Guidelines for Appropriate and Ethical Use of AI

Baseline Assumptions

The Artificial Intelligence Committee began its development of these guidelines by reviewing the baseline assumptions developed in Summer 2023 for academic usage.

> *The following assumptions undergird the University's approach to establishing initial guidance consistent with its Christian mission for the appropriate use of artificial intelligence (AI) to generate or modify text, speech, audio, images, video, music, and other media or to otherwise replace original work.*
>
> 1. *Artificial intelligence is not a substitute for creative, critical, and/or collaborative thinking.*
> 2. *Artificial intelligence is a tool that, when used appropriately, can assist individuals and groups to improve decision making, identify alternatives, streamline processes, protect individuals and societies, and provide various other benefits.*
> 3. *Artificial intelligence is transforming the way humans interact with the world; serious societal and economic questions related to privacy and consent, security, commerce, health care, bias, research, and analysis, among many others, have yet to be answered.*
>
> *Faculty should prepare students to be original thinkers, capable of creative expression and critical reasoning, and should teach them to understand, evaluate, critique, and—when appropriate—utilize AI tools in a responsible and ethical manner, thereby positioning them to participate in the ongoing global discussion on AI from a Christian perspective.*

Affirming these baseline assumptions, the Committee also stresses the importance of human control: decisions should be made by people. The Committee has developed the following guidelines for the appropriate and ethical use of artificial intelligence at Olivet for all employees. [Note: More specific guidance on best practices for academic use of artificial intelligence is currently being developed by the subcommittee for academic affairs.]

Purpose and Scope

This policy provides guidance on the responsible use of Artificial Intelligence (AI) technologies in academic and administrative settings to support the ethical and

appropriate use of AI while encouraging efficiency and innovation. The policy applies to all full- and part-time faculty and staff, including student workers, who use AI tools in conjunction with University-owned data or in fulfillment of their responsibilities.

Definitions

Artificial Intelligence (AI)- The capacity of computers or other machines to exhibit or simulate intelligent behaviour; the field of study concerned with this. In later use also: software used to perform tasks or produce output previously thought to require human intelligence, esp. by using machine learning to extrapolate from large collections of data. Also as a count noun: an instance of this type of software; a (notional) entity exhibiting such intelligence. Abbreviated AI. (Oxford English Dictionary)

Generative AI (AI)- Refers to AI tools that generate text, images, video, and other content. Generative AI uses Large Language Models (LLM) to predict the most likely response to a prompt.

Data Risk Classifications:

- High Risk Data- Restricted information that is legally protected and whose unauthorized disclosure, access, or use could cause significant harm to individuals or the institution. This includes data regulated by federal/state laws such as HIPAA, FERPA, and GLBA (e.g., student GPAs, financial transactions, ID numbers, SSNs, medical records, and the like). See Related Policies section below.
    - Should never be entered into an AI tool unless explicitly authorized by the Artificial Intelligence Committee.
- Moderate Risk Data- Sensitive information that is not explicitly protected under federal/state law but is still considered confidential as it may pose a privacy/operational risk to the university or individuals if disclosed or misused. Includes employment data, donor information, and other proprietary University data. Also includes student directory information and other personally identifiable information (PII) when combined with sensitive or operational details. Intellectual property also falls into this category.
    - Should only be entered into generative AI tools that have been assessed and approved for such use.
    - May only be used when appropriate measures are taken to ensure privacy, such as removing identifying information.
- Low Risk Data- Non-sensitive information that is available to the public or poses minimal risk if disclosed.

- Can be used with reasonable care in any generative AI tool, adhering to the acceptable use guidelines.

Machine Learning- The process by which artificial intelligence programs use data to train their algorithms for continuous improvement.

Private Data- Generally classified as high- or moderate-risk data if disclosed; it includes, but is not limited to:

- Personally Identifiable Information (PII): Names, addresses, phone numbers, email addresses, social security numbers, and other unique identifiers.
- Financial Information: Bank account details, credit card numbers, and financial transaction records.
- Health Information: Medical records, health insurance information, and any data related to an individual's health status.
- Academic Records: Student grades, transcripts, and other educational records.
- Research Data: Non-public research data that could be sensitive or proprietary.

Intellectual Property- Original creations, ideas, research, inventions, etc. that stem from an individual or group and are legally protected by rights such as patents, trademarks, copyrights, or trade secrets.

Guidelines

Accountability:

Employees of the University are responsible for their use of AI tools and following the provisions outlined in these guidelines. Employees who use AI to assist with analysis, develop communications or other material, or support decision making on behalf of the University are ultimately responsible for the decisions or output that result. Employees should take special care when using generative AI to ensure accuracy, check for bias, verify sources and information, and avoid copyright infringement. Violations of the guidelines outlined in this policy may result in disciplinary action on the part of the University, up to and including termination.

Accuracy and Bias:

Generative AI tools can reflect or amplify societal biases present in the data on which they were trained. Evaluate AI content critically to prohibit outputs that could perpetuate stereotypes, discrimination, or unequal treatment of groups or individuals. Responses from AI tools should not be treated as objective or authoritative without human oversight.

AI Tools can produce fluent and persuasive outputs; however, they are not inherently reliable sources of factual information. AI tools often generate content that may be outdated, partially correct, or entirely fabricated (hallucinations). Because of these inherent risks, AI-generated outputs must be verified for accuracy before being used in academic, research, or administrative contexts.

Approved vs. Unapproved AI Tools:

Approved tools have undergone rigorous evaluation to ensure they comply with our data privacy standards, but unapproved tools may not have the same level of scrutiny. The review includes considerations of data security, compliance, reliability, ethical considerations, support, and reliability.

When using AI tools, consider the nature of the data you are working with. If the data includes private or sensitive information, use approved tools to minimize risks. However, if you choose to use unapproved tools for low-risk data, ensure that no private data is exposed or transmitted to unauthorized entities.

Using approved tools helps maintain control over data processing and storage, as these tools are subject to regular audits and compliance checks. This process helps mitigate risks associated with data breaches and unauthorized access.

Requesting approval: To request approval for a new tool, complete the "Request to add a new AI tool" form. The requestor is responsible for working with vendors to answer an initial list of questions. The Artificial Intelligence Committee will conduct an initial review and either deny the request, send it back for additional information, or send it on to IT for final review. If the IT review establishes that the tool meets University standards, it will be added to the list of approved tools.

Cautionary Guidelines:

- Use Approved Tools for High-Risk and Moderate-Risk Data: Verify that the AI tool you are using is on the university's approved list. Entering any high-risk data into an AI tool requires approval of the AI Committee.
- Unapproved AI tools should only be used for Low-Risk Data; employees should still be cautious about sharing data. Ensure that no private or sensitive information is transmitted to these tools.

Steps to Verify Data Privacy:

To ensure no private information is used or transmitted to unapproved AI entities, follow these steps:

- Data Classification: Identify and classify the data you intend to use with AI tools. Determine if it includes any private or sensitive information.
- Data Anonymization: Where possible, anonymize data before using it with AI tools. Remove any personally identifiable information (PII) to mitigate privacy risks. If you want to use an AI tool to help redact PII, obtain approval first.
- Tool Verification: Confirm that the AI tool is approved by the university.
- Data Transmission: Ensure that data transmission to AI tools is secure. Use encrypted channels and verify the recipient's authenticity.
- Regular Audits: Conduct regular audits of AI tool usage to ensure compliance with data privacy policies.

Transparency:

Faculty and staff should disclose when and how generative AI tools are used for all academic and research-related material. Employees should also be transparent when generative AI contributes significantly to other work products (e.g., email communications to constituents, written reports, and so on) and should cite their usage. Use of non-generative AI should also be noted when it contributes substantially to data analysis, reports, or otherwise supports decision making.

It is not always simple to determine what makes usage "significant." Examples of significant use would be using generative AI to develop an initial draft for a new academic program or using non-generative AI to analyze data on student persistence or recruiting efforts. It may be helpful to use the University's Fair Use Guidelines (see section I.4 of the Copyright Usage Policy) — if the use of AI falls under what would typically be considered fair use of copyrighted material, it would not need to be cited.

Citing AI: For academic and research-related materials, refer to the relevant style guide (e.g., APA, Chicago, MLA, etc.). For all other usage where citation is appropriate, state the AI tool(s) used along with a brief explanation of how they were used and/or what content was generated. *For example, "Microsoft Copilot was used to develop the outline for the proposed policy."*

Approved tools

Approved tools: Employees may use the following AI tools for **moderate- and low-risk data** when logged in with ONU credentials. Microsoft Copilot, Kaltura, Microsoft 365, Student Success and Engagement. Using any of these tools with a personal account is not approved for high- or moderate-risk data. Approved tools may only be used for high-risk data with additional approval from the AI Committee.

Non-exhaustive list of unapproved tools: Employees may use the following tools **only with low-risk data** and after verifying that no private or confidential information is included. ChatGPT, Grammarly, Claude, Gemini 39, Grok, Llama, CopyAI, NotebookLM, Perplexity, Scribblr, Quillbot.

Related ONU Policies

Acceptable Use Policy

Data Governance and System of Record Policy

Data Security Policy

GLBA and PCI Training

FERPA

Information Security Policy

Note: Information on the Artificial Intelligence committee can be found on the portal by clicking on the link for Standing Committees on the Academic Affairs page on the portal.

Sources

This policy was built after reviewing similar policies at other universities. Microsoft Copilot and OpenAI's Chat GPT were also used to develop the outline for these guidelines. Specific language and concepts were adapted from the following sources, retrieved in April and May 2025:

Columbia University: https://provost.columbia.edu/content/office-senior-vice-provost/ai-policy
Cornell University: https://it.cornell.edu/ai/ai-guidelines
Harvard University: https://www.huit.harvard.edu/ai/guidelines
Microsoft Copilot (for Work): https://m365.cloud.microsoft/chat/
MIT: https://ist.mit.edu/ai-guidance
Northeastern University: https://nu-res.compliance.northeastern.edu/standards-for-the-use-of-artificial-intelligence-in-research-at-northeastern/
OpenAI. ChatGPT: https://chat.openai.com/chat
Program Strategy HQ: Responsible AI Checklist: https://www.programstrategyhq.com/post/responsible-ai-checklist-pshq
Stanford University: https://uit.stanford.edu/security/responsibleai
University of Utah: https://ai.utah.edu/work/ai-use-guidelines.php
University of Texas at Austin: https://ai.uta.edu/