



POLICY

Policy Name	Artificial Intelligence (AI) Use		
Section & Number	Board – G-09	Effective Date	2025-05-15
Motion Number	2026-103	Last Review	2026-10-15
Author	CEO	Next Review	2027
Policy Maintenance	Reviewed by Management		

Policy Statement

The St. Catharines Public Library (SCPL) recognizes the transformative potential of artificial intelligence (AI) in enhancing library services, operations, and user experiences. This policy establishes a framework to ensure the ethical, secure, and responsible use of AI while safeguarding data privacy, accuracy, equity and transparency. AI can significantly improve efficiency and user experiences within the library, while potential risks involved need to be systematically identified and mitigated.

Scope

This policy applies to all SCPL staff and volunteers involved in the development, procurement, and use of AI technologies in library operations. Examples include AI-powered tools for customer service, content generation, and operational efficiency.

Definitions

Algorithmic Bias: A systematic error in an AI system's outcomes caused by the use of skewed, incomplete, or prejudiced training data, resulting in unfair, discriminatory, or inaccurate predictions or decisions.

Artificial Intelligence (AI): A machine-based system that, for explicit or implicit objectives, infers from the input it receives in order to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments.

Confidential Data: Data that should be kept within the Library to protect operations, reputation, and compliance with legal requirements. General disclosure of this data could negatively impact SCPL. Access is highly restricted, and the disclosure of any subset of this data is strictly prohibited unless specifically permitted or required by law. This includes, but is not limited to: legal advice, vendor negotiations and contracts, and risk registry.

Generative AI: A type of artificial intelligence that produces new content such as text, audio, code, videos, and images based on information the user inputs (typically a short instructional text called a "prompt").

Personally Identifiable Information (PII): Data that can be used to identify an individual, such as names, addresses, and identification numbers.

Private AI: An AI system that is developed, hosted, or procured for exclusive, secure use within the Library's infrastructure or under strict contractual data protection measures. Private AI is designed to maintain confidentiality, security, and compliance.

Public AI: An AI system made broadly accessible by a vendor to any user, typically via a public platform or interface (e.g., the free version of ChatGPT). Data input into public AI systems may be transmitted and stored outside the Library's infrastructure and could be used to continuously train the vendor's algorithms, raising considerations around data privacy and control.

Sensitive Data: Restricted information that must only be accessible to authorized individuals within the Library due to legal regulations or ethical mandates. This includes, but not limited to: personal information of staff, volunteers, or library customers, employee personnel files, customers' circulation records, borrowing histories, and reference queries.

Policies and Regulations

- Applicable Copyright Laws, including the Canadian Copyright Act & Regulations.
- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
- Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024
- SCPL Risk Management Policy and Plan

Principles

Accountability: AI tools must be assessed before use to ensure they are safe, secure and reliable for a well-defined purpose and the scope of AI use must be proportionate to the problem it intends to solve. Regardless of how AI is used, individuals utilizing AI must always verify all inputs and outputs, exercise sound judgment, and take responsibility for any decisions made.

Accuracy and Reliability: Accurate, fact-based, and unbiased data must be used to produce fair, reliable, and usable results. Validate data inputs and AI outputs for accuracy and consistency before use.

Data Privacy and Security: Staff must safeguard sensitive, confidential and personally identifiable information by adhering to privacy regulations, such as the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). Specific measures and approved tools will be used to protect data privacy and security.

Ethical Use: Using AI technologies must abide by copyright regulations, align with SCPL's values, foster trust, and avoid harm, bias, or unethical outcomes.

Inclusivity: SCPL shall leverage AI to enhance accessibility and equity while actively working to avoid discriminatory outcomes.

Sustainability: SCPL recognizes that Generative AI systems can be a significant source of resource consumption, including high energy and water usage. The Library will strive to incorporate sustainability considerations into the evaluation of AI tools. Staff are encouraged to be mindful of the resource intensity of AI technologies and consider alternative approaches if the use of AI for a task yields a comparable result but requires disproportionate resources.

Transparency: SCPL must clearly communicate and label the use of AI in library operations and content creation where the content has been substantially generated by AI. However, formal disclosure is not required when AI is used strictly as an assistive tool for wordsmithing, editing, or preliminary research, provided the final content is authored and verified by staff. Meaningful and timely information about use of AI tools is made available for customers in accessible plain language.

Guidelines

Accountability

Staff must review and validate AI-generated outputs. Human oversight and professional judgement are required for all AI-assisted decisions. AI tools enhance productivity but do not replace human decision-making.

Data Handling

Library staff must not enter sensitive, confidential and personally identifiable information (PII) into AI systems, especially when using Public AI systems, such as the free version of ChatGPT. SCPL shall use robust data access and storage controls to mitigate security breaches.

Education and Training

SCPL will provide ongoing staff training on the use of AI in the workplace, including identifying AI risks, ensuring ethical use, and implementing security measures. The library will support customers with their use of AI as staff would with other technical tools. Staff will help customers understand the limitations and benefits of AI as well as any risks associated with AI and personal identifiable information.

Ethical Oversight

SCPL prohibits the use of AI for generating discriminatory, offensive, or inappropriate content and ensures all AI applications reflect SCPL's commitment to inclusivity, equity, and service excellence.

Incident Reporting

Staff must promptly report inaccuracies, security breaches, or unethical uses of AI to management. Violations of this policy may result in disciplinary action.

Procurement and Vendor Management

SCPL must evaluate vendors and AI tools for compliance with ethical, privacy, and security standards before use. Staff may not independently implement (install, configure, or integrate) or use a new AI application for Library operations without formal approval.

Risk Management

Managing AI related risks must align with the Library's Risk Management Policy and Plan. AI tools must be approved by management and deployed for use by library IT, if required. Appropriate risk mitigation measures and business continuity

plan must be identified and implemented by library IT and documented in Risk Register.

Evaluation and Approval

To maintain operational agility while managing risk, the evaluation and approval of new AI tools will follow a structured and documented framework requiring:

1. An initial endorsement or consent by department manager will be required before a formal review by Library IT.
2. A documented operational need, detailing how the AI tool (specifically whether it is a Generative AI, Public AI, or Private AI system) will be used and how it improves current library practices.
3. A Privacy Impact Assessment (PIA), which ensures sensitive, confidential, or Personally Identifiable Information (PII) is fully protected and managed in accordance with MFIPPA, particularly if the tool is a Public AI system.
4. A documented security and risk assessment, which includes evaluating the tool for security vulnerabilities, Canadian residency compliance, and potential Algorithmic Bias.
5. A Formal review by Library IT and approval from Library Management.

Rather than listing approved tools within this policy, Library IT will maintain a separate, up-to-date internal registry of all approved AI applications, distinguishing clearly between authorized Private AI systems and vetted Public AI tools, along with their permitted use cases.

Roles and Responsibilities

Management:

- Ensure staff understand and follow all AI policy requirements and related procedures.
- Provide guidance on appropriate and ethical AI use within their specific departments.
- Serve as the first point of contact for AI-related questions and evaluate departmental requests for the adoption of new AI tools.
- Report policy violations or privacy concerns to the CEO and Library IT immediately.
- In alignment with collective agreements concerning the notification of technological change, any introduction of AI systems that significantly

alters work methods shall include appropriate and timely notification to the union and impacted library staff.

Library IT:

- Maintain an up-to-date internal registry of approved AI applications for Library use, categorizing them as Private AI or approved Public AI systems.
- Ensure data used in approved AI systems is managed in accordance with privacy legislation, municipal guidelines, and the Library's privacy and confidentiality policies.
- Consult with departments concerning Privacy Impact Assessments and conduct security and Algorithmic Bias assessments for newly requested AI applications.

All Library Staff:

- Read, understand, and comply with this policy and any related operational procedures.
- Use only Library-approved AI tools as specified in internal guidelines for official Library business.
- Protect confidential and personal information by never inputting sensitive data or PII into Public AI systems. Approved Private AI systems must be used when handling sensitive Library data.
- Critically oversee, verify, and validate all AI-generated content for accuracy, potential Algorithmic Bias, and appropriateness prior to use, communication or publication.
- Report any AI-related security vulnerabilities, inaccuracies, or privacy concerns immediately to their manager.

Non-Compliance

SCPL relies primarily on staff education, professional responsibility, and human oversight to ensure the ethical use of AI. However, failure to adhere to the guidelines outlined in this policy, particularly regarding the unauthorized input of confidential data or PII into Public AI systems, poses a significant risk to the security, compliance, and reputation of the Library and its customers.

Unauthorized or inappropriate use of AI tools, or bypassing the procurement process for Generative AI software, may result in disciplinary action, up to and including termination of employment. Consequences will align with the nature and severity of the non-compliance.