Privacy Management Program

Created: June 11, 2026
Date for Review: 2029
Reference: Protection of Privacy Act and Access to Information Act Legislation
Privacy Officer contact information: privacy@fspl.ca 780-998-4288

Table of Contents

Section 1. Governance and Administration 4
Privacy Management Policy 4
Delegation of Authority Table: See Appendix A 4
Definitions: 4
Roles and Responsibilities Framework 6
Library Board (Governance Oversight) 6
Library Director (Head of Public Body & Designated Privacy Officer) 6
Library Employees (Permanent, Temporary, & Casual Staff) 7
Volunteers, Practicum Students, & Third-Party Contractors 8
Public Access to the Privacy Management Program (PMP) & Protecting Security Safeguards 9
Fulfilling Direct Public Requests: 9
Protection of Security Safeguards: 9
Section 2. Information Mapping, Safeguards & Access Controls 9
Personal Information Bank Directory – see Appendix B 9
Security Classification System 9
High-Sensitivity Information Threshold 10
Security Classification Tiers Matrix 10
Mixed Records Principle 12
Program Safeguards & Controls 12
Administrative Safeguards 12
Physical Safeguards 13

Privacy Management Program

Technical Safeguards 13
Public Workstation & Peripheral Protection 14
System Maintenance, Asset Management & Disaster Recovery 14
Records Retention Reference Statement 15
Mandatory POPA Retention Rules 15
Proactive Monitoring, Security Testing & Incident Response 15
Automated Systems & AI Security Controls 16
Video Surveillance & Security Cameras 16
Role-Based Access Control Protocol 17
Account Management & Credentials 17
Access Permissions Summary 17
Monitoring & Compliance 17
Section 3. Collection, Accuracy, and Records Retention 18
Collection Notices & Exceptions Protocol 18
Mandatory Collection Notice Requirements 18
Notice Exceptions (POPA s. 5(3) & 5(4)) 18
Data Accuracy Standard (POPA s. 6(a)) 19
Operational Standards 19
Records Retention & Secure Disposal 19
Decision-Making Records Retention Standard (POPA s. 6(b)) 19
General Records Retention & Secure Disposal 20
Authorized Destruction Methods 20
Section 4. Disclosure of Personal Information 21
Disclosure Formats (In Writing or Orally) 21
Method Determination & Data Minimization (POPA s. 13(4)) 21
Statutory Disclosure Authorities (POPA s. 13 & s. 54) 21

Privacy Management Program

Section 5. Non-Personal Data & Data Matching 22
Creation of Non-Personal Data (POPA s. 21) 22
Custody Requirement 22
Creation Standards & Requirements 22
Use & Protection of Non-Personal Data (POPA s. 22; M-Reg s. 5(2)) 23
Unrestricted Internal Use 23
Re-identification Risk Assessment 23
Security Safeguards 23
Data Matching & Data Derived from Personal Information 23
Section 6. Access to Information Requests & Service Fees 23
Information Access Rights & Request Paths 23
Power to Disregard Access Requests 24
Mandatory Procedure for Disregarding a Request: 24
Fee Schedule for Access Requests (ATIA s. 96; ATI Regulation s. 13) 25
Section 7. Operational Rights & Incident Procedures 25
Correction of Personal Information Procedure 25
Privacy Complaints Procedure 27
Privacy Incident (Breach) Response Procedure 29
Privacy Impact Assessment Workflow 30
Required PIA Content 31
Privacy Impact Assessment (PIA) Procedure 32
Privacy Impact Assessment (PIA) - Staff Intake Form ..... **Error! Bookmark not defined.**
Appendix A: Delegation of Authority Table 34
Appendix B: Personal Information Bank Directory 38
Appendix C: Oath of Confidentiality ..... **Error! Bookmark not defined.**

Privacy Management Program

Section 1. Governance and Administration

Privacy Management Policy

The Library Director is the designated Privacy Officer for Fort Saskatchewan Public Library. For questions related to the Use, Disclosure or Collection of Personal Information please contact the library's Privacy Officer at privacy@fspl.ca or (780)998-4288.

Delegation of Authority Table: See Appendix A

Definitions:

Access to Information Act (ATIA): Provincial legislation that establishes rights for people to request and access records that are in the custody or under the control of public bodies, subject to limited and specific exceptions.

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.

Artificial Intelligence (AI) / Automated Systems: Any system, software, or process that uses computation (such as machine learning) to generate outputs, determine outcomes, make or aid decisions, or profile and rank individuals.

Collection: Occurs when a public body gathers, acquires, receives, or obtains personal information. This may be done through forms, interviews, online databases, audio/video recordings, or automated systems.

Data Matching: The practice of linking personal information between two or more databases or electronic information systems to create new information about an individual.

Disclosure: To release, transmit, reveal, expose, show, provide copies of, tell the contents of, or intentionally or unintentionally give personal information to a third party by any means (including oral transmission, paper, or electronic transfer).

Employee: For the purposes of privacy obligations and training requirements under POPA, an "employee" is broadly defined as anyone who performs a service for the public body.

This legally includes paid library staff, contractors, volunteers, students, and Library Board Trustees.

Non-Personal Data: Data (including data derived from personal information) that has been generated, modified, or anonymized so that it no longer identifies any specific individual.

Personal Information: Recorded information about an identifiable individual. This includes, but is not limited to, an individual's name, home address, email, phone number, age, identifying numbers (e.g., library card number), circulation and borrowing records, financial details, photographs, and personal views or opinions.

Physical Safeguards: Measures to protect the library's physical assets, including electronic information systems, from natural/environmental hazards and unauthorized physical intrusion (e.g., locked filing cabinets, restricted staff areas).

Privacy Impact Assessment (PIA): A formal risk assessment process used to identify and mitigate privacy risks when introducing a new, or significantly changed, administrative practice, program, or service that involves the collection, use, or disclosure of personal information.

Privacy Incident (Breach): Any occurrence of loss, unauthorized access to, unauthorized collection, use, or disclosure of personal information. A breach requires notification to the provincial commissioner if it creates a "Real Risk of Significant Harm" (RROSH) to the affected individuals.

Privacy Management Program (PMP): A structured framework of policies, procedures, practices, and roles designed to ensure the library complies with, and is accountable for, its privacy obligations under the legislation.

Privacy Officer: The mandatory role designated by the head of the public body. This individual oversees the day-to-day operations of the PMP and is responsible for compliance, risk reporting, handling access requests, and ensuring staff receive privacy training.

Protection of Privacy Act (POPA): Authority-based provincial legislation that governs the protection of privacy related to personal information in the custody or control of Alberta public bodies. It establishes privacy rights and strictly controls how the library may collect, use, disclose, and secure personal data.

Privacy Management Program

Record: Any recorded information, regardless of medium or format, created or received in the course of business. Records include physical paper forms, digital database entries, emails, sticky notes, photographs, and video surveillance footage.

Technical Safeguards: Measures to protect the library's electronic information and control access to it (e.g., passwords, network encryption, cybersecurity defenses).

Use: Utilizing, handling, or processing personal information internally to accomplish the specific library purpose for which that information was originally collected.

Roles and Responsibilities Framework

Library Board (Governance Oversight)

Under provincial governance frameworks, the Library Board represents the public body. While daily operations are delegated, the Board retains ultimate governance oversight.

Responsibilities:

- Policy Approval: Review and approve the overarching Privacy Management Policy and fundamental PMP framework.
- Resource Allocation: Ensure the Library Director / Privacy Officer is provided with sufficient financial, operational, and human resources to maintain a compliant PMP.
- Governance Training: Complete mandatory privacy orientation appropriate to trustees' governance, oversight, and confidentiality obligations.
- High-Level Risk Review: Review high-level privacy risks, major Privacy Impact Assessments (PIAs), and significant breach notifications where required.

Library Director (Head of Public Body & Designated Privacy Officer)

In accordance with POPA and Board designation, the Library Director serves as the Head of the public body and fulfills the statutory role of Privacy Officer.

A. Statutory Duties as Head of the Public Body:

- Ultimate Legal Accountability: Hold responsibility for decisions made under POPA and ATIA regarding the protection of personal information.

- Delegation Instrument: Maintain and execute the written Delegation of Authority Table under Section 55 of POPA.

B. Operational Duties as Privacy Officer:

- PMP Architecture & Leadership: Design, implement, monitor, and periodically update the library's operational PMP procedures and controls.
- Primary Liaison: Act as the primary contact for public and patron inquiries, formal access requests, correction requests, and privacy complaints.
- Incident & Breach Management: Lead privacy incident containment, conduct risk assessments (evaluating Real Risk of Significant Harm - RROSH), and issue mandatory notifications to affected individuals, the OIPC, and the Minister.
- Privacy Impact Assessments (PIAs): Conduct, sign off on, and submit PIAs to the OIPC for new or significantly altered programs, automated tools, or cloud systems that collect personal data.
- Directory Maintenance: Maintain and publish the library's Personal Information Bank (PIB) directory.
- Training Program Oversight: Oversee the delivery of mandatory annual privacy training, track completion records, and address training deficiencies.
- Regulatory Reporting: Maintain statistics on access requests, complaints, and privacy breaches to fulfill provincial annual reporting requirements to the Minister.

Library Employees (Permanent, Temporary, & Casual Staff)

All staff members interact with personal information during daily library operations and are directly responsible for protecting patron and organizational privacy.

Responsibilities:

- Mandatory Training: Complete the mandatory Government of Alberta POPA training and review the internal PMP during onboarding, renewing completion annually.
- Safeguarding Information: Apply technical, physical, and administrative safeguards in daily tasks (e.g., locking computer screens, securing paper records, using strong passwords, and observing clean desk rules).

- Need-to-Know & Data Minimization: Access personal information strictly on a need-to-know basis and collect/use only the minimum information necessary to deliver library services.
- Patron Confidentiality: Hold all patron borrowing history, digital resource use, and account details in strict confidence.
- Routine Account Updates: Process basic, informal patron requests to update contact details (e.g., address, phone number, email) directly in the integrated library system.
- Incident Reporting: Promptly report any loss, unauthorized access, or misdelivery of personal information to a direct supervisor or the Privacy Officer.

Volunteers, Practicum Students, & Third-Party Contractors

Under Section 1(h) of POPA, the legal definition of an "employee" broadly includes any individual or corporation performing services for the public body, including volunteers, practicum/job shadow students, and third-party contractors.

Responsibilities:

- Compliance with PMP: Adhere to FSPL privacy policies, collection rules, and security controls for the entire duration of their service or contract.
- Role-Proportionate Training: Complete role-based privacy orientation or the GoA POPA course prior to being granted access to library network folders, physical staff areas, or personal information holdings.
- Confidentiality Agreements: Execute a formal Declaration or Oath of Confidentiality prior to commencing work.
- Contractual Safeguards (Contractors & Service Providers): Third-party service providers (such as IT maintenance, software vendors, or external auditors) must abide by privacy protection clauses embedded in their service agreements to ensure data is protected at a standard equivalent to the library's internal controls.

Privacy Management Program

Public Access to the Privacy Management Program (PMP) & Protecting Security Safeguards

Fulfilling Direct Public Requests:

In accordance with Section 25(3) of the Protection of Privacy Act (POPA) and Section 6(3) of the Protection of Privacy (Ministerial) Regulation (M-Reg), FSPL makes its Privacy Management Program (PMP) publicly available on its website. When a direct request for the PMP is received from an individual, staff will fulfill the request by providing either a hard copy or direct guidance to the web link within 30 business days.

Protection of Security Safeguards:

Under Section 6(4) of the Ministerial Regulation, when providing PMP documentation to the public or fulfilling a direct request, the library is explicitly authorized to withhold or redact sensitive technical and security-related information. This includes detailed descriptions of IT controls, server configurations, network architecture, security threat and risk assessments (STRAs), or penetration testing documentation that could be used for adversarial purposes or otherwise compromise the security of personal information in the library's custody or control.

Section 2. Information Mapping, Safeguards & Access Controls

Personal Information Bank Directory – see Appendix B

Security Classification System

In accordance with Section 6(1)(c) and Section 2(1) of the *Protection of Privacy (Ministerial) Regulation* (PPMR), the library maintains a security classification system to categorize all personal information, data derived from personal information, and non-personal data in its custody or under its control based on sensitivity.

Privacy Management Program

Classifying records ensures that reasonable administrative, physical, and technical safeguards are applied proportionally to the level of risk and sensitivity context.

High-Sensitivity Information Threshold

The following categories are legally deemed high-sensitivity information and automatically require Level 3 (Confidential) or Level 4 (Restricted) safeguards:

- Biometric Information: Unique measurable biological or behavioral characteristics.
- Financial Information: Banking details, credit card numbers, tax deductions, or salary history.
- Vulnerable Demographics: Personal information respecting a minor, senior, or vulnerable individual.

Security Classification Tiers Matrix

The library categorizes all physical and electronic records across four security levels:

Classification Tier	Access Scope	Library Record Examples	Required Security Safeguards
Level 1: Public	Unrestricted Public Access Approved for public distribution without limitation.	Board Trustee names & minutes, published policies, press releases, program guides, aggregated stats.	Admin: Website review. Physical: Public areas. Technical: Standard web backups.
Level 2: Private *(Protected A)*	Library Staff, contractors, and agents with a legitimate operational	Floor plans, vendor invoices, operational planning documents, internal stats.	Admin: Clean desk standards.

Privacy Management Program

	need. Sensitive if released externally.		Physical: Locked staff-only workrooms. Technical: Password-protected network logins.
Level 3: Confidential *(Protected B)*	Specific Need-to-Know Workgroups Authorized operational teams, department managers, or specific staff.	Integrated Library System (ILS) patron accounts, personnel evaluations, incident logs, 3rd party confidential business data.	Admin: Role-based ILS permissions, confidential paper disposal service or shredding. Physical: Locked filing cabinets. Technical: MFA, encrypted transit, auto-logout session purges on public terminals.
Level 4: Restricted *(Protected C)*	Named Executive & Administrative Roles Only Strictly restricted to named positions (Library Director / Privacy Officer, Payroll) due to legal or privacy constraints.	Social Insurance Numbers (SIN), banking details, employee injury/WCB files, formal legal/OIPC files, HRIS.	Admin: Strict need-to-know enforcement. Physical: Fireproof locked filing cabinets. Technical: High-level encryption at rest & in transit, restricted network subnets, strict audit logging.

Privacy Management Program

Mixed Records Principle

When a single file or record contains items of varying sensitivity levels (e.g., an employee personnel file containing a basic name/phone number alongside a Social Insurance Number or bank account details), staff must protect the entire record in accordance with the safeguards required for the highest security level contained within it.

Program Safeguards & Controls

In accordance with Section 10 of the *Protection of Privacy Act* (POPA) and Section 6(2)(b) of the *Protection of Privacy (Ministerial) Regulation*, the library maintains a multi-layered framework of administrative, physical, and technical safeguards. These controls are applied proportionally to the security classification of records to protect personal information against loss, theft, and unauthorized access, collection, use, disclosure, or destruction.

Administrative Safeguards

- Need-to-Know Access: Staff, contractors, and volunteers are granted access to personal information strictly on a "Need-to-Know" and "Minimum Necessary" basis to perform their assigned operational duties.
- Mandatory Privacy Training: All new employees, Board Trustees, volunteers, practicum students, and contractors must complete mandatory POPA privacy training upon onboarding, with mandatory retraining required every three (3) years.
- Confidentiality Declarations: Staff, Trustees, volunteers, and service providers must sign a formal Declaration of Confidentiality prior to being granted access to library systems.
- Transitory Records Minimization: Staff must actively delete transitory electronic files (e.g., email attachments, temporary registration spreadsheets) as soon as the primary document is saved to a restricted network folder or the program/transaction concludes.
- Clean Desk & Workstation Security: Staff must secure physical records when leaving workstations and lock computer screens (Win + L) whenever leaving devices unattended.

Privacy Management Program

Physical Safeguards

- Restricted Access Areas: Non-public staff workrooms, IT server spaces, and administrative offices are protected by secure access doors, key fobs, or physical locks.
- Secure Paper Record Storage: Level 3 (Confidential) and Level 4 (Restricted) paper records—including employee personnel files and legal/incident records—are stored in locked or fireproof filing cabinets in restricted staff areas.
- Contracted Confidential Disposal: Physical documents containing personal information (such as sign-up sheets, draft notes, or printed reports) must be deposited directly into locked disposal bins for certified destruction by the library's contracted confidential shredding service or cross-cut shredded in the in-house shredder.

Technical Safeguards

System Authentication & Access Control

- Role-Based Access Controls: Digital access to the Integrated Library System (ILS), Human Resources, and network databases is granted strictly according to staff roles and job duties. Access is limited to the lowest level required, and shared logins are minimized.
- Multi-Factor Authentication (MFA) & Password Management: Multi-Factor Authentication (MFA) is enforced wherever supported. All staff must use authorized password manager software to generate, store, and secure strong, unique passwords.
- Secure Remote Access: Staff remoting into library workstations or systems from external locations must connect through an authorized Virtual Private Network (VPN).
- Immediate De-provisioning upon Offboarding: Digital credentials, user accounts, email access, network drive permissions, and secure access cards are revoked immediately upon an employee's or contractor's resignation, termination, or contract conclusion.

Network Security, Encryption & Data Isolation

- Data Encryption: Sensitive personal information and financial data are encrypted both at rest on servers and cloud storage media and in transit across internal and external networks.
- Firewalls & Network Segmentation: Robust firewalls are maintained on all public and staff workstations. Servers, network storage devices, and critical systems are isolated on dedicated network subnets to monitor client-server traffic and prevent lateral intrusion.
- Restricted Need-to-Know Storage: Financial records, HR files, and high-sensitivity personal information are stored in restricted digital directories with explicit need-to-know permission lists.

Public Workstation & Peripheral Protection

- Public Terminal Purges: Public computer stations automatically delete patron browsing histories, session logs, downloaded documents, temporary files, and borrowing data immediately upon user logout.
- Photocopier & Scanner Memory Protection: Multifunction copiers, scanners, and print management terminals are configured with automatic image overwrites and daily memory purges to prevent temporary scan/copy data from persisting on local hard drives.

System Maintenance, Asset Management & Disaster Recovery

- Maintenance & Security Patching: Staff perform ongoing maintenance and regular updates on the ILS, server operating systems, and operational software, including scheduled application of security patches.
- Hardware & Software Asset Inventory: IT maintains a documented inventory of all physical computer hardware, mobile devices, and software licenses.

- Backups & Test Restores: Daily and weekly data backups are stored securely off-site and in the cloud. IT performs scheduled test backup restores to verify data integrity and recovery readiness.
- Disaster Recovery Mirroring: Critical server data is mirrored to off-site locations to ensure rapid disaster recovery and continuous system availability.

Records Retention Reference Statement

The creation, handling, storage, retention, and disposition of all library records—across physical, electronic, email, and digital media formats—are governed by the library's

Records Management Policy.

Mandatory POPA Retention Rules

- 1-Year Decision Retention Rule (POPA s. 6(b)): Personal information used to make an operational or administrative decision that directly affects an individual (including decisions made via automated systems) must be retained for at least one (1) year following use. This ensures the affected individual has a reasonable opportunity to request access or correction.
- Prompt Disposal of Non-Decision & Transitory Records: Personal information not used to make a direct decision about an individual, or temporary records that have served their operational purpose, must be securely deleted or shredded in accordance with library disposition procedures.

Proactive Monitoring, Security Testing & Incident Response

- Proactive Log & Threat Monitoring: Information systems holding personal data are continuously monitored to identify unauthorized access attempts and system anomalies. Automated notification tools alert IT staff to potential ransomware attacks or server outages.
- Vulnerability Assessments & Penetration Testing: The library conducts periodic internal and external security threat and risk assessments (STRAs), vulnerability scans, and penetration tests to identify and resolve system weaknesses.

Privacy Management Program

Automated Systems & AI Security Controls

- Input Safeguards: Technical controls ensure that personal, confidential, or sensitive personal information is not entered into generative AI tools or unvetted automated platforms.
- Automated System Auditing: Any automated systems processing patron or operational data are monitored to verify fair performance, prevent algorithmic bias, and ensure appropriate data protection controls remain active.

Video Surveillance & Security Cameras

Statutory Authority & Purpose: Security cameras are operated under Section 4(c) of POPA to document security breaches, ensure facility safety, and protect patrons, staff, and library property.

System Custody & Operational Scope:

- Library-Operated Cameras (Interior): Cameras located inside the library facility are managed by Library IT and the Privacy Officer. Footage is recorded onto local secure Network Video Recorders. Unflagged footage overwrites automatically on a continuous loop.
- City-Operated Cameras (Shared Facility/City Hall): Cameras positioned in shared facility entrances and exterior municipal spaces are owned and operated by City Security under municipal privacy controls.

Incident Export & 5-Year Retention: If a video clip is exported to document a specific incident (such as property damage, theft, a safety breach, or issuing a patron ban), the video file becomes part of the official Incident Report or Suspension File and must be retained for five (5) years alongside written documentation.

- Public Signage & Law Enforcement Disclosures: Prominent collection notices are posted stating the purpose, legal authority, and contact information for the Privacy Officer. Camera footage is disclosed to law enforcement agencies only upon receipt of a court order, warrant, or formal written request approved by the Library Director, or in emergency situations under Section 13(1)(cc) of POPA to avert imminent

danger to health or safety. All disclosures to law enforcement agencies are formally logged and retained.

Role-Based Access Control Protocol

In accordance with POPA Section 12(4) and Ministerial Regulation Section 6(2)(b), access to personal information is restricted to authorized personnel based strictly on "Need-to-Know" and "Minimum Necessary" principles to perform their assigned duties.

Account Management & Credentials

- Unique Authentication: All staff must use individual login credentials and strong passwords; shared logins are prohibited.
- Offboarding**:** Access privileges across all systems (ILS, network drives, email) and physical assets (fobs, keys) are revoked immediately upon departure.

Access Permissions Summary

- Public / Patrons: Restricted to personal account information. Public terminal session data and downloads are automatically purged upon logout.
- Frontline Circulation Staff: Access restricted to patron account and borrowing details necessary to issue cards, manage circulation, and update contact information.
- Program Coordinators: Temporary access to event registration rosters. Files must be securely deleted or shredded within established retention schedules.
- Library Director / Privacy Officer / Admin Coordinator: Full administrative access to personnel records, financial accounts, incident logs, and confidential files.
- Volunteers & Contractors**:** Access is restricted strictly to assigned operational tasks and conditioned on signed confidentiality agreements and role-proportionate training.

Monitoring & Compliance

User access levels and active accounts will be audited periodically. Any unauthorized access to personal records constitutes a privacy breach and will trigger the Privacy Incident Response Procedure.

Privacy Management Program

Section 3. Collection, Accuracy, and Records Retention

Collection Notices & Exceptions Protocol

Mandatory Collection Notice Requirements (POPA s. 5(2))

Unless a statutory exception applies, staff must provide a collection notice either in writing or verbally at or before the time of collecting personal information directly from an individual. Every collection notice must explicitly state:

- Purpose: The specific operational reason for collecting the information.
- Legal Authority: The specific statutory section authorizing the collection (e.g., POPA s. 4(c), *Libraries Act*).
- Contact Information: The title and contact details of the Privacy Officer (Library Director) to whom questions can be directed.
- Automated System Disclosure: Notice if the collected information will be input into an automated software or AI system to make decisions, recommendations, or generate content.

Notice Exceptions (POPA s. 5(3) & 5(4))

A collection notice is **not required** at the time of transaction under the following circumstances:

- **Ongoing or Repeat Collections (s. 5(4)):** Notice was previously provided to the individual and the library continues to collect personal information for the same ongoing purpose and legal authority (e.g., routine borrowing, card renewals, or ongoing program attendance).
- **Authorized Setting Aside of Notice (s. 5(3)):** The Privacy Officer determines that direct collection or notification would result in inaccurate information or defeat the purpose of the collection (e.g., specific security or conduct investigations). Any use of this exception must be formally documented.

Data Accuracy Standard (POPA s. 6(a))

Under Section 6(a) of the *Protection of Privacy Act* (POPA), the library must make every reasonable effort to ensure that personal information relied upon to make a decision that directly affects an individual is accurate and complete.

Operational Standards

- Verification at Collection: Staff must verify factual details (such as names, contact information, or eligibility data) directly with the individual or through reliable source documentation at the time of intake.
- Routine Maintenance: Routine factual updates (such as a patron updating an address or phone number) must be made immediately in library systems without requiring a formal written correction request.
- System & Automated Data Quality: Any personal information processed through automated software, or used to generate derived or non-personal data, must be validated and checked for accuracy and bias mitigation before being relied upon for library decisions

Records Retention & Secure Disposal

Decision-Making Records Retention Standard (POPA s. 6(b))

Mandatory 1-Year Minimum Retention Under Section 6(b) of the *Protection of Privacy Act* (POPA), if personal information is used to make a decision that directly affects an individual (such as exam proctoring verification, conduct suspensions, fee waivers, or employment decisions), the record must be retained for **at least one (1) year** after use. This guarantees the individual a reasonable opportunity to access the record and request a correction if necessary.

Exception for Non-Decision Data The 1-year mandatory retention rule does not apply if no decision—adverse or otherwise—was made about an individual. Records such as raw survey feedback rendered anonymous, transitory phone messages, or unread unsolicited resumes should be securely destroyed or anonymized as soon as their immediate purpose is served.

Privacy Management Program

General Records Retention & Secure Disposal

Core Retention Principle

Personal information must be retained only as long as necessary to fulfill the operational, business, or legal purpose for which it was originally collected. Once the intended purpose has been concluded and no legal retention mandate applies, the information must be securely destroyed or transformed into non-personal data.

Transitory Records Workflow & Data Minimization

To prevent "data sprawl" and mitigate breach risks, temporary files handled during daily operations are classified as transitory records and must be disposed of promptly once the primary document is processed:

- Email Attachments: When personal information (e.g., forms, applications) is received via email, staff must save the file to its network folder and immediately delete the email and clear the deleted items folder.
- Program & Event Rosters: Downloaded spreadsheets or printed sign-up lists must be permanently deleted or shredded as soon as the program concludes and non-personal attendance statistics are recorded.

Authorized Destruction Methods

- Paper Records: Physical files, sign-up sheets, and printed reports containing confidential or restricted data must be disposed directly into locked disposal bins for certified destruction by the contracted service.
- Electronic Records: Digital files must be permanently deleted from local computer drives, shared network folders, cloud storage platforms, and server trash bins.
- Hardware & Photocopiers**:** IT equipment, public workstations, and multifunction copiers must be configured with automatic memory overwrites and session purges upon user logout or at scheduled daily intervals.

Privacy Management Program

Section 4. Disclosure of Personal Information

Disclosure Formats (In Writing or Orally)

In accordance with provincial guidance, disclosure of personal information may occur orally (in person or over the telephone) or in writing (paper records, secure email, or electronic data transfer).

Method Determination & Data Minimization (POPA s. 13(4))

- Method Determination: The Library Director / Privacy Officer determines the most appropriate format for disclosure after evaluating the sensitivity of the information, the relationship with the receiving party, and cost-effectiveness.
- Data Minimization: In accordance with Section 13(4) of POPA, the library must ensure that any disclosure contains only the minimum amount of personal information necessary to achieve the authorized purpose in a reasonable manner.

Statutory Disclosure Authorities (POPA s. 13 & s. 54)

Personal information under library custody or control will not be disclosed to external third parties except under the following specific legal authorities:

- Consistent Purpose (s. 13(1)(b) & s. 14): For the purpose for which the data was originally collected or a purpose with a direct, logical link to operating an authorized library service.
- Consent (s. 13(1)(c) & PPR s. 2): When the individual has provided explicit written or oral consent specifying the information and purpose.
- Legal Orders & Law Enforcement (s. 13(1)(g)/(h)): In response to a subpoena, warrant, court order, or formal written request from a law enforcement agency assisting an active investigation.
- Health & Safety Emergency (s. 13(1)(cc)): Where there are reasonable grounds to believe disclosure will avert or minimize an imminent danger to the health or safety of any individual.
- Guardian of a Minor (s. 54(1)(e)): To a parent or legal guardian of a minor child, provided the minor is not exercising independent privacy rights as a mature minor.

- Next of Kin (s. 13(1)(s)): To contact emergency personnel or next of kin in an emergency or in relation to a deceased individual.

Section 5. Non-Personal Data & Data Matching

Creation of Non-Personal Data (POPA s. 21)

The library is authorized under Section 21(1) of POPA to create non-personal data for the following specific purposes:

- Research and analysis.
- Planning, administering, delivering, managing, monitoring, or evaluating library programs and services.

Custody Requirement

The library will only use personal information or data derived from personal information that is already in its custody or under its control. The library will not collect personal information from another public body to create non-personal data unless it is an authorized collection.

Creation Standards & Requirements

Non-personal data must be created following generally accepted best practices (modifying or anonymizing data to industry standards) and prescribed requirements:

- Quality Assurance: Establishing a process to verify that de-identification methods are effective and cannot be easily reversed (re-identification).
- Bias Mitigation: Implementing procedures to identify and account for potential biases in non-personal datasets so they remain accurate for research and planning.
- Auditability: Documenting creation methods so they are replicable for auditing purposes.

Use & Protection of Non-Personal Data (POPA s. 22; M-Reg s. 5(2))

Unrestricted Internal Use

Unlike personal information, there are no statutory restrictions on how the library uses non-personal data once it has been created.

Re-identification Risk Assessment

Before using or disclosing non-personal data, the library must conduct an assessment confirming to the greatest extent possible that individuals cannot be re-identified, evaluating the level of re-identification risk, and applying measures to reduce that risk.

Security Safeguards

Staff must protect non-personal data through reasonable administrative, physical, and technical security arrangements against unauthorized access, collection, use, disclosure, or destruction.

Data Matching & Data Derived from Personal Information

Data Derived from Personal Information: Data created by merging two or more sources through data matching where the personal information in the resulting dataset remains identifiable. Any collection, use, or disclosure of data derived from personal information must comply with POPA and ATIA rules.

Data matching must strictly comply with prescribed security arrangements.

Section 6. Access to Information Requests & Service Fees

Information Access Rights & Request Paths

- Right of Access: Individuals have a statutory right under the *Access to Information Act* (ATIA) and POPA to request records in the library's custody or under its control.
- Informal Requests: General library policies, public guides, and routine patron account details should be provided informally by frontline staff whenever possible without requiring formal paperwork.

- Formal ATI Requests: If records cannot be provided informally, the applicant must submit a formal ATI request in writing to the Privacy Officer. The request must specify the records sought with sufficient detail and include any applicable initial fee.
- Timelines & Duty to Assist: The library has 30 business days from receiving a complete request to respond. Staff have a legal duty to assist applicants and help clarify or narrow overly broad requests.

Power to Disregard Access Requests

In accordance with ATIA provisions, the Library Director (Head of the Public Body) may disregard a formal access to information request if:

- Operational Disruption or Abuse: Responding would unreasonably interfere with library operations or amounts to an abuse of the right to request (such as repetitive or systematic submissions).
- Abusive or Vexatious: The request is abusive, threatening, frivolous, or vexatious.
- Already Disclosed / Publicly Available: The requested information has already been provided to the applicant or is routinely accessible to the public.
- Overly Broad or Incomprehensible: The request is overly broad, incomprehensible, or remains insufficiently clear to locate records after staff attempt to assist the applicant.

Mandatory Procedure for Disregarding a Request:

1. Written Notification: The Privacy Officer must issue a formal written notice to the applicant explaining the specific grounds for disregarding the request.
2. OIPC Review Rights: The notice must inform the applicant of their legal right to request a review of the decision by the Office of the Information and Privacy Commissioner (OIPC).
3. Substantiating Evidence: The library must document and retain corroborating evidence supporting why the exception was applied in case of an OIPC review

Fee Schedule for Access Requests (ATIA s. 96; ATI Regulation s. 13)

Request Category	Initial Fee	Additional Fees & Rationale
Personal Information Request *(Applicant requesting access to their own personal records)*	**$0.00** *(No initial fee)*	No fees apply unless reproduction/copying costs exceed **$10.00**, in which case actual copying costs above $10.00 are charged.
General Access Request *(Request for non-personal, operational, or business records)*	**$25.00**	Applied to general access requests. Additional fees for searching, redacting, and duplication apply if total processing costs are estimated to exceed **$150.00**. A formal fee estimate is provided prior to commencing work, and a 50% deposit is required.
Continuing Access Request *(Request for ongoing general access over a specified period up to 2 years)*	**$50.00**	Initial fee required at submission. Additional processing costs are charged as information becomes available over the specified term.

Section 7. Operational Rights & Incident Procedures

Correction of Personal Information Procedure

Step One: Receiving the Request (Informal vs. Formal)

- Informal Routine Updates: Patrons and staff are encouraged to update simple factual information (such as changing a phone number or mailing address) directly through authorized library systems, such as their online patron account. Staff at the circulation desk can also make these routine updates immediately without requiring a formal request.

- Formal Correction Requests: If an individual wishes to correct an official record or if the library cannot address the change informally, the individual must submit a formal written request to the library's designated Privacy Officer.

Step Two: Investigation and Timelines

- Mandatory Timeline: Upon receiving a formal written request, the Privacy Officer has exactly 30 business days to process the request, investigate the claim, and provide a written response to the individual.
- Transferring Requests: If the Privacy Officer determines that the personal information in question was originally collected by or belongs to another public body (such as the City of Fort Saskatchewan or a third party vendor), they must transfer the request to that specific public body and notify the individual of the transfer as soon as possible.

Step Three: Assessing Facts vs. Opinions The Privacy Officer must evaluate the requested correction based on the nature of the information:

- Factual Information: Factual data (such as a birth date, legal name, or income information) must be corrected if the individual provides adequate proof that the current record is wrong. When a correction is made, all records containing that specific information must be updated.
- Opinions and Evaluative Records: The library is legally not required to correct professional opinions, subjective assessments, or evaluative records (for example, a staff member's written notes regarding a patron conduct incident or a performance appraisal).
- Statement of Disagreement: If an individual disputes an opinion or if a requested correction is refused, the Privacy Officer must allow the individual to submit a "statement of disagreement". This statement must be formally linked to or annotated on the original record so that anyone reading the file sees the individual's perspective.

Step Four: Notifications

- Notice to the Individual: The Privacy Officer must provide written notice to the individual detailing whether the correction was made, or if an annotation/statement of disagreement was added instead.
- Notice to Third Parties**:** If the library successfully corrects a record, the Privacy Officer must notify any other public bodies or third parties to whom the incorrect information was disclosed within the past year, so they can update their records as well.

Privacy Complaints Procedure

Individuals (patrons, staff, volunteers, or contractors) have the right under POPA to submit a complaint regarding:

- Collection: Improper or unauthorized collection of personal information.
- Use or Disclosure: Unauthorized access, internal use, or external sharing of personal information.
- Safeguarding: Inadequate physical, technical, or administrative security safeguards to protect personal information.

Step One: Intake and Submission

- Internal Review First Requirement: Under POPA section 38(2), complainants are required to submit their concern to the library for an internal review before escalating the matter to the Office of the Information and Privacy Commissioner of Alberta (OIPC).
- Written Submission: Privacy complaints must be submitted in writing directly to the library's designated Privacy Officer. The email address is privacy@fspl.ca
- Required Information: The submission should include the complainant's contact information, specific details of the incident or concern, relevant dates, and the desired resolution to allow staff to investigate.
- Acknowledgement: The Privacy Officer will acknowledge receipt of the complaint in writing within a reasonable timeframe.

Step Two: Investigation

- Role of the Privacy Officer: The Privacy Officer acts as the central investigator, reviewing relevant records, interviewing staff involved, and evaluating whether FSPL complied with POPA and internal privacy policies.
- Evaluating the Allegation: The Privacy Officer will analyze the evidence to make a formal determination:
    - Founded: Personal information was improperly collected, accessed, used, disclosed, or safeguarded.
    - Unfounded: The collection, use, disclosure, or security arrangements were fully authorized and compliant under POPA.
- Breach Escalation: If the investigation reveals that an unauthorized access or disclosure resulted in a privacy breach meeting the "real risk of significant harm" (RROSH) threshold, the Privacy Officer will immediately trigger the Privacy Incident Response Procedure.

Step Three: Response and Remediation

- Mandatory 30-Day Timeline: The Privacy Officer must complete the investigation and provide a comprehensive written response to the complainant within 30 business days of receiving the complaint.
- Written Outcome Notice: The formal written response will outline:
    - The findings of the investigation (whether the complaint was determined to be founded or unfounded).
    - Any corrective or remedial actions implemented to address the issue and prevent future recurrence (such as staff re-training, system access updates, or administrative policy revisions).
- Notice of Appeal Rights: The response must explicitly inform the complainant that if they remain dissatisfied with FSPL's response or decision, they have the right to request a formal review by the Office of the Information and Privacy Commissioner of Alberta (OIPC) under POPA section 37.

Step Four: Recordkeeping and Provincial Tracking

- File Retention: All documentation relating to a privacy complaint (including the initial complaint form, investigation notes, and final written response) must be maintained in a restricted administrative folder for at least 1 year following the final decision.
- Annual Reporting: To comply with annual tracking requirements for the Government of Alberta, the Privacy Officer will record and maintain statistics on:
    - Total number of privacy complaints received.
    - Total number of complaints closed/addressed.
    - Complaint outcomes (number determined to be founded vs. unfounded).

Privacy Incident (Breach) Response Procedure

The immediate steps Fort Saskatchewan Public Library (FSPL) staff and management must take to contain, investigate, assess, and report any privacy incidents to ensure compliance with the *Protection of Privacy Act* (POPA).

Step One: Containment and Internal Reporting (Staff Level)

- Immediate Action: Upon discovering a potential privacy breach, staff must take immediate steps to contain the incident (e.g., locking a computer, attempting to retrieve a misdirected email, or securing physical files) and prevent further harm.
- Escalation: Staff must immediately report the suspected breach to the Library Director/Privacy Officer.

Step Two: Risk Assessment (Privacy Officer)

- **Central Management:** All privacy incidents must be escalated to the Privacy Officer, who acts as the central manager coordinating with necessary IT staff, management, or legal counsel.
- **Assessing Harm:** The Privacy Officer will investigate the incident to determine the scope and evaluate if the breach creates a **"real risk of significant harm" (RROSH)** to the affected individuals.

- **Assessment Tool:** To make this determination, the Privacy Officer will utilize the official *POPA Breach Notice Assessment Tool* provided by the Office of the Information and Privacy Commissioner (OIPC) to evaluate factors like the sensitivity of the data and the probability of misuse.

Step Three: Mandatory Notifications If the Privacy Officer determines that the incident meets the RROSH threshold, the library is legally required to issue notifications **without unreasonable delay**. Notice must be given to:

- The affected individual(s).
- The Information and Privacy Commissioner of Alberta (OIPC).
- The Minister of Technology and Innovation.
- The Library Board.

Step Four: Investigation and Remediation

- **Root Cause Analysis:** The Privacy Officer and relevant department managers will conduct an investigation to determine the root cause of the incident and review the events leading up to the breach.
- **Safeguard Updates:** Following the investigation, the Privacy Officer will review the adequacy of current physical, administrative, and technical safeguards and implement corrective actions or policies to prevent future occurrences.

Step Five: Tracking and Provincial Reporting

- To comply with the Minister's annual reporting requirements to the Legislative Assembly, the Privacy Officer will track all privacy incidents throughout the fiscal year (even those that do not meet the RROSH threshold).
- The tracked data must include the number of incidents, the cause (unauthorized access, disclosure, or loss), the risk level, and the type of incident (e.g., human error, theft, or compromised electronic systems).

Privacy Impact Assessment Workflow

Under Section 26 of the *Protection of Privacy Act* (POPA) and Section 7 of the *Protection of Privacy (Ministerial) Regulation* (M-Reg), the library must complete a Privacy Impact

Privacy Management Program

Assessment (PIA) whenever implementing a new administrative practice, program, project, or service, or making a substantial change to an existing one that involves personal information. A PIA is specifically triggered if one or more of the following apply:

- Significant Harm Risk: The loss, unauthorized access, or unauthorized disclosure of personal information could result in significant harm to an individual.
- High-Sensitivity Data: The initiative involves collecting, using, or disclosing highly sensitive personal information (such as financial details, biometric data, or information respecting minors, seniors, or vulnerable individuals).
- Innovative Technology or AI: The initiative involves the use of automated decision-making systems, artificial intelligence, or innovative technology.
- Data Matching or Integrated Services: The project involves data matching between public bodies or is part of a common or integrated program or service.
- Mandatory OIPC Submission Factors**:** The project meets any of the prescribed submission criteria set out in Section 7(5) of the Ministerial Regulation.

Required PIA Content

In accordance with provincial standards, a completed PIA must document the full lifecycle of the personal information involved and include:

- **Project Summary:** A clear description of the program, tool, or service and its business rationale.
- **Data Inventory & Legal Authority:** The specific types of personal information involved and the statutory sections authorizing the collection, use, and disclosure.
- **Information Flow Diagram:** A visual or detailed map identifying how personal information moves between individuals, internal systems, and external service providers.
- **Risk & Safeguard Assessment:** Identification of potential privacy and security risks paired with specific administrative, physical, and technical safeguards to mitigate those risks.

- **Data Management Controls:** Procedures ensuring data accuracy, routine correction, and compliance with retention schedules.

Privacy Impact Assessment (PIA) Procedure

The purpose of a Privacy Impact Assessment (PIA) is to identify, assess, and mitigate privacy risks when introducing a new, or significantly changing an existing, administrative practice, program, project, or service that involves the collection, use, or disclosure of personal information.

1. When a PIA is Required Staff must notify the Privacy Officer to initiate a PIA whenever the library implements a new, or substantially changes an existing, program, software, or service, and one or more of the following conditions apply:

- The loss of, unauthorized access to, or unauthorized disclosure of the personal information could result in significant harm to the individual.
- The project involves the collection, use, or disclosure of highly sensitive personal information (such as financial data or the personal information of minors).
- The project involves the development or use of innovative technology, automated systems, or artificial intelligence.
- The project is part of a common or integrated program or service shared with another public body.

2. Components of the Assessment The Privacy Officer and IT staff, will complete the PIA using the standardized template provided by the Office of the Information and Privacy Commissioner (OIPC). The completed assessment must comprehensively document:

- A summary of the purpose for collecting, using, or disclosing the personal information.
- The specific types of personal information involved.
- The legal authorities under POPA relied upon for the collection, use, or disclosure.
- The identification of any privacy risks and the mitigation strategies implemented to address them.

- The administrative, technical, and physical safeguards in place to protect the personal information.
- The procedures for ensuring accuracy, handling correction requests, and managing the retention and destruction of the information.

3. Approval and Submission

- **Internal Approval:** Once drafted, the PIA must be reviewed and officially signed off by the Library Director or their authorized delegate.
- **OIPC Submission:** The Privacy Officer will submit a copy of the completed PIA to the Information and Privacy Commissioner if the project meets the specific submission criteria outlined in Section 7(5) of the Ministerial Regulation, or if specifically requested by the Commissioner.

4. Retention Completed PIAs and their supporting documentation (such as service provider agreements) will be retained for the entire lifespan of the related tool or program, or for a minimum of six years, to ensure ongoing accountability and compliance.

Privacy Management Program

Appendix A: Delegation of Authority Table

Delegation Authority Table

Statutory Reference: *Protection of Privacy Act* (SA 2024, c P-28.5), Section 55

Effective Date: June 11, 2026

Statement of Delegation

In accordance with Section 55(1) of the *Protection of Privacy Act* (POPA), the Head of a public body may delegate in writing any power, duty, or function of the Head under POPA or its regulations to any person, except the power to delegate under Section 55.

The delegations set out in the tables below assign operational privacy management responsibilities to the position of **Library Director / Privacy Officer**. In the absence or incapacitation of the Library Director, these delegated powers shall temporarily transfer to the designated Acting Library Director.

DELEGATION TABLE I: STATUTORY POWERS, DUTIES, AND FUNCTIONS UNDER POPA AND REGULATIONS

Duty, Power, or Function	**POPA / Regulation Reference**	**Retained by Head**	**Delegated to Privacy Officer**
Collection, Correction, and Protection of Personal Information			
Authority to set aside direct collection requirements	s. 5(3), (4)		**X**
Authority to decide on formal requests for correction of personal information	s. 7(1)		**X**
Duty to correct, annotate, or link personal information and notify previous recipients	s. 7(3), (4)		**X**

Duty to give written notice to an individual requesting correction	s. 7(7)	**X**
Authority to transfer a request for correction to another public body	s. 8	**X**
Duty to ensure protection of personal information by making reasonable security arrangements	s. 10(1); M-Reg s. 2, 3	**X**
Duty to give notice of a privacy breach (RROSH) to affected individuals, the OIPC, and the Minister	s. 10(2); M-Reg s. 4	**X**
Duty to ensure protection of data derived from personal information	s. 20	**X**
Duty to ensure protection of non-personal data	s. 24	**X**
Use and Disclosure of Personal Information		
Establishing rules and procedures for electronic consent	PPR s. 2(4)(a)	**X**
Establishing rules and procedures for oral consent	PPR s. 2(5)(a)	**X**
Authority to disclose personal information to the guardian of a minor	s. 54(1)(e)	**X**
Authority to disclose personal information to a relative or adult interdependent partner of a deceased individual	s. 13(1)(s)	**X**

Privacy Management Program

Authority to disclose personal information to avert an imminent danger to health or safety	s. 13(1)(cc); PPR s. 1(1)(b)		**X**
Authority to approve conditions for research and statistical disclosures / research agreements	s. 15		**X**
Privacy Impact Assessments (PIAs)			
Duty to complete, sign off on, and submit Privacy Impact Assessments (PIAs)	s. 26; M-Reg s. 7		**X**
Reviews and Complaints			
Authority to request advice from the Information and Privacy Commissioner	s. 28(1)		**X**
Authority to require the Commissioner to examine original records on-site	s. 29(4)		**X**
Right to make representations to the Commissioner during an inquiry/review	s. 41(6), (8)		**X**
Duty to comply with an Order issued by the Commissioner	s. 44		**X**
General & Administrative Provisions			
Power to delegate under Section 55 *(Statutorily non-delegable)*	**s. 55(1)**	**X** *(Head)*	*(Cannot be delegated)*
Duty to publish and maintain the Personal Information Bank (PIB) directory	s. 57(2), (5)		**X**
Duty to record uses or disclosures of personal information not included in the directory	s. 57(4)		**X**

DELEGATION TABLE II: ADMINISTRATIVE RESPONSIBILITIES UNDER POPA AND REGULATIONS

Duty, Power, or Function of Public Body	POPA / Regulation Reference	Retained by Head	Delegated to Privacy Officer
Collection, Accuracy, and Retention			
Establishing operational controls over collection, use, and disclosure	M-Reg s. 2(a)		**X**
Authorizing routine corrections of personal information (e.g., patron account updates)	M-Reg s. 2(b)		**X**
Ensuring authorized legal purpose for all personal information collections	s. 4		**X**
Assuring proper collection methods and provision of collection notices	s. 5		**X**
Assuring accuracy and completeness of personal information	s. 6(a)		**X**
Applying records retention and secure disposal standards	s. 6(b)		**X**

Formal Execution

Approved by: Rwall

Library Director (acting as Head of Public Body)

Date: June 11, 2026

Privacy Management Program

Appendix B: Personal Information Bank Directory

In accordance with Section 57(2) of the Protection of Privacy Act (POPA), this directory identifies the personal information banks maintained by the Fort Saskatchewan Public Library. All personal information listed in this directory is retained and disposed of in accordance with POPA Section 6(b) (minimum 1-year retention for decision-making records) and the Library's Records Retention Schedule.

Patron and Public Services Records

Registered Borrower/Patron Records

- **Maintained By:** All Staff
- **Individuals:** Library Cardholders
- **Location:** ILS secure cloud server, local secure server
- **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, identification, parent/guardian info, guarantor, type of membership, date record modified, expiry date, barcode number, and current items checked out.
- **Use:** To issue library cards, manage accounts, notify customers about holds/overdues/lost and damaged charges, and collect outstanding fees. Parent/guardian information only if the cardholder is a minor.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c); Libraries Act

Online Account Records

OverDrive/Libby Account Records

Privacy Management Program

NOTE: The library simply acts as an authentication gateway (where patrons log in with their barcode/PIN) and staff cannot log into an administrative dashboard to view, manage, or edit an individual patron's profile or history on those platforms, we do not have custody or control of that data.

- **Maintained By:** Collections Management Coordinator and OverDrive Staff
- **Individuals:** Users who register an account with OverDrive/Libby
- **Location:** Third party cloud servers
- **Information that may be contained:** Name, library card number, email address, items checked out, holds, borrowing history, and device information.
- **Use:** Allows customers to borrow, download, and place holds on digital materials (e-books, audiobooks, and magazines).
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c); Libraries Act

Hoopla Account Records

- **Maintained By:** Collections Management Coordinator and Hoopla Staff
- **Individuals:** Users who register an account with Hoopla
- **Location:** Third party cloud servers
- **Information that may be contained:** Name, library card number, email address, account password/PIN, borrowed items (movies, music, audiobooks, e-books, comics, and TV shows), borrowing history, and device information.
- **Use:** Allows customers to borrow, stream, and download digital media (movies, music, audiobooks, e-books, comics, and TV shows).
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c); Libraries Act

Bibliocommons Account Records

- **Maintained By:** Director and Bibliocommons Staff
- **Individuals:** Users who register a username with Bibliocommons

- **Location:** Third party server
- **Information that may be contained:** Name, month of birth, year of birth, email address, library card number, items charged out, current holds, cancelled and expired holds (six months only), borrowing history (six months only and is user opt-in model), preferred hold pickup location, Bibliocommons username, customer-generated lists, comments, and ratings.
- **Use:** Allows customers to place holds, renew materials, pay fines, renew memberships, and participate in online services.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c); Libraries Act.

ME Libraries / Reciprocal Borrowing Records

- **Maintained By:** Front Desk Staff / IT Team
- **Individuals:** Library patrons who register for ME Libraries or Alberta Wide Borrowing to use other library systems
- **Location:** ME Libraries provincial servers / Integrated Library System (ILS)
- **Information that may be contained:** Name, library barcode, PIN/password, home library identification, address, email address, and phone number.
- **Use:** To administer reciprocal borrowing programs and exchange required customer information with other library systems to facilitate cross-jurisdictional borrowing.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c); Libraries Act.

Interlibrary Loans (ILL)

- **Maintained By:** Library ILL staff member, Provincial network server
- **Individuals:** Library Patrons who request ILL items
- **Location:** Provincial Interlibrary Loan Network Servers, Integrated Library System (ILS)
- **Information that may be contained:** Name, address, phone number, email address, library card number, interlibrary loan items or library material purchase requested.

- **Use:** To manage Interlibrary Loan Services and library material purchase requests.
- **Legal Authority:** POPA, section 4(c)

Print Disabled Services

- **Maintained By:** Collections Management Coordinator and third party staff
- **Individuals:** Library Patrons who qualify for print disabled services
- **Location:** Third party servers, ILS
- **Information that may be contained:** Name, address, phone numbers, and contact person.
- **Use:** CELA and NNELS registration for members of the public that qualify for print disabled services.
- **Legal Authority:** POPA, section 4(c)

Program and Services Registrations

LibCal Program Registration Records

- **Maintained By:** Program Coordinator and Third party Staff
- **Individuals:** Members of the public who register for or attend library programs and events.
- **Location:** Third party cloud servers and local secure library server
- **Information that may be contained:** Full name, email address, phone numbers, custom event-specific questions, communication transaction logs (reminder emails, waitlist alerts, SMS notifications), and system logs (IP addresses, timestamps, browser types).
- **Use:** To administer library programming, manage event attendance and waitlists, send automated event reminders, and generate anonymized historical attendance metrics.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c)

Resume Tutor and Tech Help Records

- **Maintained By:** All staff
- **Individuals:** Library patrons and members of the public participating in Tech Help and Resume Tutor programs.
- **Location:** Local secure server
- **Information that may be contained:** Person's name, phone number, email address, and library card status.
- **Use:** To administer and manage attendance for adult learning programs (Tech Help, Resume Tutor), and to generate anonymized historical attendance and demographic metrics to share with community partners (e.g., CALLS).
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c).

Computer and Print Management

- **Maintained By:** IT Team
- **Individuals:** Patrons who login to public computers, Wi-Fi, or printing/scanning/faxing services
- **Location:** Third party cloud server
- **Information that may be contained:** Customer name, library card number, station used, date/time of use, length of session, email address, and temporary document scans.
- **Use:** Public computer use, print/scan management, and generating usage reports.
- **Legal Authority:** POPA, section 4(c)

3D Print Requests

- **Maintained By:** IT Team
- **Individuals:** Patrons submitting 3D print files.
- **Location:** Third party server and third party ticket system, Email (transitory files)

- **Information that may be contained:** Customer name, email address, library card number, and 3D design files.
- **Use:** To communicate with patrons regarding their 3D print submissions, provide cost estimates, and coordinate pickup.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c).

Equipment Waivers

- **Maintained By:** Library Staff
- **Individuals:** Library patrons completing waivers to use specialized library equipment (e.g., sewing machines).
- **Location:** Third-party cloud servers
- **Information that may be contained:** Full name and library card number.
- **Use:** To administer access to specialized library equipment and obtain patron agreement to safety, liability, and usage guidelines.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c).

Room Bookings

- **Maintained By:** Program Coordinator
- **Individuals:** Businesses, Community Organizations, and members of the public who book library rooms
- **Location:** Local secure server
- **Information that may be contained:** Name, phone number, email address, and purpose of meeting.
- **Use:** To administer shared use of library rooms, obtain room agreements, create signage, and contact organizers.
- **Legal Authority:** POPA, section 4(c)

Privacy Management Program

Customer Newsletters/Email Lists

- **Maintained By:** Library staff member, Third party staff
- **Individuals:** Library Patrons who have signed up to receive e-newsletters
- **Location:** Third party server, local drive (transitory record)
- **Information that may be contained:** Subscriber name, email address.
- **Use:** To distribute issues of various library newsletters and event notifications. To track subscription additions.
- **Legal Authority:** POPA, section 4(c)

Contest and Draw Entries

- **Maintained By:** Event staff and Third party staff
- **Individuals:** Community members entering contests
- **Location:** Secure draw box, Beanstack cloud servers
- **Information that may be contained:** Name, address, phone number, email addresses.
- **Use:** To manage contest and draw forms for library promotions.
- **Legal Authority:** POPA, section 4(c)

Patron Correspondence/Feedback

- **Maintained By:** Lead Team
- **Individuals:** Library Patrons who correspond with the library
- **Location:** local secure server, local website database
- **Information that may be contained:** Name, address, phone number, email address, library card number, comment, complaint, or reference question, reading preferences.

- **Use:** Responding to customer comments, reference questions, complaints, evaluation forms, and purchase suggestions/reconsideration requests. Personalized reading lists at patron's request.
- **Legal Authority:** POPA, section 4(c)

Photo Permission/Promotional Releases

- **Maintained By:** Marketing Coordinator and third party staff
- **Individuals:** Library Patrons who have provided photo permission or promotional release forms
- **Location:** Local secure server and third party server
- **Information that may be contained:** Name, email address, phone number, likeness description (photos), comments about the library, and reviews of library materials.
- **Use:** Names of people who have given the library their permission to use their names, pictures, or quotes in promotional materials, reports, or for public relations.
- **Legal Authority:** POPA, section 4(c)

Overdue Notices and Collections

- **Maintained By:** Library Director
- **Individuals:** Customers who have outstanding fees
- **Location:** local secure server, third party server
- **Information that may be contained:** Name, mailing and email addresses, telephone number, birth date, amount owed, library membership number, payment records, and notification of bankruptcy.
- **Use:** To collect outstanding accounts, recover overdue materials, and administer fee removal/bankruptcy proceedings or data sent to third-party collection agencies.
- **Legal Authority:** POPA, section 4(c); Libraries Act

Privacy Management Program

Incident Reports (Patrons)

- **Maintained By:** Library Director
- **Individuals:** Library Patrons involved in accidents or incidents at the library
- **Location:** Local secure server
- **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, parent/guardian name and circumstances of incident.
- **Use:** To record patron incident reports for behaviour that breaches the code of conduct, property damage, and health and safety incidents. Issuing library ban/trespass notice/suspension. This information may be disclosed to law enforcement in accordance with library policy and legislation.
- **Legal Authority:** POPA, section 4(c)

Suspensions/Bans

- **Maintained By:** Library Director and Enforcement staff
- **Individuals:** Currently suspended customers
- **Location:** Local secure server
- **Information that may be contained:** Name, physical description, photograph, address, incident type, and suspension length.
- **Use:** Communicating suspended customers to library staff, issuing trespass notices, and suspensions.
- **Legal Authority:** POPA, section 4(c); Libraries Act

Security Camera Footage

- **Maintained By:** IT Team, City Hall IT Team
- **Individuals:** Library Patrons and Members of the Public

- **Location:** Local secure Network Video Recording servers
- **Information that may be contained:** Video recordings of the interior and exterior of the library.
- **Use:** To support documentation of security incidents and monitor the safety of the facility.
- **Legal Authority:** POPA, section 4(c)

Access to Information/Privacy Requests

- **Maintained By:** Library Director
- **Individuals:** Individuals who have formally requested access to information or correction of records
- **Location:** Local secure server
- **Information that may be contained:** Name of the person submitting the request, address, telephone number, email address, copy of identification, request submitted, and correspondence, and copies of requested records found and provided to the requestor.
- **Use:** To respond to access to information/privacy requests and maintain a record of responses, and compile statistics required by the Minister or the OIPC for reviews.
- **Legal Authority:** POPA, section 4(c); POPA section 6

Exam Proctoring Records

- **Maintained By:** Proctoring Staff
- **Individuals:** Patrons requesting proctoring services
- **Location:** Local secure server
- **Information that may be contained:** Name, contact information (phone number, email address), student ID number, course/exam details, and correspondence with the institution.
- **Use:** To administer exam proctoring services and verify student identity.

- **Legal Authority:** POPA, section 4(c)

Local Artist Gallery Agreements

- **Maintained By:** Art Gallery coordinator
- **Individuals:** Local artists displaying and selling their artwork in the library.
- **Location:** Local secure server
- **Information that may be contained:** Artist name, contact information (phone number, email address, mailing address), signature, artwork inventory/descriptions, and pricing details.
- **Use:** To administer the library's art gallery space, coordinate exhibition schedules, obtain the artist's agreement to liability and display terms, and facilitate contact for potential sales.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c).

Employee and Staff Records

Employee Personnel Files

- **Maintained By:** Library Director / Administrative Coordinator
- **Individuals:** Current and former library employees.
- **Location:** Local secure server, locked file cabinet
- **Information that may be contained:** Name, contact information, Social Insurance Number (SIN), birth date, resumes, job classifications, performance appraisals, discipline records, training certificates, and criminal record/vulnerable sector checks.
- **Use:** To support administrative, staff scheduling, performance management, training, and payroll functions of library employment.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c); Employment Standards Code.

Privacy Management Program

Employment Applicant Records

- **Maintained By:** Library Director / Administrative Coordinator
- **Individuals:** Individuals applying for employment at the library.
- **Location:** Locked file cabinet and local secure server
- **Information that may be contained:** Name, contact information, resumes, cover letters, reference information, and interview notes.
- **Use:** To manage the recruitment, screening, and selection process for library vacancies.
- **Legal Authority**: Protection of Privacy Act (POPA), section 4(c)

Payroll and Benefits Records

- **Maintained By:** Library Director / Admin coordinator and the City of Fort Saskatchewan Payroll Department.
- **Individuals:** Current and former library employees.
- **Location:** Locked file cabinet, local secure server, and third party server
- **Information that may be contained:** Earnings, time sheets, tax forms (TD1/T4s), source deductions, direct deposit information, and leave/attendance tracking.
- **Use:** To process and manage staff payroll, administer benefits, track employee leave and attendance, issue federal tax forms, and coordinate direct deposits with the City payroll department.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c); Employment Standards Code; Income Tax Act.

Employee Medical Files & WCB Records

- **Maintained By:** Library Director / Admin Coordinator
- **Individuals:** Current and former library employees who have submitted medical documentation or filed WCB claims.

- **Location:** Local secure server, provincial WCB reporting portals, and secure physical files (locked cabinet).
- **Information that may be contained:** Name, contact information, birth date, gender, incident reports, details of workplace injuries, WCB claim details, doctors' notes, medical leave documentation, and return-to-work treatment plans.
- **Use:** To manage employee benefits and medical leaves, administer return-to-work programs, and comply with Alberta Occupational Health and Safety (OHS) and Workers' Compensation Board (WCB) reporting requirements.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c); Workers' Compensation Act.

Employee Schedules

- **Maintained By:** Library Director and Admin Coordinator
- **Individuals:** Current and former library employees (and volunteers, if scheduled through the software).
- **Location:** local secure server, third party server
- **Information that may be contained:** Employee name, assigned shifts, work unit/department, staff availability, and time-off/shift-trade requests.
- **Use:** To manage library service provision, ensure adequate staff coverage, and manage daily operational workflow.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c).

Employee Relations and Dispute Files

- **Maintained By:** Library Director / City Human Resources Staff/ Admin Coordinator
- **Individuals:** Current and past employees involved in workplace investigations, labour relations issues, or disputes.
- **Location:** Locked file cabinet, local secure server

- **Information that may be contained:** Employee name, employee number, copies of disciplinary action, research, background information, notes from fact-finding or investigations, grievance documentation and resolutions, and correspondence between the employer and employee.
- **Use:** To document and manage specific employee relations situations, fact-finding investigations, and disputes related to the discipline, suspension, or dismissal of an employee.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c); Employment Standards Code.

Employee Contact Lists / Active Directory

- **Maintained By:** Library Director/Admin Coordinator
- **Individuals:** Current library employees
- **Location:** Local secure server, physical printed lists located at various staff service desks.
- **Information that may be contained:** Employee name, job title, department/service point, work email address, work phone number, and internal extension. (Note: These lists strictly contain internal work contact information and do not include private home phone numbers or personal email addresses).
- **Use:** To manage network logins, maintain the internal staff directory (Outlook/Teams), facilitate internal communication, and coordinate daily operations across different service desks.
- **Legal Authority: Protection of Privacy Act (POPA), section 4(c).**

Help Desk / Work Orders

- **Maintained By**: Library IT Staff, Library Management, and the City of Fort Saskatchewan Facilities Department.
- **Individuals:** Current library employees who report IT issues or facility maintenance concerns.

- **Location:** Third-party vendor cloud servers and the City of Fort Saskatchewan's facility management servers. *(Note: The library does not maintain local, in-house copies of these records).*
- **Information that may be contained:** Employee name, work email address, work phone number, service point/location, and the specific details of the facility or technology issue to be resolved,
- **Use:** To manage, track, and troubleshoot IT support tickets and facility maintenance requests submitted by library staff,
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c).

Security Access Control

- **Maintained By:** Administrative Coordinator and the City of Fort Saskatchewan Facilities/Security Department.
- **Individuals:** Current and former library employees, contractors, and volunteers who have been issued physical keys, security fobs, or access cards.
- **Location:** Local secure server, City of Fort Saskatchewan's access control software/servers
- **Information that may be contained:** Individual's name, specific key or fob identification numbers issued, and electronic access logs (dates and times of entry/exit to the facility).
- **Use:** To manage and track authorized security access to restricted staff spaces, and to maintain the physical security safeguards of the facility.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c).

Work Experience Records

- **Maintained By:** Library Director and Administrative Coordinator
- **Individuals:** Students participating in temporary work experience, practicums, or job shadow placements at the library.
- **Location:** Local secure library network and secure physical files (locked cabinet).

- **Information that may be contained:** Student name, contact information, emergency contacts, school or program details, applications/resumes, evaluations, and logs of hours worked.
- **Use:** To manage, coordinate, and evaluate temporary student placements.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c).

Board, Volunteer and Community Records

Library Board Member Records

- **Maintained By:** Library Director / Administrative Coordinator
- **Individuals:** Current and former Library Board Trustees.
- **Location:** Local secure library network, third party cloud server, Government of Canada servers.
- **Information that may be contained:** Name, contact information (home address, personal phone numbers, email address), birth date, terms served, offices or committees held.
- **Use:** To manage contact information, facilitate board communication and governance duties, fulfill annual reporting requirements to the Public Library Services Branch (PLSB), and process board compensation, tax forms, and WCB coverage.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c); Libraries Act; Income Tax Act.

Volunteer Records

- **Maintained By:** Library Director / Admin Coordinator
- **Individuals:** Current, former, and prospective library volunteers.
- **Location:** Local secure server

- **Information that may be contained:** Name, contact information (home address, phone numbers, email address), emergency contact information, volunteer applications/resumes, schedules, logs of hours worked, skills, reference information, and police information/vulnerable sector checks (if applicable to the position).
- **Use:** To select, screen, and manage the library's volunteers; track completed hours for annual reporting; and contact individuals regarding volunteer activities.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c).

Donor Records and Gift History

- **Maintained By:** Library Director / Administrative Coordinator/ Marketing Coordinator
- **Individuals:** Individuals, community groups, and businesses who have made financial or in-kind donations to the library.
- **Location:** Local secure server, secure physical files (locked cabinet), and third party servers.
- **Information that may be contained:** Name, contact information (home address, phone numbers, email address), donation amounts and gift history, correspondence, special requests or circumstances, and copies of charitable tax receipts.
- **Use:** To process and track donations, correspond with prospective and current donors, administer donor appreciation and recognition activities, and generate charitable tax receipts.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c); *Income Tax Act*.

Vendor and Contractor Records

- **Maintained By:** Library Director / Admin Coordinator and City Financial Staff

- **Individuals:** Individuals, service providers, program presenters, and businesses who provide goods or services to the library.
- **Location:** Local secure server
- **Information that may be contained:** Name, company name, contact information (business address, phone numbers, email address), GST number, banking/direct deposit information, invoices, payment history, contract details, and police information/criminal record checks (if applicable to the specific contractor position).
- **Use:** To manage vendor and contractor agreements, procure library equipment or services, and issue payments or honorariums.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c); *Income Tax Act*.

Community Contacts and Stakeholders

- **Maintained By:** Various Library Staff and Lead Team
- **Individuals:** Media contacts, government personnel, community partners, and representatives of businesses or organizations used for library business.
- **Location:** Local secure server.
- **Information that may be contained:** Name, organization/company name, mailing address, email address, telephone numbers, and partnership agreements.
- **Use:** To manage community partnerships, carry out partnered programming and services, distribute correspondence, and make contact as required.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c).

Grant Applications

- **Maintained By:** Library Director / Administrative Coordinator

- **Individuals:** Current or prospective library employees (such as summer students), community partners, and volunteers whose personal information is included in grant submissions.
- **Location:** Local secure server.
- **Information that may be contained:** Name, contact information, resumes/qualifications, and specific details of the staff, students, or community members involved in the funded project.
- **Use:** To apply for, administer, evaluate, and fulfill final reporting requirements for municipal, provincial, federal, or foundational grant funding.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c).

General Financial and Accounting Records

- **Maintained By:** Library Director, Admin Coordinator, IT Team, and the City of Fort Saskatchewan Finance Department.
- **Individuals:** Individuals, employees, contractors, and businesses who have conducted financial transactions with the library, or whose personal information is included in financial documentation.
- **Location:** Local secure server and the City of Fort Saskatchewan accounting systems. *(Note: External auditing firms are granted temporary access for the annual audit)*.
- **Information that may be contained:** Accounts payable and receivable, expense claims, bank statements, records of deposits, cancelled cheques, and invoices that contain personal names or business details.
- **Use:** To manage the library's day-to-day accounting, process payments and receivables, maintain banking arrangements, and facilitate the mandatory annual financial audit by external auditors.
- **Legal Authority:** Protection of Privacy Act (POPA), section 4(c); *Income Tax Act*

Privacy Management Program

Policies and Additional Resources

Artificial Intelligence and Automated System Use Policy

Confidentiality of User Records Policy

Privacy Management Policy

Records Management Policy

ATIA Legislation

Alberta Access to Information Requests

Office of the Information and Privacy Commissioner

Protection of Privacy Act