

Privacy Management Program

TOPIC: Records Management and Privacy

PASSED: August 4, 2026

AMENDED:

REVIEWED:

NEXT REVIEW: June 2029

1. Purpose

Camrose Public Library (CPL) is governed by the Protection of Privacy Act (POPA) of Alberta and is committed to the privacy of personal information that is in the custody or control of the Library. CPL will only collect personal information if the information is necessary for employment records and purposes, an operating program, or activity of the library. CPL will only use information for the purpose it was collected for. CPL will only share information when authorized or required by law.

Under POPA, you have the right to request access to your personal information. You have the right to request corrections to your personal information. You can ask questions about how your information is collected or used, and you can make a complaint if you believe your privacy has been compromised.

Library employees and volunteers will not inappropriately disclose any private information gathered in the due course of their employment. CPL will make its Privacy Management Program available upon request. The Privacy Management Program will be reviewed every 3 years.

2. Definitions

- 2.1 **Artificial Intelligence (AI) System** – A system that uses input data to generate outputs such as predictions, recommendations, or content.
- 2.2 **Automated System** – A system or process that uses computation to support or inform decision-making.
- 2.3 **Custody** – The care and possession of such personal information that is in the possession of the Camrose Public Library.
- 2.4 **Collection Notice** – A statement provided to individuals at the time of collecting personal information, explaining the purpose of collection, the legal authority for collection, and contact information for questions.
- 2.5 **Consent** – Voluntary agreement by an individual for the collection, use, or disclosure of their personal information. Consent may be written, electronic, or



verbal, provided it meets the requirements of the Protection of Privacy Act (POPA) and Library policy.

- 2.6 **Control** – The management, restriction, regulation, administration of use, disclosure or disposition of personal information held by Camrose Public Library.
- 2.7 **Formal Access Request** – A request for access to information or records that are not routinely disclosed and cannot be provided through existing procedures.
- 2.8 **Informal Access Request** – A request for access to your own personal information or information of another person for whom you have proof of authority to act on their behalf.
- 2.9 **Personal Information** – Any information about an identifiable individual, including but not limited to name, address, email, race, nationality, religious or political beliefs, age, sex, gender, marital status, identifying numbers (such as Driver's License or Social Insurance Number), health information, employment history, financial information, photographs, and opinions from or about an individual.
- 2.10 **Privacy Breach** – Any occurrence of unauthorized access to, collection, use, or disclosure of personal information.
Unauthorized access includes:
 - 2.10.1 Access by the public where there is no right to access;
 - 2.10.2 Access by a Library employee who does not need the information for their duties;
 - 2.10.3 Storage of information in an unsecured manner that allows unauthorized access.
- 2.11 **Privacy Impact Assessment (PIA)** – A process used to identify and mitigate privacy risks when introducing new or significantly changed programs, projects, or services that involve personal information.
- 2.12 **Privacy Management Program** – A documented framework of policies, procedures, and safeguards established by the Library to meet its obligations under POPA, including training, incident response, and privacy controls.
- 2.13 **Privacy Officer** – The individual designated by the Library Board or Library Director to oversee compliance with the Privacy Management Program and the Protection of Privacy Act, including handling privacy breaches, training, and responding to access requests.
- 2.14 **Privacy Training** – Mandatory training that ensures individuals understand their obligations under POPA regarding the collection, use, disclosure, and safeguarding of personal information.
- 2.15 **Record** – Any recorded information, regardless of medium or format, created or received in the course of business. Records include, but are not limited to, emails, registrations, waivers, database entries, sticky notes, photographs, and video recordings.



3. Legislative and Policy Authorities

- 3.1 [Alberta Access to Information Act](#) (ATIA)
- 3.2 [Alberta Protection of Privacy Act](#) (POPA)
- 3.3 [Alberta Protection of Privacy \(Ministerial\) Regulation](#) (PPMR)
- 3.4 [Alberta Libraries Act](#) (ALA)
- 3.5 [Alberta Libraries Regulations](#) (ALR)
- 3.6 [Alberta Employment Standards Code](#) (AESC)
- 3.7 [Canada Income Tax Act](#) (CITA)

4. Designation of a Privacy Officer

PPMR - Section 6(1)a

- 4.1 As a public body under the Protection of Privacy Act (POPA), the Board allows access to its records while ensuring the protection of the privacy of individuals' personal information. The Board designates the Library Director as the Head, in accordance with POPA. The Head may delegate specified responsibilities under the Act.
- 4.2 The Privacy Officer will:
 - 4.2.1 Manage the Library's Privacy Management Program.
 - 4.2.2 Act as contact for complaints, access, and correction requests. Oversee incident reporting, PIAs, and compliance monitoring.
 - 4.2.3 Ensure timelines, documentation, and notifications comply with POPA.
 - 4.2.4 Ensure the implementation and maintenance of mandatory privacy training.

5. Correction of Personal Information

POPA - Section 7

- 5.1 An individual who believes there is an error or omission in their personal information held by CPL may request that their information be corrected, in accordance with guidelines outlined in Section 7 of POPA.
- 5.2 This applies to all personal information about identifiable individuals held by CPL, whether in paper or electronic form. It also applies to individuals who request a correction of their own personal information, or who are authorized to act on behalf of another individual.
- 5.3 Some personal information collected by CPL is stored or managed through Parkland Regional Library System (PRLS). Where personal information is held by PRLS, CPL will assist the individual in directing their correction request to PRLS.
- 5.4 CPL is not required to correct opinions, professional judgments, or evaluative records. Individuals may request that a statement of disagreement be added to the record in accordance with POPA.



- 5.5 Individuals have the right to seek a review by the Office of the Information and Privacy Commissioner if they are dissatisfied with how a correction request was handled.

6. Notification of Incident or Loss of Personal Information

POPA Section 10(2)

- 6.1 If an incident occurs involving the loss of, unauthorized access to, or unauthorized disclosure of personal information in CPL's custody where there is real risk of significant harm to an individual as a result of that loss, CPL will give notice to:
- 6.1.1 The individual
 - 6.1.2 CPL's Privacy Officer
 - 6.1.3 The Library Board
 - 6.1.4 The Commissioner
 - 6.1.5 The Minister
- 6.2 An individual who believes there is an error or omission in their personal information held by CPL may request that their information be corrected, in accordance with guidelines outlined in Section 7 of POPA.
- 6.3 This applies to all personal information about identifiable individuals held by CPL, whether in paper or electronic form. It also applies to individuals who request a correction of their own personal information, or who are authorized to act on behalf of another individual.

7. Privacy Complaints

POPA Section 38(2)

- 7.1 Privacy complaints must be submitted in writing or electronically to the Library's Privacy Officer and should include sufficient detail to allow the complaint to be understood and investigated.
- 7.2 CPL will acknowledge receipt of a privacy complaint within a reasonable timeframe.
- 7.3 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.
- 7.4 The complainant will be informed in writing of the outcome of the investigation and any corrective actions taken, where appropriate.
- 7.5 If a 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 under POPA.
- 7.6 If a complaint regarding personal information about an individual has been received by CPL, a request for review cannot be delivered to the Commissioner



unless CPL does not respond to the complaint within 30 business days of receiving the complaint.

8. Creation, Use, and Disclosure of Personal and Non-Personal Information

PPMR Section 6(1) ii

- 8.1 CPL may create and use non-personal data, in compliance with POPA.
- 8.2 CPL uses personal information for the following purposes:
 - 8.2.1 The provision, delivery, management, and communication of library services, including, but not limited to, issuing library cards, purchasing and circulating materials, handling patron complaints, collecting fees, handling facility booking requests, and issuing suspensions.
 - 8.2.2 Evaluating, planning and improving services.
 - 8.2.3 Employment, volunteer, contraction and donor administration.
 - 8.2.4 Library fundraising.
 - 8.2.5 To advocate for library services to stakeholders.
 - 8.2.6 As otherwise allowed by law.
- 8.3 CPL does not disclose personal information, except for the following purposes:
 - 8.3.1 In response to a subpoena or court order.
 - 8.3.2 When there are reasonable grounds to believe that the disclosure will avert or minimize an imminent danger to the health and safety of any person, or a risk of harm to the health and safety of a minor.
 - 8.3.3 To contact the next of kin or emergency response personnel in case of an emergency.
 - 8.3.4 When a formal information-sharing agreement is in place between the Library and a third party.
 - 8.3.5 Otherwise, as required by law.

9. Records Retention and Disposal

POPA Part 3 (18) and (20)

- 9.1 Provisions for the protection and retention of data:
 - 9.1.1 The Library will use reasonable measures to protect against the risk of unauthorized access, collection, use, disclosure or disposal of personal information.
 - 9.1.2 The Library applies technological, physical, administrative, and operational safeguards appropriate to the nature and format of personal information.
 - 9.1.3 The Library will take reasonable steps to ensure the personal information it holds is accurate, complete, and up to date.



- 9.1.4 The Library will retain the personal information it collects for as long as it is needed for the purpose for which it was collected. Once it is no longer required, it will be destroyed.

10. Privacy Management Training Program

PPMR Section 6(1) d and e

- 10.1 CPL staff, contractors, consultants, volunteers, students, trustees and appointees or service providers acting on behalf of the Library will be trained annually regarding their responsibilities under POPIA. Privacy training will be proportionate to an individual's role.
- 10.2 Privacy training is mandatory, and must be completed during onboarding and before being granted access to personal information, and annually thereafter. Material changes to the legislation, policies, procedures, or identified privacy risks will also result in training.
- 10.3 Completion of privacy training will be documented.
- 10.4 The Library Privacy Management Program will be reviewed and updated, if needed, every three years.

11. Security Classification System

PPMR Section 6(1) c

- 11.1 High-sensitivity information is defined in the (Ministerial) Regulations to include personal information related to biometric, financial, or personal information regarding a minor, senior, or vulnerable individual. Any high-sensitivity information will be protected with additional safeguards.

12. Privacy Impact Assessments

PPMR Section 7(1)

- 12.1 CPL will conduct a Privacy Impact Assessment (PIA) whenever there is a new or changed administrative practice, program, project, or service that will involve the collection, use, or disclosure of personal information if one or more of the following apply:
- 12.1.1 The loss of personal information could result in significant harm
- 12.1.2 One or more of the factors requiring the submission of a PIA to the Commissioner apply. See Section 7(5) (MIN) CPL will submit a copy of any PIA to the Commissioner, if required by guidelines outlined in the (Ministerial) Regulations or by specific request of the Commissioner.



12.2 A Privacy Impact Assessment must:

- 12.2.1 Include a summary of the purpose of the collection, use, or disclosure of personal information for the new or substantial change to an existing administrative practice, program, project, or service.
- 12.2.2 Identify the types of personal information that will be collected, used, or disclosed and reasonable security arrangements in place to protect that personal information.
- 12.2.3 Identify the legal authorities for the collection, use, or disclosure of the personal information.
- 12.2.4 Identify any privacy risks and mitigation strategies respecting the personal information.
- 12.2.5 Identify the administrative, physical, and technical safeguards in place to protect the personal information.
- 12.2.6 Describe accuracy, correction, and retention procedures that will be implemented to ensure the personal information is accurate and complete.

12.3 Completed PIAs will be retained for six years.

13. Consent to Gather Personal Information

PPMR - Section 6 (2) iv

- 13.1 CPL will require oral, written, or electronic consent for the gathering of personal information. If the information is to be used to make a decision that directly affects the individual, the library will retain the records for one year, or as specified in Appendix B, or for the amount of time agreed to by:
 - 13.1.1 The individual
 - 13.1.2 The Library Director

14. Manner of Collection

PPMR Section 5(2)

- 14.1 CPL will collect personal information directly from the individual the information is about. A collection notice will be provided at the time of collection and can be provided either in writing, or verbally during an in-person conversation. The collection notice must include:
 - 14.1.1 The purpose for which the information is collected
 - 14.1.2 The specific legal authority for the collection
 - 14.1.3 The contact information to which the individual may direct the individual's questions about the collection



15. Administrative, Technical, and Physical Safeguards

PPMR - Section 6(2) b

- 15.1 Administrative Safeguards: CPL will restrict access to personal information to those who need it for the regular duties of their employment.
- 15.2 Physical Safeguards: Hard copies of personal information will be locked in cabinets depending on the Security Classification of the information.
- 15.3 Technical Safeguards: CPL via the Parkland Regional Library System will employ firewalls and restrictions to electronic access to personal information within the SuperNet or Cloud-based storage.

16. Artificial Intelligence (AI) and Automated System Use

PPMR Section 6(1)(b)(iii)

- 16.1 CPL will prioritize humans over automated systems to generate content or make decisions, recommendations, or predictions whenever possible.
- 16.2 If CPL uses an artificial intelligence (AI) or automated system to generate content or make decisions that directly affect an individual, the Library will identify this use in its collection notices.
- 16.3 The Library will ensure personal information used in these systems is accurate, protected, and used in accordance with applicable legislation. Human oversight will be maintained to review outputs.
- 16.4 The Library will prioritize the use of non-personal or de-identified information when using artificial intelligence and automated systems wherever possible.
- 16.5 Personal information will only be used where necessary and permitted by law.
- 16.6 Individuals will be informed when personal information is used in AI or automated systems, as required by legislation.
- 16.7 AI and automated systems will not operate without appropriate human review.
- 16.8 Staff will validate output before they are used to inform decisions that affect individuals.
- 16.9 Personal information will be protected in accordance with legislation and internal policies.
- 16.10 Only necessary information will be used.

17. Confidentiality of User Records

ALR Section 7

- 17.1 Library board members, staff, and volunteers will only collect patrons' personal information when it is required for the purposes of delivering public library service.
- 17.2 No records are kept of the frequency or content of visits to the library by specific patrons.



- 17.3 No records are kept of a cardholder's item checkout history unless an item is associated with an unpaid fine by the borrowing patron, or if the cardholder has given written permission for this record to be kept. If this record is kept, it is subject to disclosure with the cardholder's other records under the conditions described in points (17.4 + 17.8)
- 17.4 Library staff, Board Members, and volunteers will not disclose a patron's personal information to a third party without the individual's consent, except:
 - 17.4.1 In response to a court order (e.g. subpoena, search warrant)
 - 17.4.2 In partnership with other Alberta libraries and library systems for the purposes of sharing materials under conditions defined in existing resource sharing agreements and programs (e.g. interlibrary loan agreements, ME Libraries, etc.), collecting fees or fines, and retrieving borrowed materials.
 - 17.4.3 For the purpose of contacting next of kin or emergency response personnel in the case of an emergency.
- 17.5 Cardholders will acknowledge that their contact information will be available to other organizations for the purposes identified in 17.4.
- 17.6 Information about a patron's use of the Library, including their presence in the Library, will not be provided by phone.
- 17.7 Staff and volunteers are to keep confidential the reading and viewing habits of individual patrons.
- 17.8 Upon request, a library patron will be given access to all information concerning their records that the Library has on file. Access to a user's records is limited to that user except where the user is a minor, or if the user has given written permission for someone else to access their records. Where a parent or guardian's permission is required for a cardholder to obtain a library card, that parent or guardian may have full access to the cardholder's records for retrieval.

18. Retention of Library Records

ALR Section 7

- 18.1 Library Board members, staff, and volunteers will only collect patrons' personal information when it is required for the purposes of delivering public library service.
- 18.2 Library Records which have been slated for disposal following the time guidelines outlined above shall be shredded, incinerated, or deleted by the Executive Assistant and/or appointed personnel and a record made of the date, method and time of disposal.
- 18.3 Hard copy Library records will be kept locked in the library in either a filing cabinet or a room for this purpose.



19. Delegation by Head of Public Body

POPA - Section 55

See APPENDIX A – Protection of Privacy Act Delegation Tables

APPENDIX A Protection of Privacy Act Delegation Tables

Duty, power or function of Head	Section reference	Retained by Head	Delegated to Privacy Officer
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	
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	



APPENDIX B

Library Records Retention Schedule

Camrose Public Library will retain the following library records based on the schedule provided by the Canadian Income Tax Act and in accordance with the schedules provided by the Camrose Public Library Board. The records are held in hardcopy and/or electronic formats.

Document Type	Length of Retention
Cash receipts, deposit books, copies of paid invoices, receipt books, cancelled cheques, cheque stubs, year-end trial balances, accounts payable, bank statements, grant applications, and a record of charitable receipts.	7 years from the date that the tax return is submitted.
Bank reconciliations, outstanding cheques, and design estimates.	7 calendar years.
Employee records including personnel files, job applications of hired personnel and personnel evaluations, payroll records, including T-4 slips, WCB claims, and attendance records.	3 years past last working day.
Solicited resumes, job applications (not hired), interview packages (not hired), applications for grant funded positions, etc.	12 months from receipts.
Interlibrary loan requests and daily logs will be held.	Until the transaction is complete.
Board minutes and agendas, assets and final audit reports including financial statements, bylaws, court cases, deeds, insurance claims, legal opinions and proceedings, record of files destroyed, and Income Tax Records.	Permanently.
Privacy Impact Assessments.	6 years.

