



SOUTH SHORE
LITERACY
COUNCIL

CONSEIL
DE LITTÉRATIE
DE LA RIVE-SUD

4-279 rue Hubert • Greenfield Park, QC J4V 2W1 • www.southshoreliteracy.org • 450-671-4375

South Shore Literacy Council

Privacy Policy

Policy name	South Shore Literacy Council Protection of Personal Information Policy
Policy number	2024-0125-01
Initially approval by the Board of Directors	25 Jan 2024
To be Updated on	25 Jan 2026
Legal framework	chapter P-39.1 Act Respecting the Protection of Personal Information in the Private Sector

1 Definitions

Personal Information

Any information, regardless of the form or medium used to hold this information, which is about a natural person and allows that person to be identified, directly or indirectly. Personal data may include, among others:

- Racial or ethnic origin
- Political opinions
- Religious or spiritual beliefs
- Trade union membership
- Genetic data
- Health information
- Sexual orientation
- IP Address
- Home address

The Act

The Act refers to chapter P-39.1, the Act Respecting the Protection of Personal Information in the Private Sector and the modifications made to modernize the Act.

Medium Used

Any form used to hold information, whether written, graphic, taped, filmed, computerized, or other.

Members

Any of SSLC's members, as defined in their by-laws.

Employee

An employee is anyone who is remunerated by SSLC on a bi-weekly basis in exchange for achieving specific, pre-identified objectives.

Volunteers

Any person who conducts work on behalf of SSLC or actively supports the achievement of its mission but is not remunerated.

Patrons

In the context of this policy, a patron is any natural person, including employees, volunteers, members, clients, donors, or participants who support SSLC. In addition to those already mentioned, patrons include suppliers, consultants, any person who benefits from activities at SSLC, or who provides services or supplies to SSLC.

Applicants

Any person who is interested in becoming an employee of SSLC and provides personal information through the application process.

Commission

The Commission is the *Commission d'accès à l'information* that oversees the application of the Privacy Act and the Access to Information Act.

2 Policy Elements

Patrons of SSLC are natural persons who have the right to have their personal information protected. This policy outlines SSLC's commitment to protecting personal information while outlining the framework for keeping and destroying said information.

2.1 Objective

The objective of this policy is to comply with the changes to the Privacy Act and ensure SSLC's responsibility in the management of patrons' personal information while allowing them to have better control over the personal information SSLC collects.

This policy defines the roles and responsibilities of SSLC leadership as well as those who collect, access, or otherwise interact with personal information throughout its life cycle at SSLC and provides a process for dealing with complaints regarding the protection of information.

2.2 Scope

All patrons, who are natural persons, who share any amount of personal information with SSLC are protected by the law with which this policy aims to comply. All patrons who access personal information available at SSLC at any point throughout the life cycle of information are bound to respect the elements contained in this policy.

2.3 Roles and Responsibilities

Specific roles and responsibilities are attributed to specific patrons and groups at SSLC, as outlined in the following paragraphs.

2.3.1 Board of Directors

The Board of Directors is responsible for:

- Adopting the present policy and ensuring its implementation.
- Designating the person who is responsible for the protection of personal information, in writing.
- Ensuring appropriate resources are allocated to the designated a Privacy Officer to implement the policy and processes required to protect personal information.

South Shore Literacy Council • 4-279 rue Hubert • Greenfield Park, QC J4V 2W1
www.southshoreliteracy.org • info@southshoreliteracy.org • 450-671-4375

2.3.2 Executive Director

The Executive Director is designated as the Privacy Officer and is responsible for:

- Developing this policy and presenting it to the Board of Directors for approval.
- Approving practices and procedures to ensure the implementation of this policy.
- Preparing an inventory of all personal information held at SSLC, evaluating their level of sensitivity, the purpose for which it was gathered, and who has access to each information.
- Conducting Privacy Impact Assessments (PIA) and suggesting remedial measures.
- Recording Confidentiality Incidents and implementing measures to prevent their reoccurrence.
- Maintaining a registrar of Confidentiality Incidents and sharing it with the Commission when requested.
- Informing the Commission when a Confidentiality Incident presents a serious risk of injury or irreparable damage.
- Responding to requests to access information or requests to make modifications to personal information.
- Receiving and addressing complaints from patrons.
- Destroying personal information as per the parameters of this policy.
- Ensuring privacy information, including the name of the Privacy Officer, are transparently displayed on SSLC' website.

2.3.3 Director of Operations

The Director of Operations is responsible for:

- Knowing, understanding, and respecting the tenets of this policy and all accompanying processes.
- Receiving information from the Privacy Officer to publish on SSLC's website and ensuring it is in simple and plain language.
- Ensure that information about the Privacy Officer is updated every two years.
- Ensuring all patrons sign Confidentiality Agreements.
- Informing the Privacy Officer about client or employee information that is more than five years old.
- Developing consent forms and ensuring they are signed.
- Training new employees on the application of this policy.
- Supporting the Privacy Officer with the inventory of personal information.

2.3.4 Employees

Any employee may, in the course of their employment, collect or access personal information. These employees are responsible for:

- Knowing, understanding, and respecting the tenets of this policy and all accompanying processes.

- Signing a Confidentiality Agreement and adhering to it.
- Ensuring patrons sign consent forms before any personal information is collected.
- Ensuring personal information is kept in a secure location, whether this is a physical or virtual location.
- Accessing and using only the personal information which is necessary to do the job.
- Informing the Privacy Officer about client information that is more than five years old.
- Informing the Privacy Officer of any Confidentiality Incidents and any violations of the tenets of this policy.
- Returning personal information to its secure location after it is consulted.
- Referring patrons who wish to submit a formal complaint.
- Referring patrons who wish to access or modify their personal information.

2.4 Personal Information at SSLC

Any personal information collected by SSLC is to be used only for the purpose for which it was collected and is kept in a secure location.

2.4.1 Client/Participant/Donor/Volunteer Information

Participants, clients, or donors may be asked to provide personal information for the purpose of keeping them informed about SSLC's activities, programs, services, and fundraising campaigns.

2.4.2 Applicant Information

When a potential employee or volunteer submits their curriculum vitae to SSLC they implicitly provide consent to use their personal information to contact them to determine whether or not their candidacy is accepted.

Applicant information may be transferred to employee or volunteer information if the applicant is successful.

2.4.3 Employee Information

Personal information is collected throughout the hiring process. Information is contained in each employee's secure employee file and includes sensitive data. Only the Executive Director and Director of Operations have access to these files.

2.4.4 Consent Forms

Consent forms are written in plain language and provide clear and transparent information about the reason for which consent is obtained. The purpose for collecting personal information must be serious and legitimate and the reason for collecting this information must be defined before consent is obtained and information gathered.

No person will be denied access to services if they do not consent to providing personal information, unless the information is absolutely necessary.

2.4.4.1 For Participants and Clients

The purpose of these forms is to obtain personal information to promote SSLC's activities, programs, and services. The form also explains that information about date of birth may be used to celebrate patrons.

The consent form asks patrons to use pictures and videos taken during these activities to advertise activities and programs on SSLC's website and social media sites. The consent form specifies the length of time SSLC may use these images.

Should patron information be shared with a third party, each patron's prior informed consent is required.

All consent forms are kept in a secure location, alongside personal information collected.

Personal information may only be used for the purpose identified in the consent form and for the period of time indicated on the consent form. Any deviation from the purpose or timeline must be communicated to the person who signed the consent form.

2.4.4.2 Minors

No personal information about a minor under the age of 14 years may be collected without the consent of a parent or guardian.

Any personal information about minors at SSLC is kept in a secure location, within their parent's or guardian's file.

Persons over the age of 14 years may sign their own consent form to authorize SSLC to gather and use their personal information. However, SSLC will request parental consent along with the minor's consent for those aged between 14 and 18 years of age.

2.4.4.3 For Applicants and Employees

SSLC must inform applicants and employees the reason for which personal information is collected.

When SSLC seeks to verify references, the applicant must consent. If a third party is hired to validate references, this information must be shared with the applicant so that informed consent is acquired.

When an applicant becomes an employee, the employee can expect that SSLC will keep their personal information in a secure location. The employee may request to access or modify their personal information.

Employees must be informed of any surveillance tools or biometric information used by SSLC to survey or track employees. Though this currently does not apply at SSLC, employees will be informed if it does change.

2.4.4.4 For Donors

Donors who provide their personal information in the course of making a donation are asked to check a box to consent to be placed on SSLC's mailing list and receive ongoing information.

Those who are on a mailing list must be informed of how they may be removed from such a list. Any donor rescinding consent to receive communications from SSLC must be immediately removed from all mailing lists. All their personal information must be destroyed within the year in which their request is received.

2.4.5 Requesting Access to Personal Information

Any patron may request to access or modify their personal information. SSLC must comply with this request within 30 days of receiving the request.

Any patron may request to transfer or transport their personal information to another service provider.

2.4.6 Rescinding Consent

Any patron may rescind consent at any time. SSLC respects any patron's desire to rescind consent. A request to rescind consent or to request the destruction of personal information may be made orally, electronically, or in writing.

2.4.7 Destroying Personal Information

The Privacy Officer is responsible for maintaining an inventory of personal information held at SSLC and updating it regularly. The inventory may be organized by date of consent to facilitate the destruction of personal information process.

When destroying personal information, the Privacy Officer must ensure the information cannot be reconstituted. The Privacy Officer may shred the information or hire a third party to shred the information securely, after completing a PIA.

The Privacy Officer must adhere to the following guidelines for the destruction of personal information:

- The personal information of patron's who rescind consent must be destroyed within 30 days of receiving the request.
- Personal information belonging to patrons who have not been active for five years may be anonymized for data collection purposes.
- Personal information belonging to patrons who have not been active for five years and is not being anonymized must be destroyed.
- Employee information must be destroyed five years after the last day of employment.
- Applicant files, results of interview questionnaires, and consent to verify references must be destroyed six months after the selection process is completed for applicants who do not become employees.
- When a patron dies, their personal information must be removed from any active mailing lists and may be anonymized immediately.

The process of anonymization ensures that no identifying information is available in a file, but the data accumulated over the years may serve SSLC for research, analysis, or reporting purposes.

2.5 Privacy Impact Assessment

The Privacy Officer must conduct a privacy impact assessment (PIA) before the purchase of any new software, information system or electronic service delivery system involving the collection, use, communication, storage, or destruction of personal information.

The PIA begins with a consultation with the person responsible for the protection of personal information within the company from which the new information system is to be purchased.

The PIA includes:

- A description of the project and software.
- An evaluation of compliance with the protection of personal information.
- An identification and evaluation of the privacy risks.
- A description of the measures to attenuate the risks identified.

In the case that a PIA determines that nominal information must be shared, an agreement between SSLC and the company may be reached. Such an agreement must be sent to the Commission. Contents of the agreement must be in line with article 21.0.2 of the Act.

2.6 Confidentiality Incidents

A confidentiality incident occurs when personal information is:

- Lost or stolen.
- Accessed without authorization.
- Used for purposes other than those for which it was provided, without prior consent or authorization.
- Otherwise impacted and not protected.

The Privacy Officer must identify confidentiality incidents and keep a register of such incidents. The Commission may request a copy of the register at any time.

Each confidentiality incident must be assessed to determine how reoccurrence can be avoided and if it presents a risk of prejudice, of serious injury, or irreparable harm.

The risk of prejudice is assessed by determining:

- The level of sensitivity of the information concerned.
- The possible consequences of the use of the information concerned.
- The likelihood of the information being used in a prejudicial manner.

When a Confidentiality Incident is assessed as a high risk of prejudice, it must be reported to the Commission. When such an incident occurs, the Privacy Officer must also inform the person concerned by the incident.

2.7 Process for Complaints

Complaints may be submitted directly to the Commission.

Information about filing a complaint to SSLC's Privacy Officer should be made available in plain and simple language on SSLC's website.

Should a complaint be filed with SSLC first, the process to address it is for the Privacy Officer to:

- Acknowledge receipt electronically or in writing within seven business days, or as soon as possible.
- Investigate the elements of the complaint diligently or hire a third party to investigate.
- Provide a response to the complainant in writing within 30 days of acknowledging receipt.
- Inform the complainant of their right to file a complaint with the Commission if the outcome of the investigation does not address their issue.

Should the Commission receive a complaint and prescribe a specific course of action, SSLC must comply within 30 days.

3 Consequences

The Commission has the power to impose administrative consequences for any breach to this policy, which is aligned with the law. Administrative fines include:

- Up to \$50,000 for individuals who contravene the law.
- Up to 10,000,000\$ for legal persons (including companies and organizations) who contravene the law, or 2% of gross revenue.

Other penalties may go up to \$100,000 for an individual and up to \$25,000,000, or 4% of gross revenue for legal persons.

The information contained in this policy was published on SSLC's website on: _____