

## Artificial Intelligence (AI) Policy

### 1. Purpose

This policy establishes ethical and operational guidelines for the use of Artificial Intelligence (AI) tools by Sylvan Lake Municipal Library employees, contractors, and volunteers. The goal is to leverage AI responsibly to enhance service delivery, operational efficiency, and employee capacity, while safeguarding privacy, ensuring accuracy, and promoting ethical standards.

### 2. Scope

This policy applies to all staff, contractors, and volunteers using AI tools in the course of their duties. It also provides guidance for assisting patrons with AI-related inquiries.

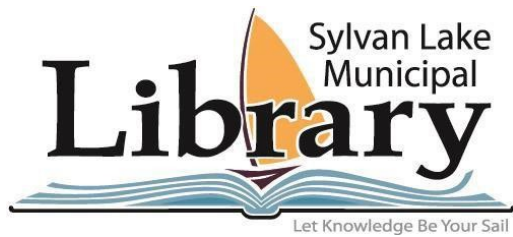
### 3. Definitions

- **Artificial Intelligence (AI):** Computer systems capable of performing tasks typically requiring human intelligence, such as learning, reasoning, and problem-solving.
- **Generative AI:** AI that creates original content (e.g., text, images) based on input prompts.
- **Predictive AI:** AI that analyzes data to forecast outcomes or trends.
- **Consumer AI:** Widely available AI tools for individual use (e.g., ChatGPT, Gemini).
- **Enterprise AI:** AI systems designed for large-scale business applications.
- **Confidential Information:** Internal library data not intended for public disclosure.
- **Personal Information:** Identifiable information about individuals, including library usage.
- **Sensitive Information:** Includes demographic, financial, and security-related data.

## I. GUIDING PRINCIPLES

### A. Data Privacy and Confidentiality

Generative AI tools are inherently blind to privacy and any data entered into them can be used for unintended purposes. Due to privacy concerns, employees must not input personal, confidential or sensitive information into a Generative AI tool. The tool may share this content verbatim with other



## **Artificial Intelligence (AI) Policy**

users, or it may be used by the AI vendor. If in doubt, an employee should speak to the Library Director. Employees must ensure compliance with data privacy laws and Library Privacy policies.

### **B. Accuracy and Reliability**

Employees must ensure the information provided by a Generative AI tool is factual and/or can be independently verified (meaning to cross-reference AI responses with known facts and reliable sources). Employees are responsible for any decisions that are made based on content provided by an AI tool, and also for the final content of any work completed using AI.

### **C. Ethical Usage**

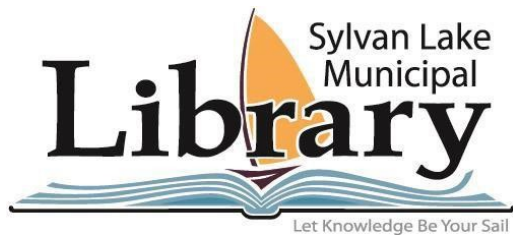
Generative AI tools are largely unregulated and may produce content that is biased or discriminatory. Employees must ensure that the information derived from these tools aligns with library values, and standards set out in library policies. Employees must not use AI tools to spread harmful content or for malicious reasons.

The current development model is for Generative AI to assimilate information from a large variety of sources. This means that it is not possible to confirm copyright compliance in images and videos created by Generative AI. This content must not be used in public communication channels or in public documents, including the library's social media accounts, on the library's website, or in posters that are intended to be displayed to the public.

### **D. Transparency**

Employees must be transparent about their use of Generative AI tools in the creation of work-related materials. This includes internal reports, presentations, and any other content where AI has provided substantial assistance, whether in the form of text or images. A simple disclaimer is sufficient to meet this requirement—for example, "This document was prepared with the assistance of AI tools."

It is important to recognize that AI tools may reproduce content from external sources verbatim. Disclosing the use of AI-generated content helps protect the organization from potential copyright infringement. Employees



## **Artificial Intelligence (AI) Policy**

must make reasonable effort to verifying the accuracy of the information they use and for documenting their sources appropriately.

### **E. Security**

Employees will be vigilant against AI-enabled phishing or cyber threats. Report suspicious communications to Parkland IT support.

### **F. Collaboration**

Employees are encouraged to openly share their learnings and best practices with colleagues.

Date Approved: October 15, 2025  
Board Chair: Carol Moore