University of Massachusetts Lowell

Policy Title:	Generative Artificial Intelligence Security and Privacy Policy
Policy Number:	IT-5-136
Responsible Office:	Information Technology
Responsible Position:	Chief Information Officer

I. Policy Statement

To protect UMass Lowell information from improper or illegal disclosure or reuse, non-public information may only be entered into, uploaded to, analyzed or otherwise processed by Generative Artificial Intelligence (GenAI) solutions when there is a legally binding agreement with the AI solution provider, reviewed and approved through the University's procurement processes, which includes data protection provisions commensurate with the sensitivity of the type of information. Non-public University information and data must not be entered into, uploaded to, analyzed or otherwise processed by free, public GenAI solutions. This requirement applies both when using freestanding GenAI technology tools and when GenAI functionality has been integrated by vendors into other software products.

All use of GenAI at the University must also comply with relevant contractual, legal, or regulatory obligations, as well as with any other University appropriate use policies governing (or disallowing) the use of GenAI for specific data and/or use cases. (See Applying the Policy section 1 below for more information about requirements for Confidential and Restricted data, such as data regulated under FERPA or protected by research data use agreements.) GenAI users at the University must take ultimate responsibility for content created with these tools, and they must understand and mitigate the risks associated with them. These risks may include AI "hallucinations," bias, unintentional plagiarism and intellectual property issues, and transparency concerns.

II. Purpose

The purpose of this policy is to ensure that the University's non-public data is not inappropriately or illegally used or disclosed by GenAI solutions and that members of the University community are aware of and manage other risks associated with GenAI technologies appropriately. GenAI technology offers tremendous potential to expand users' capabilities, efficiency, and productivity. Software vendors are rapidly embracing opportunities to enhance their products with GenAI features and functionality. Exploring and benefiting from GenAI is in UMass Lowell's interest. However, GenAI solutions can pose risks to the security, privacy and confidentiality of the University's information and can raise other ethical and compliance concerns. The University expects members of its Workforce and student body who use GenAI technologies to educate themselves about these concerns, to use GenAI ethically and compliantly, and to take responsibility for managing risks appropriately.

III. Scope

This policy applies to the use of GenAI solutions by university Workforce and students.

IV. Definitions

Generative Artificial Intelligence (GenAI) encompasses the range of artificial intelligence software tools that ingest large training datasets and rely on probabilistic models to generate new text, data, images, or video. The technology relies on Large Language Models (LLMs) that can process and respond to natural language prompts. Common applications include chatbots, text-to-image tools, text-to-video, and orchestration tools. These tools are rapidly developing and proliferating. As used in this policy, GenAI is intended to mean both the growing list of standalone tools and the incorporation of GenAI into other common software and platforms.

Public GenAI solutions for the purposes of this policy are the free versions available to the public. These services typically take users' queries and inputs as training data and may disclose them, in either their original or a modified form, to other users of the services. For this reason, they are not considered secure or permissible for use with non-public or sensitive data of any kind.

AI Hallucinations are instances where a GenAI system creates content or information that is factually incorrect, misleading or fabricated. Hallucinations are a consequence of the vast datasets used to train GenAI models (effectively the entire Internet, including all its correct and incorrect information) and the models' probabilistic nature.

Workforce is used in this policy to mean all members of the University community who are employed in any capacity – union and non-union employees; contractors and consultants; faculty - tenured, adjunct and emeritus; research staff and trainees; and any other agents of the university that function as members of its workforce.

Plagiarism refers to an author's ideas or words being copied or included in content without proper citation. When this occurs without specific intent, it is sometimes called Unintentional Plagiarism. Because it can be impossible for a user to know the original sources of GenAI-generated content, GenAI content may expose users to a heightened risk of committing Unintentional Plagiarism.

V. Applying the Policy

1. Security and Privacy

GenAI tools are trained on large datasets and may reuse, recombine, and present information in new contexts. Information entered in free, public GenAI solutions may be used as training data for the model and may be disclosed to other users in response to their queries.

For this reason, only data that is classified "Public" and can be disclosed to anyone with no limitations on access or reuse may be entered into free public GenAI solutions. No nonpublic University data of any kind may be entered into, uploaded to, analyzed or otherwise processed by GenAI solutions that do not provide contractual data security/privacy guarantees.

To process nonpublic University data using GenAI, there must be a formal agreement with the AI solution provider established through the University's procurement processes that includes appropriate data protection provisions. The agreement must establish that data entered into, uploaded to, analyzed and/or processed by the solution will be kept separate from other users' information, will not be used as general training data by the model, and will not otherwise be made available or accessible to other users of the solution. This requirement also applies for software vendors incorporating GenAI functionality into their products.

Data classified by the University as Restricted or Confidential, such as personally identifiable information, medical data, research data protected under data use agreements, or other information protected by regulation or contract, must not be entered into, uploaded to, analyzed or processed by GenAI solutions unless there has been specific legal and/or contractual review confirming that the GenAI agreement satisfies the regulatory or contractual data protection requirements.

As a type of software-as-a-service (SaaS)/cloud application, university-wide or departmental GenAI solutions must also go through the University's existing policies and review processes for selecting and onboarding SaaS/cloud vendors.

2. Evolving Policy, Legal and Regulatory Landscape

GenAI users should be aware that both University policy and the legal and regulatory landscape in the United States and other nations are evolving in response to the growing use of GenAI technology. Some examples of considerations in these areas include:

- **Academic integrity** – when use of GenAI is and isn't permissible in a learning environment;
- **Consent** – when GenAI is used as a virtual presence, such as serving as a virtual meeting attendee or transcription service to capture and summarize meeting discussion, wiretapping laws may be violated in jurisdictions (such as Massachusetts) that require prior consent of the parties; and
- **Copyright** – US law currently does not allow works made with GenAI to be copyrighted.

This list is intended to provide examples but is not exhaustive. Users must take care to check for the latest University policy, and state and national regulatory and legal information before beginning new GenAI projects.

3. Other Risks and Ethical Concerns

GenAI users at the University must bear final responsibility for content created with GenAI tools and decisions made using AI support, and they must understand and mitigate the associated risks and ethical concerns, such as:

- **AI Hallucinations** While solution providers can tune GenAI models to reduce the likelihood and prevalence of hallucinations, the way the models work makes eliminating hallucinations infeasible. For this reason, any GenAI output intended for dissemination, decision-making, correspondence or other contexts in which accuracy and appropriateness are important must receive comprehensive human review, fact-checking, and sign off before release. GenAI users bear the ultimate responsibility and accountability for the content they create with GenAI tools and the decisions they make by relying on GenAI-provided information.
- **Bias** – The large datasets used to train GenAI models, and the uneven nature of their content, can also cause GenAI to generate output that has captured and recapitulates biases found in the training data. This is especially a concern when GenAI may be used in contexts to support decision-making or may impact the treatment of individuals. Just as human users of GenAI tools must take ultimate responsibility and accountability for

the accuracy of GenAI output, they must also be responsible for identifying and addressing issues with bias and fairness in GenAI output.

- **Unintentional Plagiarism and Intellectual Property Concerns** – AI-generated content can incorporate copyrighted material or create outputs that closely resemble existing works. Use of such content without attribution or awareness of the source can result in unintentional plagiarism and intellectual property concerns.

- **Transparency –** As norms, policies, laws and regulations surrounding the use of GenAI continue to evolve, transparency is a best practice that can help manage some ethical concerns. The use of GenAI systems in any academic or administrative processes should be disclosed, and content generated by GenAI systems should be identified as such.

VI. Responsibility

All users of GenAI tools at the university are responsible for complying with the provisions of this policy. The UMass Lowell Chief Information Officer is the initial point of contact for questions about this policy.

VII. Other Resources

- US Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence
- National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0)
- OWASP AI Security and Privacy Guide

VIII. Related Policies and Procedures

- Data Classification Policy, IT-5-106
- University of Massachusetts Procurement Policy

Effective As Of:	July 2024
Next Review Date:	July 2027