

Jasper County Public Library Artificial Intelligence (AI) Use Policy

Jasper County Public Library (JCPL) recognizes that Artificial Intelligence (AI) tools can assist staff with research, content creation, productivity, accessibility, and library operations. This policy establishes guidelines for the responsible, ethical, and secure use of AI technologies while protecting patron privacy, confidential information, and the integrity of library services.

This policy is informed by the American Library Association's *Guidance on the Use of Artificial Intelligence in Libraries*, which emphasizes privacy, intellectual freedom, transparency, and human oversight. It applies to all JCPL employees, volunteers, contractors, and representatives using AI technologies while conducting library business or using AI in connection with their duties for JCPL.

Definitions

Consumer AI: AI services intended for the general public, including free or individually purchased AI services and AI accounts that are not managed or administered by JCPL.

Examples may include ChatGPT Free or personal ChatGPT accounts, Gemini, Claude, and free or personal versions of other publicly available AI services.

Enterprise AI: AI services provided through an organization-managed environment with administrative, security, privacy, and access controls appropriate for organizational use.

Examples may include Microsoft 365 Copilot when licensed and administered by JCPL and other AI services specifically approved by JCPL.

AI Agent: An AI-powered system capable of performing actions, accessing information or systems, making changes, initiating workflows, communicating with users, or acting on behalf of a person or organization.

General Principles

JCPL will strive to be transparent regarding library-provided AI tools and services and, when appropriate, inform users when they are interacting with AI-generated content or AI-assisted services. JCPL's use of AI shall be guided by the following principles:

- Protect patron privacy and confidentiality.
- Protect confidential, restricted, and non-public JCPL information.
- Use AI in a manner consistent with applicable laws, regulations, professional standards, and JCPL policies.
- Maintain human oversight and accountability.
- Verify AI-generated information before relying upon or distributing it.
- Consider potential bias, misinformation, and other limitations of AI-generated content.
- Use AI tools appropriate to the sensitivity of the information being processed.
- Evaluate privacy, security, data retention, and other risks before adopting AI technologies that interact with JCPL systems or information.

Approved Uses

AI may be used to assist with:

- Drafting emails, letters, and correspondence
- Creating marketing materials and promotional content
- Preparing training materials and documentation
- Research assistance and information gathering
- Brainstorming and project planning
- Summarizing non-confidential information
- Drafting policies, procedures, forms, and reports
- Accessibility support, such as plain-language summaries and alternative text
- Other routine activities approved by JCPL

AI-generated content should be considered a draft and reviewed by a staff member before use.

AI Platform Classification

Approved for Library Business

JCPL-approved enterprise AI platforms may be used for library business, subject to this policy and any applicable JCPL procedures or restrictions. JCPL's preferred enterprise AI platform may include Microsoft 365 Copilot when appropriately licensed and administered by JCPL. Other AI services may be approved by Library Administration and the Systems Administrator following appropriate review. Approval of an enterprise AI service does not authorize staff to disclose information that they are otherwise prohibited from disclosing. Staff must continue to follow all applicable privacy, confidentiality, records retention, cybersecurity, personnel, and other JCPL policies. Consumer AI platforms may be used for general research, brainstorming, drafting, and other permitted activities involving public information that does not contain confidential or library-sensitive information.

Examples may include:

- Free Microsoft Copilot
- ChatGPT Free or personal AI accounts
- Gemini
- Claude
- Similar publicly available AI services

Personal or consumer AI accounts may be used for permitted activities that do not involve confidential, personally identifiable, or library-sensitive information. They may not be used to process restricted information or non-public information obtained through a staff member's employment with JCPL. As a general rule, information that would not be appropriate to post publicly on the Internet should not be entered into a consumer AI service.

Restricted

Staff shall not use personal AI subscriptions, experimental AI tools, or unapproved AI services to process confidential, restricted, or library-sensitive information.

Prohibited Information

The following information shall not be entered into consumer AI systems or unapproved AI tools:

- Patron names or personally identifiable information
- Library account information
- Borrowing histories or reading histories
- Reference transactions or other confidential reference information
- Personnel records
- Medical information
- Financial information
- Passwords or authentication credentials
- Security configurations
- Network or system information that could create a security risk
- Incident response information
- Confidential cybersecurity-related information
- Attorney-client communications
- Confidential or non-public library records
- Other information restricted by law, regulation, contract, or JCPL policy

Use of an approved enterprise AI service does not automatically authorize the use of the information listed above. Sensitive information may only be processed when the particular AI service and use case have been specifically approved by JCPL. Exceptions to these restrictions require prior approval from Library Administration and the Systems Administrator and may require review of the AI service's privacy, security, data retention, contractual, and other applicable terms.

Human Oversight

AI shall assist, not replace, staff judgment. Staff remain responsible for:

- Verifying accuracy
- Correcting errors
- Evaluating potential bias
- Confirming compliance with library policies
- Protecting confidential and restricted information
- Making final decisions
- Reviewing AI-generated content before it is used or distributed

AI-generated information, citations, quotations, images, audio, video, or other content shall not automatically be assumed to be accurate, authentic, complete, or free of bias.

AI-generated content used in public-facing materials, research assistance, policy decisions, or other consequential activities shall be independently reviewed and verified as appropriate.

Human staff remain accountable for all final work products and decisions.

Privacy and Confidentiality

JCPL is committed to protecting patron privacy and confidentiality. Before adopting AI-enabled services, the Library may evaluate:

- Data collection practices
- Data retention practices
- Vendor privacy protections
- Security controls
- Data ownership and usage rights
- Whether information submitted to the service may be used to train or improve AI models
- Administrative and access controls
- Integration with JCPL systems and data

Approved AI services may be periodically reviewed to ensure they continue to meet JCPL's privacy, security, accessibility, operational, and business requirements. Library staff shall comply with all privacy, cybersecurity, records retention, and confidentiality requirements when using AI technologies.

Copyright and Intellectual Property

Staff shall consider copyright, licensing, intellectual property, attribution, and other applicable legal requirements when using AI-generated or AI-assisted content. AI-generated content shall not automatically be assumed to be free of copyright or other restrictions. Staff should use appropriate judgment when submitting third-party copyrighted materials to AI services and should avoid submitting copyrighted or licensed materials when doing so would violate applicable rights, licenses, contracts, or JCPL policies.

Library AI Systems and AI Agents

The deployment or use of AI-powered chatbots, automated assistants, AI agents, or other AI systems that access library data, patron information, staff information, library services, or JCPL systems requires prior approval from the Library Director and Systems Administrator. AI systems capable of taking actions on behalf of JCPL—including sending communications, modifying files or records, accessing systems, initiating workflows, or making decisions—shall receive appropriate security and privacy review before deployment. Staff shall not connect an unapproved AI service, AI agent, browser extension, plug-in, or other AI technology to JCPL systems or accounts.

Training

JCPL will provide guidance regarding:

- Responsible use of consumer and enterprise AI technologies
- Privacy, confidentiality, and data security requirements
- Verification of AI-generated information, including potential bias, misinformation, and other limitations of AI output
- Copyright and intellectual property considerations

- AI literacy, emerging AI risks, and evolving best practices

Staff assigned an enterprise AI license may be required to complete JCPL-provided AI training before using the service for Library business.

Compliance

Staff are responsible for following this policy and all other applicable JCPL policies when using AI technologies. Failure to comply with this policy may result in loss of access to AI technologies and may be subject to applicable personnel policies. Suspected disclosure of confidential information, security information, patron information, or other restricted information to an AI service shall be reported promptly to the Systems Administrator and Library Administration.

Adopted 9/14/26