Privacy Management Program

Program Record

Area:	**Operational**
Title:	Privacy Management Program
Date Created:	June 11, 2026
Date Amended:	
Date for Review:	2029
Policy Cross Reference:	**Protection of Privacy Act (POPA) and Access to Information Act (ATIA) Legislation**

Purpose

Strathcona County Library's Privacy Management Program (PMP) outlines the library's privacy procedures, policies, and roles and responsibilities.

Part of the way that a public body fulfills its obligation to protect Personal Information, data derived from Personal Information, and Non-Personal Data in its custody or under its control is to have a privacy management program which is open and transparent. Section 25(1) of the Protection of Privacy Act sets out the requirement for Strathcona County Library to implement a Privacy Management Program (PMP).

Key purposes of a PMP include the following:

- Promote accountability by establishing clear roles, responsibilities, and processes for managing privacy risks.
- Foster trust with Employees, patrons, and partners by demonstrating a commitment to privacy.
- Specify safeguards to protect Personal Information, data derived from Personal and Non-Personal Information.
- Enable risk management tools to identify, assess, and mitigate privacy risks proactively.
- Support organizational objectives by integrating privacy into library operations, enabling innovation while respecting individuals' rights.

Background

On June 11, 2025, Alberta's *Freedom of Information and Protection of Privacy Act* (FOIP) was repealed and replaced with the *Access to Information Act* (ATIA) and the *Protection of Privacy Act* (POPA). The ATIA and POPA apply to public bodies, including government departments, municipalities, libraries, and many more.

ATIA establishes rights for people to access records that are in the custody or control of public bodies subject to limited and specific exceptions.

POPA establishes privacy rights for Albertans concerning Personal Information. It also permits public bodies to Collect, Use or Disclose Personal Information in new ways, including Data Matching and to create Non-Personal Data.

Definitions

Access: When an individual requests access to information or library records—this is a right that individuals have access under ATIA.

Administrative Safeguards: A policy, procedure or practice to manage the library's conduct that protects the privacy of personal information, data derived from personal information and non-personal data.

Applicant: Individual who makes a formal access to information request to an Alberta public body under ATIA.

Artificial Intelligence System: A machine-based system that, for explicit or implicit objectives, infers from the input it receives how to generate outputs (such as predictions, content, recommendations, or decisions) that can influence physical or virtual environments. Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment. (Source: OECD AI Principles, April 2025)

Automated System: An automated system is any system, software, or process that uses computation as a whole or part of a system to determine outcomes, make or aid decisions, inform policy implementation, collect data or observations, or otherwise interact with individuals and/or communities. Automated systems include, but are not limited to, systems derived from machine learning, statistics, or other data processing or artificial intelligence techniques, and exclude passive computing infrastructure. (Source: National Archives (USA), Office of Science and Technology Policy, May 2025).

Business Day: Under the ATIA, a "day" is defined as a "business day". A business day means a day other than a Saturday, Sunday, a holiday, or a day when Government of Alberta offices are closed as part of the Government of Alberta's Christmas closure period.

Collection/Collect: Occurs when a public body gathers, acquires, receives or obtains personal information which may be done through forms, interviews, questionnaires, surveys, polling,

video surveillance, etc. The collection format may be in writing, by audio or video, electronic data entry, via an automated system or other means.

Contractor: A person, partnership or group of people who, through a contract, or an agreement with the library, directs the activities of one or more employers or self-employed people involved at work at a workplace and are not an Employee of Strathcona County Library. **In accordance with POPA, Contractors, Volunteers, and Board Members are considered Employees for the purpose of Privacy obligations and training requirements.*

Cybersecurity: Means protecting electronic devices and electronically stored information. It includes defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks and unauthorized access.

Data derived from Personal Information: Data derived from personal information means data created by data matching and identifies any individual whose personal information was used in data matching. Both elements of the definition need to be met for data to be considered 'data derived from personal information', meaning it must be the merging of two or more sources to create new information about an individual and that the personal information in the data must still be identifiable. *Sections 18 to 20 of the Act did not previously exist under the former FOIP Act and pertain to the retention, use, disclosure, and protection of data derived from personal information.*

Data Matching: Linking personal information between two or more databases or other electronic sources of information. Data matching may only be carried out in accordance with the prescribed security arrangements and public bodies may only collect, use and disclose data derived from data matching in accordance with the Acts (ATIA and POPA) and other regulations.

Disclose/Disclosure: To release, transmit, reveal, expose, show, provide copies of, tell the contents of, or intentionally or unintentionally give personal information by any means to someone. In this context, it includes oral transmission by telephone or in person, provision of Personal Information on paper, by fax or mail and electronic transmission through email, text, messages, data transfer or the internet.

Employee: A person employed by the Strathcona County Library under the terms and conditions of the Library Employee Handbook (HR 01).

Incident Notification: Public bodies must give notice when privacy incidents with a real risk of significant harm occur (RROSH). In those instances, they must give notice, without unreasonable delay, of the incident to the individual to whom there exists a real risk of significant harm, as well as to the Privacy Commissioner, and to the Minister.

Non-Personal Data: Data, including data derived from personal information, that has been generated, modified or anonymized so that it does not identify any individual, and includes synthetic data and any other type of non-personal data identified in the regulations. *Further*

information on the creation and use of non-personal data can be found in section 21(1) of POPA.

Non-Personal Data (continuing information access request): See definition for non-personal data above. A continuing request allows an applicant to receive records concerning a particular subject or issues at **regular intervals** over time **up to 2 years** *(see section 11 of the ATIA).*

Personal Information: Defined under POPA as recorded information about an identifiable individual. *For a complete listing of what is considered Personal Information, please see section 1(q) of POPA*.

Physical Safeguards: Measures to protect the library's physical assets, including electronic information systems, from natural and environmental hazards and unauthorized intrusion**.**

Privacy Incident: A Privacy Incident, as described in section 10(2) of POPA, occurs when personal information – or data derived from personal information – under the custody or control of a public body is lost, accessed or disclosed without authorization, and there is a real risk of significant harm to an individual as a result.

Privacy Officer: The Privacy Officer is the designated library employee that handles the day-to-day operations of POPA and is responsible for the public body's compliance with the Act.

Record: Refers to a document or log that exists at the time a request for access is made or that is routinely generated by a public body that can be any format or combination of texts, graphics, data, audio, pictorial or other information represented in a digital form that is created, maintained, archived, retrieved or distributed by a computer system.

Technical Safeguards: Measures to protect the library's electronic information and control access to it.

Use: The use of personal information means utilizing (handling or processing) the information to accomplish the library's purposes for which it was collected. Under the Protection of Privacy Act (POPA), a use of personal information is considered consistent with the purpose for which the personal information was originally collected or compiled, if it has a reasonable and direct link to the original purpose and is necessary to provide an authorized program or service.

Volunteer: A person who performs tasks which contribute to the operation of the library or the provision of any library service and is not paid a wage or salary by the library for performing these tasks. Some exceptions may be granted for one-time Volunteers. **In accordance with POPA, Contractors, Volunteers, and Board Members are considered Employees for the purpose of Privacy obligations and training requirements.*

Roles and Responsibilities

Chief Executive Officer (CEO)

- Head of the Strathcona County Library for the purposes of POPA and ATIA;
- Responsible for the library's compliance with the POPA and ATIA Acts;
- Responsible for decisions made under the POPA and the ATIA regarding the protection of privacy as it relates to the library; and
- May delegate powers and duties, in writing, to another Employee of the library under section 55, except the power to delegate.

Strathcona County Library Privacy Officer (PO) and Access to Information Coordinator

- Delegated library Employee;
- Responsible for day-to-day operations of library's Privacy Management Program (PMP);
- Responsible for the library's compliance with the POPA and ATIA Acts;
- Serves as the primary point of contact for privacy inquiries and concerns as well as access to information requests;
- Responsible for the development, implementation and ongoing review/management of the library's (PMP);
- Develops library specific and role-based training in collaboration with the Human Resource Specialist;
- Ensures completion of Privacy Impact Assessments to confirm that any programs, administrative practices, etc., involving Personal Information or data derived from Personal Information, comply with the privacy protection provisions of the POPA;
- Responds to correction of Personal Information requests in accordance with the library's policies and legislated timelines; and
- Investigates privacy complaints, taking actions (as may be needed) to address the complaint and mitigate the risk of recurrence.

Human Resources

- Delivers onboarding Privacy Training to new Employee(s);
- Track privacy training statistics to ensure legislative compliance and report training deficiencies to the Privacy Officer;
- Develops library specific and role-based training in collaboration with the Privacy Officer; and
- Provides support to the CEO or Privacy Officer in the event of an ATI request, if required.

Employees

- Understand their roles and responsibilities under POPA;
- Protect Personal Information, data derived from Personal Information, and Non-Personal Data against such risks as unauthorized Access, Collection, Use, Disclosure or destruction;
- Complete any required training related to their privacy protection obligations;
    - Mandatory Government of Alberta Privacy Training for Public Bodies; and
    - Role-based training and refreshers that may be developed;

- Adhere to the library's privacy management program policies and procedures;
- Ensure any Collections/Uses/Disclosures of Personal Information and Non-Personal Data are authorized under the Act, and done only to the extent necessary to complete their job duties;
- Notify and work with their supervisor and other parties as required, to assist with the investigation process in the event of a Privacy Incident; and
- Ensure the appropriate agreements, safeguards or other compliance mechanisms are in place prior to Collecting, using or Disclosing Personal Information, data derived from Personal Information or Non-Personal Data.

Library Board Members

- Understand their roles and responsibilities under POPA;
- Protect Personal Information, data derived from Personal Information, and Non-Personal Data against such risks as unauthorized Access, Collection, Use, Disclosure or destruction;
- Complete any required training related to their privacy protection obligations;
- Review and approve PIA risks and mitigations; and
- Adhere to the library's privacy management program's policies and procedures.

Volunteers

- Understanding their roles and responsibilities under POPA;
- Protecting Personal Information, data derived from Personal Information, and Non-Personal Data against such risks as unauthorized Access, Collection, Use, Disclosure or destruction;
- Completing any required training related to their privacy protection obligations; and
- Adhering to the library's privacy management program's policies and procedures.

Practicum and Job Shadow Students

- Understanding their roles and responsibilities under POPA;
- Protecting Personal Information, data derived from Personal Information, and Non-Personal Data against such risks as unauthorized Access, Collection, Use, Disclosure or destruction;
- Completing any required training related to their privacy protection obligations; and
- Adhering to the library's privacy management program's policies and procedures.

Contractors

- Understanding their roles and responsibilities under POPA;
- Protecting Personal Information, data derived from Personal Information, and Non-Personal Data against such risks as unauthorized Access, Collection, Use, Disclosure or destruction;
- Complete any required training related to their privacy protection obligations**; and
- Adhering to the library's privacy management program's policies and procedures.

***Please see Training and Education section for more information.*

Designation of Privacy Officer

The Organizational Development Project Libarian is the delegated Privacy Officer for Strathcona County Library. For questions related to the Use, Disclosure or Collection of Personal Information please contact the library's Privacy Officer at privacy@sclibrary.ca or (780) 416-6712.

See **APPENDIX A**—— Protection of Privacy Act Delegation Table for official appointment letter and delegation table.

Collection, Use and Disclosure of Personal Information

Collection of Personal Information

Strathcona County Library is authorized to Collect Personal Information under the circumstances set out in section 4 of the POPA. The library only Collects Personal Information that is directly related to and necessary for the program or activity that the information is being Collected for in accordance with privacy legislation.

In accordance with POPA section 12(1)(a) and 13(1)(b), the library is authorized to Use or Disclose Personal Information for a purpose that is consistent with and has a reasonable and direct connection to the original purpose (*i.e. Personal Information Used for a library registration may be Accessed when patron registers for a program using the same card number).*

As per section 5(1) of POPA, the library Collects information directly from the individual it pertains to. This ensures individuals are aware of the type of information being Collected and transparency around how it will be Used, allowing an individual to challenge the need for the information or refuse to provide the information or participate in the program or activity.

Use of Personal Information

Strathcona County Library may only Use Personal Information to accomplish the library's purposes for the Collection (i.e. to administer a program or activity, provide a service, or to sign up for a library card) or with the consent of the individual in accordance with privacy legislation. The library will only Collect the minimum amount of Personal Information necessary to achieve the purpose for the Collection.

The library will not sell Personal Information in its custody or under its control in any circumstances or for any purposes, including for marketing or advertising purposes.

Collection Notices

When the library Collects Personal Information directly from an individual, in accordance with section 5(2) of POPA, a notice will be provided at the time of Collection and can be provided either in writing, or verbally during an in-person conversation.

Collection notices will include the following information:

- The purpose/reason for the Collection;
- The specific legal authority for the Collection (the specific section(s) that authorized the Collection for the identified purpose);
- Contact information for the Library's Privacy Officer, to which the individual may direct any questions they have about the Collection; and
- The library's intention, if any, to input the information into an Automated system to generate content, make decisions, recommendations or predictions.

Collection Notice Exceptions

If the library has already provided a Collection notice to an individual, and they continue to Collect Personal Information from that individual, they are not required to give notice to the individual every time, provided the purpose and specific legal authority have not changed from the original notice.

Accuracy and Retention

POPA requires that if the library Uses an individual's Personal Information to make a decision that directly affects the individual—including any decision made using an automated system—the library will:

- Make every reasonable effort to ensure the information is accurate and complete; and,
- Retain the Personal Information for at least one year after using it so that the individual has an opportunity to obtain Access to it, if applicable.

Retention may be for a shorter period under certain conditions, as stated in section 6(b) of the Act, which would allow an individual to review, and if necessary, to request a correction of the information Used to make a decision on them before the information is disposed.

Section 6 does not apply if no decision, adverse or otherwise, will be or has been made about an individual. *Examples include: Raw survey data where Personal Information is Collected but the results are rendered anonymous, telephone messages, and unsolicitied resumes that are never considered in relation a position.*

Disclosure of Personal Information

Disclosure of Personal Information can occur both orally or in writing and should be made in a way that helps the requestor and is cost-effective for the library.

The library's Privacy Officer or the CEO will determine the best method of Disclosure after considering the sensitivity of the information requested, the relationship with who it will be Disclosed to, and the type of disclosure. Just as when Collecting or using Personal Information, the library will ensure they only Disclose what is necessary to carry out its purpose in a reasonable manner.

Creation, Use and Disclosure of Non-Personal Information & Data Matching

Creation of Non-personal Data

Section 21(1) of POPA authorizes the creation of Non-personal Data for one or more of the following purposes:

- Research and Analysis; and
- Planning, administering, delivering, managing, monitoring or evaluating a program or service.

Under 21(3), the library will only Use Personal Information or data derived from Personal Information if it is already in the custody or under the control of the library. The library will not Collect Personal Information from another public body to create Non-personal Data unless it is an authorized Collection. Non-personal Data created must be created in accordance with:

- **Generally accepted best practices—**ensuring that information is modified, generated or anonymized in accordance with industry standards.
- **Prescribed requirements:**
    - **Quality assurance:** A data quality assurance process to verify that de-identification methods are effective and cannot be easily reversed (re-identification).
    - **Bias mitigation:** Procedures should identify and account for potential biases in the Non-personal Data sets to ensure they remain accurate for research or planning.
    - **Auditability:** Methods used to create Non-personal Data must be documented, and replicable for auditing purposes.

Use of Non-Personal Data

The library may Use Non-Personal Data created under section 21(1) for any purpose. Unlike Personal Information and data derived from Personal Information, there are no restrictions on the library's Use of the Non-Personal Data it has created.

Before using or disclosing Non-personal Data, the library will conduct an assessment that ensures, to the greatest extent possible, that the identity of any individual who is the subject of the Non-Personal Data cannot be identified or reidentified from the data and will identify the level of risk of reidentification as well as take measures to reduce any risk *(as per section 5(2) of the Protection of Privacy Ministerial Regulation)*.

Protection of Non-Personal Data

All staff must protect Non-Personal Data by making reasonable security arrangements against such risks as unauthorized Access, Collection, Use, Disclosure or destruction.

The library has procedures on Use of Non-Personal Data within SCL that have been included in the Administrative, Physical, and Technical Safeguards section.

Access to Information Requests

Information rights

An Applicant has a right of Access to any Non-Personal Record in the custody or under the control of a public body, including a Record containing Personal Information about the Applicant.

How to Make an Informal ATI Request

Any library Record containing Personal Information about a patron can be made available to the patron upon request. Most general information about the library policies, guidelines, and practices are already made publicly available on the library website; however, if you require Access to your own Personal Information, or are authorized to act of behalf of another individual, an informal request by email, phone, or in person is the best place to start. If information is unable to be supplied informally, then you will be referred to make a formal Access to Information Request.

How to Make a Formal ATI Request

For an Access to information request to be considered valid under the Access to Information Act, it must meet all four (4) requirements outlined in Section 7(2):

1. Be in writing (email, physical mail, dropping off a request form or letter, or using an online request service);
2. Be submitted to the library because the Applicant believes the library has custody or control of the Record;
3. Provide enough detail to enable the library to locate and identify the Record within a reasonable time with reasonable effort; and
4. Be accompanied by a fee, where a fee is required under this Act.

***Note**: The library has 30 Business days from receiving a **completed** request. The time frame for processing a request does not start until a request meets all four of the above requirements.*

If a request does **not** provide enough detail to enable the library to locate or identify a Record within a reasonable time with reasonable effort, the library may request further information from the Applicant that is necessary to process the request, and the Applicant shall respond within *30 Business days* with the information being requested.

In a request, the Applicant may ask

1. for a copy of the Record; or
2. to examine the physical Record.

Power to disregard requests

The CEO of the library may disregard a request made under section 7(1) if:

1. Responding to the request would unreasonably interfere with the operations of the public body or amount to an abuse of the right to make a request (*i.e. the request has been made repeatedly or in a systematic nature*) *;
2. The request is abusive, threatening, frivolous or vexatious or is made in an abusive or threatening manner;
3. The information the request relates to has already been provided to the Applicant, or has been made available to the public under section 90 or 91;
4. Despite receiving further information from an Applicant under section 7(3), the library does not have information that is sufficiently clear to enable the library to locate and identify the Record within a reasonable time with reasonable effort; or
5. The request is otherwise overly broad or incomprehensible. **

**Exception: Records related to workplace investigations may not be Disclosed if the head of the library expects it could interfere or cause harm.*

***The library has a duty to assist and will make every effort to help the Applicant Access the information requested.*

Fees for Services

The right to Access Records in custody or under the control of the library may be subject to the payment of a required fee, under Section 96(1) of the ATIA.

If the information requested is **not** publicly available, you must submit a Formal ATI request to the library's Privacy Officer. Section 13 of the Access to Information Regulation requires payment of a *$25.00 initial fee* when an Applicant is requesting Access to information that is *not* their own Personal Information otherwise known as a *general Access request.* If applicable, the initial fee of $25.00 must be paid before work can begin on the request.

Request Type	2026 Cost	Rationale
Fees for requests for Access to Personal Information	None, unless costs **exceeds $10.00.**	For a request for an Applicant's own Personal Information, the library may assess fees only for producing a copy of the Record *(in excess of $10.00, as noted).*
Fees for requests for Access to Non-Personal Information *(general Access requests)*	**$25.00**	For requests for Access to Non-Personal Information otherwise known as *general access requests*, fees above and beyond the initial fee may be charged if the cost of processing the request is estimated to exceed $150
Fees for requests for Access to Non-Personal Information *(continuing Access to information request)*	**$50.00**	

Note: *Schedule 1 of the ATI Regulation sets out the services that the library may charge when processing a general Access request and the maximum fees that may be charged for each service. As laid out in Section 96(3) of the ATIA, if an Applicant is required to pay fees for services, the library must provide the Applicant with an estimate of the total fee before providing the services.*

Correction of Personal Information

The library is committed to ensuring that Personal Information in its custody or under its control is accurate, complete and up to date. In accordance with POPA, an individual has the right to request a correction of Personal Information held by the library. The library will respond to requests within legislated timelines.

Correcting Factual Information vs Opinions

Factual information includes age, date of birth, income information or qualifications.

- The individual must provide proof in support of the correction request that it is of the same nature and at least the same quality as the Personal Information required when the original Collection took place.

Opinions include subjective assessments or evaluations of an individual's condition, abilities or performance.

- The library is not required to correct opinions, professional judgments, or evaluative Records.
- However, individuals may request to have their views about that opinion or a statement of disagreement added to the Record.

Note that a right to request information is **not** a right to have a correction made, depending on the nature of the request. *See 'Correcting Factual Information vs. Opinions' table for more information.*

Informal Requests

An individual may ask for Personal Information (such as a change of name or address) to be corrected and supply proof of correction in a non-formal way. The library may make corrections without a formal requests. Where personal information can be corrected directly by the individual through library authorized systems (such as patron membership acounts), it is encouraged for them to do so without staff intervention.

Formal Requests

Where, in the opinion of the individual, an error or omission exists that the library is unable to address or change informally, a request for correction should be made to the library in writing via the Correction of Personal Information Form. This form can be emailed to privacy@sclibrary.ca.

If decisions or explanations for a Personal Information are deemed unsatisfactory, Applicants have the right to request a review by the Office of the Information and Privacy Commissioner regarding how the correction request was handled (including any annotations, linkages or refusals of the correction request).

Responsible Use of Information and Information Technology

Program Safeguards/Controls

The library applies reasonable security arrangements to protect Personal Information, including Physical, Technical, and Administrative Safeguards based on the sensitivity of the Personal Information or Non-Personal Data.

Administrative Safeguards: *Policies for handling data, such as staff training and Access controls.*

- Limited Information Retention
    - Deletion of patron borrowing data when library materials are returned.
    - Deletion of patron browsing data and downloaded documentation when public computers are logged out.
    - Limits to Employee Access to Personal Information or data derived from Personal Information collected on a need-to-know basis.
- Strong Access Controls
    - Multi-factor authentication wherever possible to add an extra layer of security and employ strong and unique passwords with a required password manager, and a VPN when remoting into library computers.
    - Collect and deactivate Employee secure access cards as part of library's offboarding process.
- Current Procedures and Policies:
    - Privacy Incident procedure;
    - Information Security Policy;
    - Confidentiality Policy;
    - Tabletop Cybersecurity exercises;
    - Non-Personal Data (e.g., methods used, forms, approvals, etc.) procedures are regularly reviewed to ensure they are adequate and current.
- Mandatory Employee training on:
    - Information security regarding social engineering/phishing;
    - Protection of Privacy Act for Public Bodies;
    - Relevant guidelines & procedures, including AI Guidelines and Cybersecurity.

Physical Safeguards: *Protection of physical assets, including secure storage for paper Records and, for electronic information systems, protection from unauthorized intrusion.*

- Restricted areas:
    - Access to non-public areas of the library is protected from unauthorized intrusion by having secure doors.
- Alarms and Security:
    - The library also has an alarm monitoring system and County security are on-site and monitoring video cameras in the Community Centre/County Hall to prevent unauthorized and/or after-hours access.

- Records management policies and program in place:
    - Employee personnel files are stored in a locked cabinet in a secure staff area.
    - Role based access provided to the library's Human Resource Information System (HRIS), is limited to self serve access for all Employees and elevated roles only provided to Managers and Employees that require it for the functions of their position.
    - Policies are in place related to library technology and access to Records.
    - The library follows the protocols established in the Information Security Policy.
    - Acceptance page on public computers includes ways to maintain patron privacy and all patron data is deleted when the patron logs out of a public computer.

Technical Safeguards: *Measures like encryption, firewalls, and secure transmission protocols to protect electronic data.*

- Maintenance and regular updates:
    - Ongoing maintenance and updates to Integrated Library System (ILS) and other software programs;
    - Regular application of software patches and test backups on a scheduled basis;
    - Daily/weekly backups stored off site and on the cloud;
    - Maintained computer hardware and software inventory.
- Technical protections and protocols:
    - Robust firewalls on public and staff computers;
    - Regularly performed internal and external security assessments, penetration testing, and vulnerability scanning to help identify potential weaknesses and areas for improvement;
    - File mirroring with servers located off site for a quicker recovery.
    - Cybersecurity Incident Response Plan, based on recent experience of other public libraries.
    - Automated notifications to IT about potential ransomware attacks and server outages.
    - Use of password managers software to better secure passwords.
    - Encrypted sensitive data (both at rest and in transit) to ensure that if compromised, it remains unreadable and unusable without encryption keys.
    - Servers and network devices have separate subnets on network to better protect them and monitor communications between clients and servers;
    - Restricted need-to-know access to digital storage of financial and sensitive personal data.
- Termination of Employees procedure:
    - Immediate termination of access to library systems.

Role-based Access

The library provides role-based access to the library's Human Resource Information System (HRIS). Employees will only have access to their own Personal Information unless they have an elevated role based on their current position and job duties.

Access to patron information through our Integrated Library System (ILS) and databases is assigned according to staff roles and responsibilities and there are parameters and restrictions around access through minimized shared logins and a multifactor login process. Access to other library systems is provided on a need-to-use basis and is limited to the lowest level of information or roles required to carry out their job duties.

Artificial Intelligence and Automated Systems

Artificial intelligence and Automated systems are increasingly used across the public sector, as these technologies can offer value in their ability to enhance efficiency, automate processes and generate insights. Libraries are enabled to use these technologies in accordance with all relevant legislation.

Transparency
Strathcona County Library adheres to our **AI Best Practices Guideline** to promote transparent, responsible, secure, ethical and human-centered Use. Library AI guidelines determine that personal, confidential or sensitive information will **not** be Used or put into Generative AI tools. Patrons will be notified anytime automated systems will be Used to generate content or make decisions. Any AI-generated content shared with the public will be Disclosed as being AI-generated.

Automated system-specific security controls
Anywhere the library inputs Personal Information into automated systems, appropriate security measures will be in place to protect against unauthorized access and potential incidents. *See Technical Safeguards for more information.*

Surveillance

All security cameras in the library belong to Strathcona County, as our security operates in a shared facility. This footage is restricted to County security and held in accordance with POPA and in adherence to the County's privacy policies and procedures.

The library posts signage to indicate when and if photos may be taken, as well as a Film and Photography for Library Purposes Guideline that requires written permission be obtained before images of people from programs or events are used for any promotional or public facing purposes.

Retention and Disposal of Personal Information

Personal Information Banks

A Personal Information Bank (PIB) is a Collection of Personal Information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an indivdual.

An inventory of the library's Personal Information Banks can be found in **APPENDIX B** of this PMP. The library's PIB will be reviewed and updated whenever the PMP is reviewed or updated, or anytime a new service, Use or type of Personal Information is being Collected.

Security Classification System

Security Classification	Who can Access	Examples
Public	Information explicitly or implicitly approved for distribution to the public without restriction. This information can be and is freely distributed to anyone.	• Board Member names on the library's public website; • Library Board minutes; • Policies and Guidelines; • Press releases; • Statistics; and • Library program descriptions and program guides
Private Also referred to as *Protected A*	Information intended for internal library business and intended only for library staff, including Employees, Contractors, sub-Contractors, and agents with a legitimate need. A-classed information is deemed sensitive outside the library and is generally not made available to outside agencies but is available by default to members of the library.	• Planning documents, operational statistics; • Floor Plans; and • Invoices
Confidential Also referred to as *Protected B*	Information intended for specific Use by a workgroup, department, or group of individuals with a legitimate need-to-know, such as an operational or project team.	• Systems holding patron information; • Personnel files and evaluations; • 3rd party business information submitted in confidence; and • Management Team planning documents

	Authorization by the information owner, or delegate, is required for access.	
Restricted Also referred to as *Protected C*	Highly sensitive information intended for limited specific Use by named individuals or a small group of individuals, with a legitimate need-to-know. Explicit authorization by the information owner is required for access due to legal, contractual, privacy, or other constraints.	• Social Insurance Numbers; • Drivers' License Numbers; • Health related information; • Staff injury reports; • Human Resource Information Systems; and • Financial systems.

Records Retention

The library follows an established Record Retention Program, as set out in library policy OP 04 Records Retention and Disposition and the Records Retention and Disposition Guideline. The program applies to the creation, receipt, Use, handling, maintenance, storage and Disposition of all library Records. This includes Records of all media and formats including email, video and photographs, etc.

Training and Education

Mandatory Training for Employees

All new library Employees and practicum students will complete the Government of Alberta Protection of Privacy Act for Public Bodies course as part of the mandatory training and onboarding process at the library. Retraining will take place every **three years**, starting from the date of POPA and ATIA implementation (June 11, 2025)

All current and new Employees will review the library's Privacy Management Program and sign a Declaration of Confidentiality, Conduct and Data Security as part of their continued employment conditions or onboarding process for all new Employees.

Specific role-based privacy training and staff refresher training will be developed and conducted at the discretion of the CEO or the library's Privacy Officer as part of the library's PMP.

Volunteers and Contractors

POPAs definition of 'Employee' is broad and includes Volunteers, Contractors and suppliers. As such, Volunteers, Contractors and suppliers must complete either:

1. Role-based training about their obligations under Privacy Legislation; or
2. Both the Protection of Privacy Act for Public Bodies course and the Access to Information Act for Alberta Public Bodies course provided by the Government of Alberta.

That training must be completed before such Volunteers, Contractors and suppliers perform any service for the library, and valid training must be maintained during the performance of any service for the library. For purposes of the Privacy Management Program, the training expires and will no longer be considered valid on the date that is 3 years after completion.

The exception to this will include any Volunteer, Contractor or supplier whose service or role requirements **do not** include Accessing, Collecting, using, Disclosing, or managing Personal Information (i.e. CS Shelf Reading and Shelving Volunteers, Elevator maintenance Contractors, etc.). Access to Personal Information will be restricted for those in these roles and will be protected through the measures and safeguards outlined in this program.

Limited role-based training will be provided to library Volunteers and Contractors who will *not* Access, Collect, Use, Disclose or manage Personal Information, but may have supervised access to secure library areas.

Responding to Privacy Incidents

Privacy Incidents

Should there be a loss, unauthorized Access, or unauthorized disclosure of Personal Information due to a Privacy Incident, where there is a real risk of significant harm, the library will give notice to:

a) the individual;
b) the Library Board;
c) the Commissioner (OIPC) if necessary; and
d) the Minister responsible for this Act if necessary.

How Incidents are Managed

It is the responsibility of SCL's Privacy Officer and the CEO to ensure that all Employees — including Volunteers and Contractors — are informed of, and understand, the library's privacy policies and procedures, as well as their specific responsibilities related to Privacy Incident management and notification. The following actions will occur immediately to manage a Privacy Incident:

- Upon confirmation of the existence of a Privacy Incident, the CEO, Privacy Officer, or designate, will determine the scope of the incident and provide an Incident notification to the impacted individual(s), the Library Board and, in cases of significant risk, the Office of the Information and Privacy Commission of Alberta (OIPC) and Minister.
- Staff shall work constructively with the OIPC staff to mitigate the extent of the incident and prevent any further harm.
- The CEO, or designate, in consultation with the manager of the department in which the breach of Policy occurred, shall investigate the cause of the disclosure and investigate events that have led up to the Privacy Incident, with the goal of eliminating potential future occurrences.
- Staff shall work with the departmental manager and the CEO, or designate, to take all reasonable actions to recover the Record and limit the Record's disclosure.
- CEO, or designate, and Privacy Officer will also review the adequacy of privacy protections to prevent future incidents.

Privacy Complaints

The Strathcona County Library is committed to responding promptly, fairly, and transparently to privacy complaints.

In accordance with POPA, *(section 6(1)(b)(i)(C), POPA section 38(2))*, individuals have a right to raise concerns about the Collection, Use, Disclosure or Safeguarding of their Personal Information and to have those concerns reviewed under POPA.

Procedure

Submission of Complaints
Privacy complaints must be submitted in writing to the library's Privacy Officer and should include sufficient detail to allow the complaint to be understood and investigated.

Acknowledgement
The library will acknowledge receipt of a privacy complaint within a reasonable timeframe (no more than *30 business days* after the complaint is received).

Investigation
The Privacy Officer will assess and investigate the complaint, which may include reviewing records, consulting with staff, and taking steps to determine whether POPA has been complied with.

Response
The Privacy Officer is responsible to investigate any complaints to determine whether the complaint is substantiated and take any action as may be needed to address the complaint and mitigate the risk of recurrence.

The complainant will be informed in writing of the outcome of the investigation and any corrective action taken, where appropriate.

Referral to Commissioner
If the complainant is not satisfied with the library's response, they may request a review by the Office of the Information and Privacy Commissioner of Alberta.

For further information regarding the OIPC and Privacy Complaints, visit https://oipc.ab.ca/privacy-correction-complaint.

Privacy Impact Assessments

Completing and Submitting

Strathcona County Library will prepare a Privacy Impact Assessment (PIA) whenever there is a new, or a substantial change to an existing, administrative practice, program, project or service—if one or more of the following applies:

I. If the loss of, unauthorized Access to, or unauthorized disclosure of Personal Information could result in significant harm,
II. A practice, program, project or service will Collect, Use or Disclose Personal Information considered to be of high sensitivity,
III. A practice, program, project or service involves the development or Use of innovative technology.
IV. Or, one or more of the factors requiring the submission of a PIA to the Commissioner apply. *See Section 7(5)* (MIN)

Before launching new programs or changing existing programs that Collect, Use, or Disclose Personal Information, SCL is required to complete a Privacy Impact Assessment that must:

- Describe the project,
- Identify the types of Personal Information that will be Collected, Used or Disclosed,
- Identify any risks to privacy, and
- Explain how risks will be managed to protect that Personal Information.

The library will submit a PIA to the Office of the Information and Privacy Commissioner under certain circumstances, if required by guidelines outlined in the Ministerial Regulation or by specific request of the Commissioner.

Completed PIAs will be retained for the lifespan of the tool or program retention. See Records Retention Policy for more information.

For more information please visit the Government of Alberta Fact Sheet: **Privacy Impact Assessments (PIAs)**

Ongoing PMP Assessment and Revision

The Library's PMP will be reviewed every three years or if a Privacy Incident occurs, to help assess our programs effectiveness and mitigate risks.

Policies and Additional Resources

ATIA Legislation

Confidentiality Policy (OP01)

POPA Legislation

APPENDIX A

Delegation of Authority - Privacy Legislation

REFERENCES: *Access to Information Act*, SA 2024, c A-1.4 ("ATIA")
Freedom of Information and Protection of Privacy Act, RSA 2000, c F-25 (repealed) ("FOIP Act")
Protection of Privacy Act, SA 2024, c P-28.5 ("POPA")
Strathcona County Library Bylaw II Access to Information and Protection of Privacy, *Approved November 17, 2025*

BACKGROUND

In June 2025, the ATI Act (ATIA) and the POP Act (POPA)— together the "Privacy Legislation"— came into force and the FOIP Act was repealed. The transitional provisions provided that the appointment of the 'head' by the library continued until the appointment was made under the Privacy Legislation. Appointment of the Chief Executive Officer as the 'head' of Strathcona County Library for the purposes of the Privacy Legislation will be in effect.

As part of the Privacy Legislation, the Strathcona County Library must implement a privacy management program by June 2026. The development and roll out of a privacy management program and a change in the designation of a “Privacy Officer” require adjustments in some of the delegations of authority.

PERMANENT DELEGATIONS OF AUTHORITY

The delegations of authority set out in the document attached are hereby made by the Chief Executive Officer as delegations of authority of powers, duties, and functions of the Chief Executive Officer as the 'head' of the library for purposes of the Privacy Legislation. The attached delegation table shall be interpreted with references to the ATIA or the POPA as applicable, and to the corresponding section numbers in the ATIA or the POPA as applicable. If the interpretation of a delegation of authority based on the attached delegation table is ambiguous, or if the Privacy Legislation includes any new or changed power, duty, or function of the 'head' in the Privacy Legislation, then such power, duty, or function is hereby delegated by the CEO.

This Delegation of Authority is effective as of June 11, 2026.

Signature, CEO

June 11, 2026

Date

Protection of Privacy Act Delegation Tables

DELEGATION TABLE – PROVISIONS OF THE *PROTECTION OF PRIVACY ACT* AND REGULATION FOR WHICH DELEGATION OF AUTHORITY SHOULD BE CONSIDERED

Duty, power or function of Head	Section reference	Retained by Head	Delegated to Privacy Officer	Delegated to other person(s) (provide title(s) – specific or generic)
COLLECTION, CORRECTION, PROTECTION OF PERSONAL INFORMATION				
Authority to set aside Collection requirements	5(3), (4)	**X**		
Authority to decide on requests for correction of Personal Information	7(1)	**X**		
Duty to correct, annotate or link Personal Information, duty to notify previous recipients	7(3), (4)	**X**		
Duty to give notice to individual requesting correction	7(7)		**X**	
Authority to transfer a request for correction	8	**X**		
Duty to ensure protection of Personal Information by making reasonable security arrangements	10(1) Regulation (MIN) 2, 3	**X**		
Duty to notify the affected individual when there exists a significant risk of harm	10(2) Regulation (MIN) 4	**X**		

Duty to ensure protection of data derived from personal information	20	**X**		
Duty to ensure protection of data derived from non-personal data	24	**X**		
USE AND DISCLOSURE OF PERSONAL INFORMATION				
Establishing rules for electronic consent	Regulation 2(4)(a)	**X**		
Establishing rules for oral consent	Regulation 2(5)(a)	**X**		
Authority to Disclose to guardian of a minor	54(1)(e)	**X**		
Authority to Disclose to relative or adult interdependent partner of deceased individual	13(1)(s)	**X**		
Authority to Disclose to avert imminent danger to health or safety	13(1)(cc) Regulation 1(1)(b)	**X**		
Authority to approve conditions for disclosure for research and statistical purposes and for administration of research agreements	15	**X**		
Authority to Disclose to guardian of a minor	54(1)(e)	**X**		

REVIEWS AND COMPLAINTS				
Authority to ask the Commissioner for advice	28(1)		**X**	
Authority to require Commissioner to examine original Record on site	29(4)	**X**		
Right to make representations to the Commissioner	41(6),(8)	**X**		
Duty to comply with Commissioner's Order	44	**X**		
GENERAL PROVISIONS				
Duty to publish a directory of the body's Personal Information banks and keep it current	57(2), (5)		**X**	
Duty to Record Uses or disclosures of Personal Information not included in directory	57(4)	**X**		

DELEGATION TABLE – ADMINISTRATIVE RESPONSIBILITIES IN THE *PROTECTION OF PRIVACY ACT* AND REGULATION THAT MAY BE ASSIGNED

Duty, power or function of public body	Section reference	Retained by Head	Delegated to Privacy Officer	Delegated to other person(s) (provide title(s) – specific or generic)
COLLECTION, ACCURACY AND RETENTION OF PERSONAL INFORMATION				
Establishing controls over the Collection, Use and disclosure of Personal Information	2(a)		**X**	
Authorizing routine correction of personal information	2(b)		**X**	
Ensuring authorized purpose of Collection	4		**X**	
Assuring proper Collection and notification	5		**X**	
Assuring accuracy of Personal Information	6(a)		**X**	
Applying retention standards	6(b)		**X**	
USE AND DISCLOSURE OF PERSONAL INFORMATION				
Assuring appropriate Uses	12		**X**	
Assuring appropriate purposes of data matching	17		**X**	
Assuring appropriate Uses of data derived from personal information	18		**X**	
Assuring appropriate purposes of disclosure of data derived from Personal Information	19		**X**	
Assuring appropriate purposes for creation of non-personal data	21 Regulation (MIN) 5(1)		**X**	

Assuring appropriate Use and disclosure of Non-personal Data	22, 23 Regulation (MIN) 5(2)		**X**	

Chart from ©2025 Government of Alberta | June 10, 2025 | Technology and Innovation

Appendix B: Strathcona County Library Personal Information Banks Directory
Revised: June 2026

Type	Individuals	Location	Personal Information Collected	Use	Legal Authority for Collection
Board Member Records	Current and retired Library Board Member phone lists of members of the public appointed to the Library Board by Strathcona County Council.	Strathcona County Library	*Information that may be contained:* name, address, phone numbers, email address, number of years of service, birthdate, social insurance number, offices held and committees served on.	Contact information used to allow Library Board members to carry out governance duties, reporting requirements and financial obligations (e.g. charitable fundraising license and return) If the Board Member accepts Worker's Compensation Board coverage, birthdate is required. If the Board Member claims compensation for a board meeting, social insurance number is required for the purpose of issuing T4A forms if the total is greater is $500 in a year.	Protection of Privacy Act (POPA), section 4(c)
Community Contacts	Business and Community Partners	Strathcona County Library	*Information that may be contained:* name, organization, address, email address, phone number.	Used to carry out library partnered programming and other library services.	Protection of Privacy Act (POPA), section 4(c)
Contractor Records – Program Presenters	Library Contractors and Program Presenters	Strathcona County Library	*Information that may be contained:* name, address, phone numbers, email address, emergency contact information, police information records check (if applicable to position).	Used to manage library contracts for services such as Resume Tutoring and Writer in Residence Program. Used to issue payments or honorariums.	Protection of Privacy Act (POPA), section 4(c)
Donor Records	Donors to Strathcona County Library	Strathcona County Library Donor Management Software	*Information that may be contained:* name, address, phone numbers, email address, amount of donation or gift, and special requests/circumstances.	Used for correspondence and contact with Library donors and prospective donors and to create charitable tax receipts for donations made to the library. Name used with permission for annual report.	Protection of Privacy Act (POPA), section 4(c)
Employee Records	Current and Past Library Employees	Strathcona County Library Human Resources Information	*Information that may be contained:* name, address, phone numbers, email address, employee number, resume, social insurance number, birth date, earnings, salary grid placement, employment	Personnel files for past and present library employees in print and electronically in library's HRIS to support administrative, financial, staff scheduling and payroll functions of library employment.	Protection of Privacy Act (POPA), section 4(c);

		System (HRIS)	commencement date, emergency contact, benefit plans, vacation leave, sick leave, flex, OT and extra time earned, medical appointment time, special leave, hours worked, tax records, performance appraisals, correspondence, employment letters, training certificates, criminal record checks, driver's licence and abstract.		Employment Standards Code; Income Tax Act
Employment Records	Employment Applicants	Strathcona County Library	*Personal information requested on the library application form*: name, address, phone number, and email address. Additional information depends on what was submitted by the applicant on paper or via email.	Submitted resumes and cover letters for employment application and screening purposes.	Protection of Privacy Act (POPA), section 4(c); Employment Standards Code; Income Tax Act
Employee Records	Current and Past Library Employees	Strathcona County Library When to Work (W2W) Software	*Information that may be contained:* employment start date, maximum hours, name, email, phone numbers, position, pay rate.	When to Work (W2W) staff scheduling software is used to manage library employment and operations.	Protection of Privacy Act (POPA), section 4(c); Employment Standards Code; Income Tax Act
Employee Records Grant Applications	Current and Past Library Employees	Strathcona County Library	*Information may include*: name, contact information.	Grant applications that include personal information e.g. STEP, CSJ, Young Canada Works.	Protection of Privacy Act (POPA), section 4(c)
Incident Reports - *Employees*	Library Employees who are injured or have a near miss while at work.	Strathcona County Library Patron Interaction Tracking Software (PITS)	*Information that may be contained:* name(s), contact information, nature of injury or loss, and circumstances of incident.	Incident Reports for damage to personal property and health and safety incidents to comply with Alberta OHS legislation and safe workplace obligations. Used to create WCB claims for staff workplace injuries, for insurance purposes, and Health and Safety Committee review of safe work procedures and hazard assessment.	Protection of Privacy Act (POPA), section 4(c)

Incident Reports - *Patrons*	Library Patrons who are involved in accidents or incidents at the library	Strathcona County Library Strathcona County Community Centre Security Patron Interaction Tracking Software (PITS)	*Information that may be contained:* name(s), physical description, photograph, contact information, nature of injury or loss, witnesses and their contact information, first aid treatment provided and circumstances of incident.	Used to record and create patron incident reports for behaviour that breaches library patron code of conduct, damage to personal or library property and health and safety incidents to comply with Alberta OHS legislation and safe workplace obligations. Used to issue library suspensions, bans or trespass notices. Information may be disclosed to Strathcona County Community Centre Security or law enforcement in accordance with County and Library policy and legislation.	Protection of Privacy Act (POPA), section 4(c)
Outreach Patron Records	Library Patrons or members of the public requesting this service.	Strathcona County Library	*Information that may be contained:* name, address, phone numbers, email address, borrower's card number, name of emergency contact, phone number, reading or resources interests, partnered volunteer name, their relationship to patron and contact details, and start and end date of program participation.	Used to administer and manage the library's Outreach and Service Where You Are programs and match outreach volunteers with program patrons.	Protection of Privacy Act (POPA), section 4(c)
Patron Records	Library Cardholders	Strathcona County Library	*Information that may be contained:* patron name, address, email addresses, phone numbers, computer identification number, status of materials, charges, outstanding balance of materials and fees, pseudo birth date to indicate when minor will come of age, identification, parent/guardian, alternate address, email address, personal identification number, guarantor, type of membership, day the card was last used, date record was last modified, expiry date of membership, the number of items	Cardholder registration records are used to issue library cards and to create email notices and letters for/from Strathcona County Library cardholders and cardholders from other libraries regarding circulation accounts. (may include information regarding overdue notices, fines owing, requests and hold notification – stored on database). **Note:** *Parent/guardian information only collected if cardholder is a minor.* Used to create E-newsletters with information relevant to cardholders.	Protection of Privacy Act (POPA, section 4(c); Libraries Act

			checked out on the card, barcode number of card and of items borrowed from the Bookmobile on the day of registration.	**Note**: *Cardholders can opt out of E-newsletter service at any time.*	
Patron Records	Library Patrons who correspond with the library about programs and services, collections and library card accounts	Strathcona County Library	*Information may include:* name, address, phone number, email address, library card number, interlibrary loan items or library material purchase requested, reading interests, and reading history.	Correspondence including email with patron contact information. Used to manage Interlibrary Loan Services and library material purchase requests. Respond to patron reference or assistance requests sent to general information email accounts, including info@ circinfo@ Used to create personalized reading lists at patron's request. **Note:** *Contact information is recorded for detailed or difficult reference questions where it might be necessary to contact the patron when additional information is located.*	Protection of Privacy Act (POPA), section 4(c)
Patron Records	Library Patrons who qualify for print disabled services	Strathcona County Library Daisy Collection Service CELA	*Information that may be contained:* name, address, phone numbers, and contact person.	Daisy Collection Service and CELA registration for members of the public that qualify for print disabled services.	Protection of Privacy Act (POPA), section 4(c)
Patron Records	Library Patrons entering contests.	Strathcona County Library	*Information that may be contained:* name, address, phone number, email addresses.	Contest/Draw forms	Protection of Privacy Act (POPA), section 4(c)

Appendix B: Strathcona County Library Personal Information Banks Directory
Revised: June 2026

Patron Records	Library Patrons who request event notification	Strathcona County Library	*Information that may be contained:* name, address, phone numbers and email address.	Notification of upcoming library events	Protection of Privacy Act (POPA), section 4(c)
Patron Records	Library Patrons who have signed up to receive e-newsletters	Strathcona County Library	A third-party vendor stores the patrons email address then generates customized content to fit patron profile.	Used to share library information with cardholders. **Note*:*** *Patrons can opt out of this service.*	Protection of Privacy Act (POPA), section 4(c)
Patron Records	Library Patrons who have provided photo permission or promotional release forms	Strathcona County Library	*Information may include*: name, email address, phone number, likeness description (photos), comments about the library, reviews of library materials and titles of materials reviewed.	Names of people who have given the library their permission to use their names and/or pictures, review of library materials or to quote their comments about the library in promotional materials, reports or public relation purposes.	Protection of Privacy Act (POPA), section 4(c)
Patron Records	Library Patron Program Participants	Strathcona County Library	*Information that may be contained:* name, phone numbers, email address, library card number	Downloaded program participants listed for members of the public that register for or attend Library programs or use Library services where registration is taken e.g. Resume Tutor	Protection of Privacy Act (POPA), section 4(c)
Patron Records	Library Patron Program Participants	Strathcona County Library	*Information that may be contained:* name, phone numbers, email addresses, ages, or grade levels.	Used to administer library programming.	Protection of Privacy Act (POPA), section 4(c)
Room Booking Agreements	Businesses, Community Organizations, members of the public and library patrons who book/use library rooms	Strathcona County Library	*Information that may be contained:* name, phone numbers and email address and purpose of meeting and reason for refusal or library-initiated cancellation.	Used to administer shared use of library rooms and obtain agreement about how the room will be used.	Protection of Privacy Act (POPA), section 4(c)
Security Camera Footage	Library Patrons; Members of the Public;	Strathcona County Community	*Information that may be contained:* Video recordings of interior and exterior of library and Strathcona	Information collected by video surveillance systems will only be used for the purpose for which it was collected and only used or	Protection of Privacy Act (POPA), section

	Employees	Centre Security	County Community Centre.	disclosed by County Community Centre Security in accordance with legislation. May be disclosed to law enforcement in accordance with County policy and legislation.	4(c)
Vendor Records	Library Vendors	Strathcona County Library	*Information that may be contained:* name, company name, address, phone, email address, GST# if applicable.	Used to manage vendor contracts, procure equipment or services, and issue payments or honorariums	Protection of Privacy Act (POPA), section 4(c)
Volunteer Records	Library Volunteers	Strathcona County Library	*Information that may be contained:* name, address, phone numbers, email address, emergency contact information, aide or support worker contact and emergency contact information, skills, police information records check (if applicable to position) and hours available for volunteering and completed hours.	Used to manage the library's volunteer program. Volunteer forms and schedules for individuals who have applied or been accepted to volunteer on behalf of the library recorded on paper or electronically.	Protection of Privacy Act (POPA), section 4(c)

Strathcona County Library

Declaration of Confidentiality and Information Security

As an Employee, Volunteer or Board Member of the Strathcona County Library, it is understood and hereby agreed to abide by the following conditions by the undersigned:

1. All confidential or personal information which comes to me during my employment with Strathcona County Library shall be kept confidential and only used for the purpose for which it was collected. Personal information will not be released to anyone unless the Library CEO or Privacy Officer specifically consent to its disclosure, in accordance with POPA and ATIA legislation.
2. Social media posts or public statements about the library, shall only be made to the media in keeping with the Strathcona County Library Social Media and Media Relations Policies.
3. All employees have a responsibility to ensure that they have read and are familiar with the library's policies, guidelines and procedures relating to Information and Data Security that are relevant to their work, and that they manage information accordingly, or as set out in the library's Information Security Policy.
4. I understand and accept that, should I breach this Confidentiality Agreement, it may result in disciplinary action including dismissal.
5. I have read and agree to comply with the following Strathcona County Library policies and guidelines and agree to comply with all future revisions to or replacements of these policies and guidelines.

    - OP 01 – Confidentiality and Disclosure of Personal Information Policy
    - OP 09 - Information Security Policy
    - PR 03 – Social Media Policy
    - PR 09 – Media Relations Policy
    - Guideline – AI Best Practices Guideline
    - Guideline - Employee Use of Technology
    - Strathcona County Library Privacy Management Program (PMP)

Print Name _____

Signature _____ **Date** _____

Collection and use of personal information: *Personal information is collected under the authority of s. 4(c) of the Protection of Privacy Act and will be used to manage and administer Strathcona County Library's Privacy Management Program. If you have any questions regarding the collection or use of this information, please contact the Privacy Officer at privacy@sclibrary.ca*