of passwords, encryption, and secure servers).

SOLUS requires anyone who collects, uses, or discloses personal information on its behalf to be aware of the importance of maintaining the confidentiality of personal information. This is done through the signing of confidentiality agreements, privacy training, and contractual means.

SOLUS has taken steps to ensure that the personal information in its custody and control is protected against theft, loss and unauthorized use or disclosure.

Care is used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

Principle 8: Openness About Personal Information Policies and Practices

Information about SOLUS’s policies and practices relating to the management of Personal Information are available, including:

• Contact information for the Chief Privacy Officer, to whom complaints or inquiries can be made.

• the process for obtaining access to Personal Information held by SOLUS and making requests for its correction.

• a description of the type of Personal Information held by SOLUS, including a general account of its use and disclosures.

• a copy of any information that explains SOLUS's privacy policies, standards, or codes.

Principle 9: Individual Access to Personal Information

Individuals may make written requests to have access to their records of personal information, in accordance with SOLUS' policy for access and correction to records. SOLUS will respond to an individual's request within reasonable timelines and costs to the individual, as governed by legislation. SOLUS will take reasonable steps to ensure that the requested information is made available in a form that is understandable. Individuals who demonstrate the inaccuracy or incompleteness of their personal information may request that SOLUS amend their information.

Principle 10: Challenging Compliance with SOLUS's Privacy Policies and Practices

An individual may address a challenge concerning compliance with this policy to the Privacy Officer. SOLUS will receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal information. It will inform individuals who make inquiries or lodge complaints of other available complaint procedures. SOLUS will investigate all complaints. If a complaint is found to be justified, SOLUS will take appropriate measures. For further information about SOLUS complaints process please contact the Privacy Officer, Christine Miranda at, admin@solussupportservices.com.

2. SCOPE:

This policy applies to all paper-based (hard-copy) and electronic collection, use, disclosure and storage and destruction of personal and/or personal health information belonging to individuals and staff of SOLUS.

3. DEFINITIONS:

Confidentiality means the obligation of all staff to keep personal information private. Confidentiality arises during a relationship in which confidential information is shared as part of interactions with an individual in service.

Consent means the knowledge and consent of a person that is required for the collection, use or disclosure of personal information and personal health information about them. For consent to be valid, it must be informed, knowledgeable, must be freely given, and must specifically relate to the information that will be collected, used, or disclosed. This is also referred to as authorization.

Personal Health Information includes medical and health related information as defined under the Personal Health Information Protection Act ("PHIPA").

Personal Information means information about an identifiable individual. It includes but is not limited to name, home address, telephone numbers, email, age, sex, marital or family status, identifying numbers such as social insurance number, driver's license, race, national or ethnic origin, color, religious or political beliefs or associations, educational history, medical history,

disabilities, blood type, employment history, financial history, criminal history, and name, address and phone number of parent(s), guardian, spouse or next of kin.

Privacy means “the right of the individual to control the collection, use and disclosure of information about the individual,” limiting it to “that which is necessary.” The right to privacy applies to written material and verbal communication. Privacy includes having the right to determine what information is collected, how it is used, and the ability to access collected information to review its security and accuracy.

Redact means to remove third party personal information from a record, including but not limited to electronically blacking out and removing identifiable information about a third party such as name, phone number, gender, address, phone number, job title etc.

Staff refers to all SOLUS staff (full-time, part-time, relief and/or on contract), and any person who performs work for SOLUS.

Substitute Decision-Maker (“SDM”) means a legally authorized decision-maker under the Substitute Decisions Act and the Child, Youth Family Services Act where applicable.

4. PRACTICES

4.1: Staff access and use and storage of confidential information:

Sharing of personal information, personal health information, and sensitive information regarding the operations of SOLUS may be essential for accurate assessment, diagnosis, provision of services for SOLUS staff and/or treatment of persons supported by SOLUS. The ethical duty of confidentiality is imposed upon SOLUS to ensure that information obtained while providing services is kept secure and confidential.

All staff who are granted access to Confidential Information must collect, use, disclose and protect the information in a manner that is both compliant with SOLUS’s policies and procedures and relevant privacy legislation.

Confidential Information will be kept in a physical or electronic file which is considered the property of SOLUS, however, the information in the file is the property of the individual.

4.2: Access to information and records by persons supported and/or family or substitute decision maker.

Children/Youth:

A child under the age of 16 receiving supports and services from SOLUS may be denied access to all or part of his/her record if:

- SOLUS is of the opinion that access to the information could reasonably cause the child physical or emotional harm;
- SOLUS is of the opinion that access to the information could reasonably lead to the identification of a person who was required by law to provide the information in the record to SOLUS or a person who provided information to SOLUS explicitly or implicitly

in confidence and SOLUS considers it appropriate to keep the identity of the person confidential;
- The information does not primarily relate to the provision of service to the person supported;
- The information was obtained in anticipation of a legal proceeding and such proceeding has not yet concluded or is otherwise subject to legal privilege.

The parent, guardian, or Substitute Decision-Maker of a child under the age of 16 may identify specific information in the child's records relating to the parent/guardian that cannot be disclosed to the child, unless disclosure is required by law.

Adult:

An adult receiving supports and services from SOLUS may be denied access to all or part of his/her record if:
• SOLUS is of the opinion that access to the information could reasonably be expected to threaten the life or well-being of another individual;
• SOLUS is of the opinion that access to the information could reasonably compromise the availability or accuracy of the information, and the information was collected for the purposes of conducting an investigation with respect to a breach of agreement or law;
• The information is subject to legal privilege or was generated in the course of a formal dispute resolution process.

4.3: Consent for use of information pertaining to persons supported:

Staff must obtain consent from persons in service or someone on their behalf before collecting, using, or disclosing personal information or personal health information about an individual, except as otherwise required or permitted by law.

An individual in service who is 18 years of age or older may identify in their Individual Support Plan what kind of information may be shared and with whom or they may choose to provide consent on an as needed basis.

Consent to disclose information about a child or youth under the age of 16 must come from the parent, guardian, or substitute decision-maker.

A person supported may withdraw consent at any time

SOLUS may collect and/or use personal information and personal health information without consent when:

a) it is in the person’s best interest to their health and safety and consent cannot be obtained in a timely manner;
b) there is a risk to the life, health and safety of a person or group of people;
c) information is required for the purposes of law enforcement;
d) information was provided in the course of employment; and
e) the accuracy of the information must be preserved

4.4: Disclosure or Release of Information to a Third Party:

Written consent is required prior to the release of any information to a third-party (i.e., a party outside of SOLUS). An individual supported, parent, guardian or Substitute-Decision Maker must complete the applicable Consent to Release Information form, which must be reviewed by SOLUS Support Services Director and Privacy Officer prior to the release of the information to ensure that information has been appropriately redacted and will be securely transmitted.

SOLUS may disclose personal information and personal health information of people supported without their consent when:

a) There is a risk to the life, health and safety of a person or group of people;
b) information is required for the purposes of law enforcement, including but not limited to complying with a court order or other decision-making body with the appropriate jurisdiction;
c) information is being disclosed to SOLUS's legal counsel;
d) information is being shared between SOLUS employees about persons receiving supports and services. However, such information should be restricted to employees with a "need to know" and will be communicated via secure methods, for example, using password protected files, redacting identifying information in documents sent.
e) information is being shared for the provision of health care such as to a public hospital where the individual is being treated, an attending physician or dentist, or the coroner or medical examiner

4.5 Privacy and Confidentiality Training

As part of onboarding, new SOLUS staff will receive orientation to SOLUS policies and procedures respecting privacy, confidentiality and consent to collection, use and disclosure of personal information, including data security and management practices. This policy is reviewed annually by all staff.

4.6 Breach of Privacy or Confidentiality

Any suspected of actual unauthorized collection, use or disclosure of Confidential Information should be reported immediately to a Coordinator/Manager/Director and SOLUS's Privacy Officer at admin@solussupportservices.com –with the subject – PRIVACY CONCERN.

5. RELATED LEGISLATION:

Personal Health Information Protection Act 2004 SO 2004 c. 3 Sched A

Personal Information Protection and Electronic Documents Act SC 2000 c.5

Services and Supports to Promote the Social Inclusion of Persons with Developmental Disabilities Act 2008, SO 2008 c 14

O-Reg 299-10 *Quality Assurance Measures*

Child, Youth and Family Services Act (CYFSA), 2017

6. INFORMATION COLLECTED:

6.1: What personal information do we collect?

Canadian privacy legislation defines personal information broadly as information about "an identifiable individual" or as information that allows an individual to be identified. Personal information includes information that relates to their personal characteristics (i.e., gender, age, home address or phone number, ethnic background, family status, language, identifying features, insurance benefit coverage), their health (i.e., health history, health conditions, health services received by them, prognosis or other opinions formed during assessments or treatments, health diagnosis and assessment), or their activities and views (i.e., religion, politics, opinions expressed by an individual, an opinion or evaluation of an individual, criminal history, involvement with the agency). Personal information is to be contrasted with business information (i.e., an individual's business address and telephone number), which is not protected by privacy legislation.

6.2: Who do we collect information on and for what purpose?

Clients
We collect, use, and disclose personal information in order to serve you, our client. We do this in order that we can deliver our rehabilitation support services. Generally, we collect information about the results of client evaluations and assessments, physical condition and function, social and familial situations in order to implement rehabilitation recommendations. In addition, a primary purpose is to seek recommendations from the client's rehabilitation team and to document and report concerns and / or progress as needed.

While it would be rare of us to collect and share such information without, the client's expressed consent, this might occur in an emergency (i.e., the client is unconscious) or where we believe the client would consent if asked and it is impractical to obtain consent (i.e., a family member passing a message on from our client and we have no reason to believe that the message is not genuine) or where consent is implied (i.e., sharing information with a medical professional when attending an appointment with the client). In cases where the client is incapable of consenting (i.e., a child, an incapacitated person), an appropriate substitute will provide the consent (i.e., parent, guardian, spouse, power of attorney).

Families and Friends
In collecting and sharing information related to families and friends of our clients the primary purpose is to provide effective rehabilitation services to the client. This may include seeking recommendations from the client's rehabilitation team and to document and report concerns and / or progress as needed. It would be rare of us to collect such information without the client's express consent, but this might occur in an emergency.

Prospective Clients
For prospective clients, our primary purpose for collecting personal information is to evaluate the availability of services we have and can offer. Consent to collect such information is implied when contact is initiated by the client's rehabilitation team, family and / or the client themselves.

General Public
For members of the general public, our primary purpose for collecting personal information is to make them aware of SOLUS Support Services Inc. We use work contact information where possible, however we might inadvertently collect home addresses, fax number and email addresses. We will upon request immediately remove any personal information from our

distribution list.

On our website we only collect, with the exception of cookies, the personal information you provide and only use that information for the purpose you gave it to us (i.e., to respond to your email message). Cookies are only used to help you navigate our website and are not used in any other way.

Employees, Contract Staff, Service Providers

For employees, contract staff and service providers of SOLUS Support Services Inc., our primary purpose for collecting personal information is for necessary work-related communication (i.e., sending out pay cheques, tax receipts), to monitor work-related performance and for necessary work-related communication. Examples of the type of personal information we collect for those purposes include home addresses and telephone numbers. It is rare for us to collect the information without prior consent, but it may happen in the case of a health emergency or to investigate a possible breach of law (i.e., if a theft were to occur in the office). If employees wish a letter of reference or an evaluation, we will collect information about their work-related performance and provide a report as authorized by them.

Other purposes:

- To invoice clients for goods or services or collect unpaid accounts.

- To advise clients and others of special events or opportunities (i.e., presentations, seminars, programs, new services) that we have available.

- Our agency reviews client and other files for the purpose of ensure that we provide high quality services, including assessing the performance of our staff. In addition, external consultants (i.e., lawyers, accountants, practice consultants) may on our behalf do audits and continuing quality improvement reviews of our agency, including reviewing client files and interviewing our staff.

- As professionals, we will report serious misconduct, incompetence, or incapacity of other rehabilitation team members if necessary. Also, our organization believes that it should report information suggesting serious illegal behaviour to the authorities. External regulators have their own strict privacy obligations. Sometimes these reports include personal information about our client, or other individuals, to support the concern (i.e., improper services). Also, like all organizations, various government agencies (i.e., Information and Privacy Commission, Human Rights Commission, etc.) have the authority to review our files and interview our staff as part of their mandates. In these circumstances, we may consult with professionals (i.e., lawyers, accountants) who will investigate the matter and report back to us.

- Our agency is legally obligated to copy and forward the client's file where a subpoena, warrant or court order has been issued to do so.

- Our agency believes it should report information suggesting self-harm, danger to self or others to the authorities.

- The cost of some goods / services provided by the agency to clients is paid for by third parties (i.e., OHIP, WSIB, private insurance). These third-party payers often have your consent or legislative authority to direct us to collect and disclose to them certain information in order to demonstrate client entitlement to this funding.

• Clients or other individuals we deal with may have questions about our goods or services after they have been received. We also provide ongoing services for many of our clients over a period of months or years, for which our previous records are helpful. We retain our client information for a minimum of ten years after the last contact to enable us to respond to those questions and provide these services.

Website privacy and confidentiality policy

SOLUS places a high value on privacy, both in person and online. SOLUS is committed to maintaining the privacy of all individuals who use www.solusupportservices.com ("the Site"). This Site may contain links to other web sites. Upon entering other sites, you are subject to the privacy and security policies of those sites. This policy identifies the privacy practices of the SOLUS Site only.

No personal information (which means personally identifiable information including, without limitation, your name, street address, telephone number, screen name and e-mail address) about the user is collected from users of this Site unless specifically and clearly requested, and only when the user provides it voluntarily. This Site does not use or collect digital cookies to track visitors.

Personal information that has been provided by users is secure information and is requested to enhance the user's access to information at SOLUS. We only use personal information provided for the express purpose for which it was collected unless the user specifically agrees to the use of the personal information for additional purposes. In order to prevent unauthorized access and ensure proper use of your personal information, we have developed electronic and managerial procedures to secure information provided on-line. In addition, personal information will not be shared with any third party.

SOLUS gathers general trend data concerning traffic on the website for statistical analysis. This information is used for auditing and tracking purposes and to improve the content of the Site. It is not linked to your personal information.

As a user of this Site who has provided personal information to SOLUS, you can have access to your personal information for the purposes of correcting or updating any of your personal information or to delete the personal information you provided on this Site from our records. A contact email address for such purposes will be provided at the points of collection of personal information on this Site.

7. CONTROL OF YOUR PERSONAL INFORMATION:

At SOLUS Support Services Inc., we want you to be able to maintain control over how we use your personal information. In particular:

- You have the right to "opt out" of some or all of the identified purposes, uses and disclosures listed above.

- SOLUS Support Services requires written and verbal consent from our clients before collecting, using, or disclosing personal information. These consents specifically state with whom the information and the type of information that will be shared.

- You may refuse or withdraw your consent to certain of the identified purpose at any time by contacting us. However, if you refuse or withdraw your consent, we may not be able to provide you or to continue to provide you with certain services.

8. WHERE IS YOUR PERSONAL INFMORMATION STORED:

Your personal information is stored in secured locations and on servers controlled by SOLUS Support Services, located either at our offices or at the offices of our service providers. For access to your personal information, please contact our Chief Privacy Officer using the contact information in the "Contact Us" section below.

9. HOW CAN YOU ACCESS YOUR PERSONAL INFORMATION?

Upon written request, subject to certain exceptions, SOLUS Support Services Inc., will inform you of the existence, use, and disclosure of your personal information and will give you access to that information. Access requests should be sent to our Chief Privacy Officer, using the contact information in the "Contact Us" section below.

10. HOW DO WE PROTECT YOUR PERSONAL INFORMATION?

We make every reasonable effort to protect against the loss, misuse, and alteration of personal information under our control. Our security policies are periodically reviewed and enhanced as necessary. We operate secure data networks protected by industry standard firewall and password protection systems. Only authorized employees and suppliers have access to your personal information.

11. CHANGES TO THE PRIVACY POLICY

We reserve the right to modify or supplement the SOLUS Privacy Policy at any time.

12. CONTACT US

SOLUS has appointed a Chief Privacy Officer to oversee compliance with this Privacy Policy and applicable Privacy Laws. You can contact the Chief Privacy Officer, Christine Miranda:
By calling: 416-824-6201
e-mail: admin@solusupportservices.com

ANNUAL DECLARATION:
SOLUS is fully committed to the protection and privacy of information. On an annual basis all associates/employees shall review the Privacy Policy and sign the following declaration:

SOLUS is fully committed to the protection of personal information of our individual clients, individual service providers and other individuals. By signing below, the consultant/employee is confirming that he/she has read and understood and agrees to comply with the SOLUS Privacy Policy.