Artificial Intelligence Acceptable Use Policy for Faculty and Staff

June 10, 2025

Document Properties

Property	Description
Title	YU – Information Security Incident Response Plan
Owner	Jorge Warman
Group	Information Technology Services
Authors	Steve Kalvar
Version	2.0
Document Classification	Internal Use Only
Signature of Approval	
Date	06/10/2025
Applicable Laws and Regulations	

Revision History

Version	Date	Comment	Updated by
1.0	05/12/2025	Initial Draft	Steve Kalvar
2.0	06/10/2025	Incorporated Edits from OCIO	Steve Kalvar

Contacting Support:

ITS Help Desk, helpdesk@yu.edu, 800-337-2975 or 646-592-4357, Teams dial 4357

Table of Contents

Table of Contents

Artificial Intelligence Use Policy for Faculty and Staff

1.1 Overview

Generative AI is a type of artificial intelligence that can learn from and mimic large amounts of data to create content such as text, images, music, videos, code, and more, based on inputs or prompts. Yeshiva University supports responsible experimentation with generative AI tools by its faculty and staff, but there are important considerations to keep in mind when using these tools, including information security and data privacy, compliance, copyright, and academic integrity.

1.2 Purpose

Yeshiva University is dedicated to advancing knowledge and learning and Generative AI (or "AI") tools such as OpenAI's ChatGPT, Google's Bard, Stability AI's Stable Diffusion, and others, have captured the public's imagination as these tools become widely available for everyday use. Generative AI tools have the capacity to expedite existing processes and make possible new ones. These tools also advance many aspects of research and health care delivery. While the University supports the responsible use of AI, these novel tools have notable limitations and present new risks that must be taken into consideration when using these technologies.

Three key attributes of these tools are 1) the risk that an input could potentially become public, 2) the risk that the output may be biased, misleading, or inaccurate, and 3) the risk it may be used in phishing campaigns. There are risks related to information security, data privacy, copyright, academic integrity and bias, for example:

- If Generative AI is given access to personal information, the technology may not respect the privacy rights of individuals, including in a manner that may be required for compliance with applicable data protection laws;
- If Generative AI is given access to Internal or Restricted information or trade secrets, the University may lose its intellectual property (IP) rights to that information and the information may be disclosed to unauthorized third parties through their independent use of the Generative AI technology;
- Generative AI outputs may violate the intellectual property rights of others, and might not themselves be protected by intellectual property laws;
- Generative AI outputs might be factually inaccurate, and users might be exposed to liability if they rely on those outputs without properly reviewing them; and
- Generative AI may produce decisions that are biased, discriminatory, or otherwise inconsistent with university policies, or that are otherwise in violation of applicable law.
- Generative AI has made it easier for malicious actors to create sophisticated phishing emails and "deepfakes" (i.e., video or audio intended to convincingly mimic a person's voice or physical appearance without their consent) at a far greater scale.

Yeshiva University requires that any use of Generative AI be in a manner reflective of its inherent limitations and to avoid these limitations and other emerging risks to the University, its faculty, staff and other stakeholders. Because AI is a rapidly evolving technology, the University will continue to monitor developments and will consider responses from the University community. This policy contains overarching guidelines that apply to all in the YU community while pursuing their YU activities. After these general requirements, this policy includes specific guidelines related to instruction and research.

1.3 Scope

This Generative AI policy ("Policy") governs the use of Generative AI tools by University faculty and staff (the "YU community") in the performance of their functions for or on behalf of YU. Because this Policy may be updated from time to time, YU faculty and staff are encouraged to regularly review the most recent version of this Policy. Constructive comments from YU faculty and staff may be submitted here: helpdesk@yu.edu

1.4 Definitions

- **"Internal or Restricted Information"** means any business or technical information or research result belonging to YU, a YU faculty or staff member, collaborators or other third parties, that is not publicly known or that has been provided or received under an obligation to maintain the information as Internal or Restricted. Please note this includes Protected Health Information or PHI.
    - **Restricted** means information whose loss, corruption, or unauthorized disclosure would cause severe personal, financial, or reputational harm to the University, its faculty and staff, and its students and other constituents/people served. Restricted also means information required by an outside party, via regulation or contract, to be safeguarded due to confidentiality, integrity, or availability risks.
    - **Internal** means information whose loss, corruption, or unauthorized disclosure would likely cause limited personal, financial, or reputational harm to the University, its faculty and staff, and its students and other constituents/people served.
- **"Generative AI"** includes any machine-based tool designed to consider user questions, prompts, and other inputs (e.g., text, images, videos) to generate a human-like output (e.g., a response to a question, a written document, software code, or a product design). Generative AI includes both standalone offerings such as ChatGPT, Bard, Stable Diffusion, as well as offerings that are embedded in other software, such as Github's Copilot.
- **"Personal Information"** means any information that, whether alone or in combination with other available information, identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to an individual.
- **"Intellectual Property"** (IP) rights are legal protections that safeguard creations of the mind, like inventions, literary and artistic works, designs, and symbols, ensuring creators can benefit financially and control the use of their creations.

1.5 Policy

YU expects all YU faculty and staff to follow these guidelines when using Generative AI tools for teaching and learning, research, and work-related functions:

- **Procuring AI Tools/Software (including free tools):** Contact Yeshiva University Information Technology Services (ITS) before purchasing (or acquiring for free) AI products or products that contain functions that rely on AI to operate – especially when using University resources or University data. ITS vendor management team will route the request to resources that can help validate the vendor's product and verify that use does not introduce undue risk to the University. These processes can also direct you to existing vendors and potentially avoid duplicate spending.
- **Do not input Internal or Restricted Information:** YU faculty and staff **must** not input any information classified as Internal or Restricted into Generative AI tools, except when expressly permitted by ITS after confirming appropriate contract language and security controls. See Institutional Data Classification Policy for more information.
- **Do not input Personal Information:** YU faculty and staff must not input any information that is identifiable to a person, third party, or the University into a Generative AI tool except when expressly permitted by ITS after confirming appropriate contract language and security controls.
- **Do not input information that violates IP or general contract terms and conditions:** All YU faculty and staff are responsible for complying with copyright laws (and other intellectual property and proprietary rights). In general, copyright laws protect and grant exclusive rights to authors of published or unpublished original works that have been recorded in tangible form, including literary works, musical works, dramatic works, pantomimes and choreographic works, pictorial, graphic, and sculptural works, motion pictures and other audiovisual works, sound recordings and architectural works. See the Use of Copyrighted Material section of the ITS Administration Faculty and Staff Handbook
- **Confirm the accuracy of the output provided by Generative AI tools:** YU faculty and staff must check the accuracy of information generated by Generative AI tools prior to relying on such information. Generative AI tools should not be relied upon without confirmation of accuracy from additional sources. It is possible for AI-generated content to be inaccurate, biased, or entirely fabricated (sometimes called "hallucinations"). Note that such AI-generated content may contain copyrighted material. You are responsible for any content that you publish that includes AI-generated material.
- **Check the output of Generative AI tools for bias:** YU faculty and staff must consider whether the data input into, and the output of, Generative AI tools produce decisions that may result in a disparate impact to individuals based on their protected classifications under applicable law, such as race, ethnicity, national origin, age, sexual orientation, or disability status. You should not rely on any output that is indicative of potential bias.

- **Disclose the use of Generative AI tools:** YU faculty and staff who leverage Generative AI to produce any written materials or other work product must disclose that those materials and that work product is based on or derives from the use of Generative AI. You must always be transparent if you are relying on the output of a Generative AI tool.
- **Comply with third-party intellectual property rights:** YU faculty and staff must not represent any output generated by Generative AI tools as their own. In addition, if you quote, paraphrase or borrow ideas from the output of Generative AI tools, you must confirm that the output is accurate and that you are not plagiarizing another party's existing work or otherwise violating another party's intellectual property rights.
- **Do not use Generative AI tools to produce malicious content:** YU faculty and staff are prohibited from using Generative AI tools to generate malicious content, such as malware, viruses, worms, and trojan horses that may have the ability to circumvent access control measures put in place by YU, or any other third-party , to prevent unauthorized access to their respective networks.
- **Ask the Generative AI system not to use inputs for training the system:** Some Generative AI systems permit users to opt out of the use of their data to train future iterations of the Generative AI system. Where that option is available, YU faculty and staff should exercise it and opt out of such use.

1.5.1 University Approved Applications, Exemptions, and Exceptions

ITS will publish a list of specific applications that have been vetted by ITS and Procurement and deemed fully or partially acceptable under this Policy. The list of these vetted Generative AI tools and the scope of the approval will be posted on the YU ITS Portal. YU faculty and staff are expected to use any approved Generative AI tools in accordance with the scope of this Policy.
ITS may provide additional approval for AI tools where appropriate and for compelling business cases. Please contact helpdesk@yu.edu to raise requests for exceptions to this Policy.

1.6 Generative AI and Academic Integrity

At Yeshiva University, it is our shared responsibility to promote intellectual honesty and scholarly integrity, which could be undermined with the utilization of AI-generated content being presented as one's own work. The University offers many support resources regarding academic integrity.

1.7 Generative AI and Research

The guidelines above apply to all YU research activities. In addition, the following considerations and guidelines also extend to all research activity using AI:

- As with other tools and research methods, individuals who use Generative AI in research must be transparent regarding its use, in describing methods, acknowledgements, or elsewhere, as appropriate.
- Generative AI has been found to generate citations to papers that do not exist by authors who do not exist, as well as generate images for experiments that were never actually

conducted. Researchers are responsible for the accuracy of any content created by AI that is included in any research output and must use caution in utilizing AI output in research.

- Researchers are expected to follow the policies of journals, funding agencies and professional societies through which they report their research. For example, some journals, such as Science, currently explicitly prohibit text, figures, images or graphics generated by ChatGPT or any other AI tools.
- Researchers must avoid uploading, or using as input, any unpublished research data or other Internal or Restricted Information into a Generative AI tool.
    - When a researcher inputs unpublished work of any kind into a Generative AI tool, the unpublished work becomes part of the AI universe of data. Moreover, the researcher must recognize that the model may incorporate the unpublished work into responses to queries from other researchers. In addition, disclosure of unpublished work to an AI tool also may impede or prevent future intellectual property protection for the unpublished work or give rise to privacy violations.
- Researchers must not upload, or use as input, Internal or Restricted Information of the University or third parties. Generative AI tools may not provide protection for Internal or Restricted Information, and their use could violate contractual commitments.
    - This includes, e.g., unpublished manuscripts or funding proposals that researchers may be asked to peer review. NIH and NSF, among others, prohibit using Generative AI for peer review.
    - This also includes the Personal Information of research subjects. For example, inputting interview data to perform preliminary analysis creates the possibility that quotations or other information from research subjects could become public, and potentially, that subjects could also be identified.
- Researchers should be mindful that the output of AI tools may infringe the rights of third parties since the responses generated are pooled from already established works.

1.8 Guidance on Ethical Considerations

The integration of AI tools must align with ethical standards and policies to ensure academic integrity. Examples of unethical uses include:

1) **Lack of Transparency/Disclosure**: Instructors should inform students whenever they use AI tools. Clear disclosure of the technology's involvement in classroom activities helps maintain trust and avoid confusion.
2) **Generating or perpetuating Bias**: AI models may inherit biases from the data they are trained on, which can lead to biased or unfair information. Offensive, violent, or otherwise inappropriate content may surface when AI uses biased input. Instructors should be vigilant and work to counteract these to ensure unbiased information is not created, shared, or perpetuated.

3) **Lack of Accessibility**: Instructors must ensure that using AI tools does not exclude any students with disabilities from participating in class activities. The technology should be used in a way that is accessible to all students.
4) **Reduced Learning Engagement**: Overreliance on AI may hinder deep engagement and cause a lack of understanding of course materials, leading to incomplete learning experiences.
5) **Unauthorized Collaboration**: AI tools might be used for improper collaboration, blurring individual contributions, and violating academic integrity.
6) **Intellectual Property Infringement**: AI tools do not disclose whether the information they use and regurgitate is protected by copyright. Therefore, instructors should exercise caution when distributing texts or images created with AI.
7) **Privacy violation**: Users have no control over the data they provide to an AI tool. Feeding these tools with sensitive information that could lead to privacy violations must be avoided.

1.9 AI Policy regarding Third-Party Vendors

Third-party vendors perform certain services on behalf of and through a contract or agreement with Yeshiva University. YU may provide these companies with access to university records, data, or other information, including personal information or personal data, to carry out the services they are performing for YU.

1) During any contract negotiations with third-party vendors, YU will consider the usage of AI by the vendor and evaluate its inclusion as part of the agreement.
    a) YU ITS will document processes for procuring and approving the use of AI tools and platforms to ensure that they are thoroughly vetted and consistent with the university's mission and values.
2) YU will establish clear objectives for the use of AI by a third-party vendor in the service agreement or contract.
    a) AI use will be lawful, purposeful, accurate, reliable, and effective; safe, secure, and regulatory monitored; transparent; and accountable.
    b) The utilization of AI tools and platforms as established in the service agreement or contract will align with appropriate data governance practices and functional use areas across the organization.
    c) YU will address confidential information and the institutional record in any agreements with third-party service providers.
3) As appropriate, the use of AI by a third-party vendor will be authorized within the service agreement or contract.

1.10 Training and Awareness

YU is committed to promoting the use of AI in ethical ways through training and awareness programs. All users of AI are required to complete a training program on the ethical use of AI. This training program will cover topics such as:

- The responsible use of AI
- Ethical considerations
- Privacy
- Data protection
- Compliance with this policy.

1.11 Monitoring and Auditing

YU ITS will periodically monitor the use of AI to ensure compliance with this policy. Audits will also be carried out by relevant departments to assess adherence to ethical guidelines and identify areas for improvement.

- The YU ITS will document processes for monitoring and evaluating the use of AI tools and platforms to demonstrate oversight of implementation.

1.12 Review and Updates

This policy will be reviewed at least bi-annually, or more frequently, if necessary, to ensure it remains relevant and up to date with technological advancements and legislative changes. Recommendations for updates or improvements to the policy may be submitted to ITS.