MARIST + AI

AI Operational Guidelines

Purpose

Marist University recognizes the transformative potential of generative AI tools and embraces their use in the workplace to enhance productivity and innovation. These AI Operational Guidelines ensure this technology is utilized in a responsible, ethical, and productive manner, aligning with institutional policies, security requirements, and legal regulations.

Guiding Principles

The use of generative AI tools (text, image, audio/video, etc.) in our workplace must adhere to principles that both harness innovation and protect our institutional values. For operational uses, the following considerations are essential:

Data Privacy & Security

In alignment with our commitment to ethical oversight and the responsible stewardship of information, these guidelines prioritize data privacy and security when using AI tools.

a. Do not input sensitive university data, trade secrets, or student, faculty, or staff information into AI tools without approval.
b. Ensure AI-generated content is reviewed for accuracy before use.
c. Adhere to institutional policies, legal requirements, and industry regulations when using AI tools.

Human Oversight & Accountability

Guided by the principle of human-centered innovation, these guidelines emphasize the critical role of human oversight in the use of AI tools. While AI offers significant potential, employees remain accountable for verifying AI-generated content to ensure accuracy, identify potential biases, errors, or inaccuracies, and ultimately, maintain the integrity of our work.

a. Utilize AI in a manner that supports processes and does not circumvent human decisions or actions.
b. Review AI outputs for bias, errors, or inaccuracies.
c. Verify AI-generated content before using it for business purposes.
d. Make final decisions by employees, not AI, unless explicitly approved by management.

Acceptable and Unacceptable Uses

Acceptable Uses

Adhering to the principles of data privacy & security, employees may use AI tools for:

a. Enhancing productivity, efficiency, and decision-making.
b. Automating repetitive or routine tasks.
c. Assisting in research, data analysis, and reporting.
d. Drafting emails, documents, or presentations.
e. Supporting customer service and internal communications.
f. Generating ideas, brainstorming, and problem-solving.

MARIST + AI

Unacceptable Uses

AI tools should not be used for:

a. Generating or sharing misleading, false, or unethical content.
b. Creating, storing, or processing confidential information (including student records, business practices, strategic plans, contracts, trade secrets, negotiations, IT resources, accounting records, and financial data) requires special handling regardless of format. No FERPA, HIPAA, or personally identifiable information should be used.
c. Making autonomous business decisions without human oversight.
d. Violating intellectual property rights, copyright laws, or licensing agreements.
e. Circumventing security protocols or engaging in unauthorized data access.
f. Employee or student assessment without special approval, as these areas require careful consideration of privacy and individual rights.

Process for Employee Use of AI Tools

Department leaders are responsible for establishing appropriate use cases for AI, overseeing implementation, and reporting on AI tool usage within their teams. This institutional oversight ensures responsible AI use, maintains data security, promotes compliance with regulations, and maximizes the strategic value of AI investments.

Department Responsibilities:

a. Monitor the tasks that employees will be performing with AI tools.
b. Maintain records of the type(s) of AI tools or solutions being used.
c. Document what data will be used by team members, consult with data stewards when necessary.
d. Track how the data will be used across the department.
e. Provide ongoing training and promote AI literacy among staff.
f. Monitor and evaluate the use of AI tools

Process for Department Implementation of AI Tools

All AI tools and solutions must go through the review process outlined below prior to implementation:

Information Technology:

- Examine whether the solution can be managed and supported in our current environment.

Cybersecurity:

- Review risk and security related to the solution.
- Ensure vendor completes and submits HECVAT 4.0 if one is not currently on file.
- Determine whether AI tool is open source/closed-source and evaluate appropriate use cases.

Legal Responsibilities:

- Review and understand terms and conditions associated with solution.
- Establish clear objectives for AI use in service agreements or contracts with third-party vendors.