

# ILLINOIS TECH

## GENERATIVE AI POLICY

Version:	1.0
Date of version:	June 18, 2026
Created by:	CTS
Approved by:	
Confidentiality Level	INTERNAL USE

# ILLINOIS TECH

## GENERATIVE AI POLICY

### PURPOSE AND SCOPE

Artificial Intelligence (“AI”) presents significant opportunities to enhance innovation, creativity, discovery, and efficiency across teaching, research, administration, and in faculty’s external professional activities that reference their university affiliation. As a relatively new and evolving technology, AI must be used in ways that align with university policies and applicable laws, safeguard confidential and personal information, protect restricted research data, and appropriately manage any associated risks to the university and its community.

The purpose of this policy is to establish core requirements for the ethical, lawful and responsible use of AI systems at Illinois Tech. This policy applies to all faculty, staff, students, contractors, affiliates and research collaborators who collect, access, generate or use data for AI-related purposes in connection with authorized University activities including, without limitation: (i) research projects involving machine learning, deep learning, and other AI-related methodologies; (ii) administrative and operational use of AI systems, (e.g., admissions, financial aid, academic advising); (iii) instructional use of AI tools and data sets in classrooms or teaching environments; and (iv) collaboration with external partners involving AI data.

### DEFINITIONS

For the purposes of this policy:

“AI System” refers to any engineered or machine-based system or functionality designed to achieve specific objectives by generating outputs such as text, images, or predictions, or by making recommendations or decisions that influence human actions or impact real or virtual environments. AI Systems may operate with varying levels of autonomy.

“**Confidential Information**” includes any information whose access, use, or disclosure is restricted by contract, applicable law, or university policy. This encompasses but is not limited to: Restricted Research Data; student and personnel records; Personally Identifiable Information; health records; alumni and donor data; university financial information; computer passwords; and any other proprietary or nonpublic information belonging to the university. For additional guidance, refer to the Policy on the Confidentiality of University Records and Information.

“**Personally Identifiable Information**” (PII) means any data relating to an individual that identifies, or can reasonably be used to identify, that individual—either directly or indirectly—by reference to identifiers such as a name, social security number, A number, location data, online identifier, biometric identifier, biometric information, or other personal characteristics. This also includes de-identified information that could reasonably be re-associated with an individual, including through the use of AI systems.

Restricted Research Data refers to any data used in university research that is subject to limitations on access, use, or disclosure due to contract terms, applicable law, or university policy.

## **POLICY**

**Faculty and staff members who wish to use an AI System must:**

- Ensure that proposed use of the AI System is permitted by and compliant with applicable: (i) University policies; (ii) federal, state and municipal laws and, if applicable, international guidelines (e.g. Illinois Biometric Information Privacy Act (BIPA), Family Education Rights Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR), the Illinois Personal Information Protection Act (PIPA); and (iii) applicable sponsor requirements and research protocols, such as IRB and institutional policies.
- Provide proper attribution when using an AI System to generate content that is included in a scholarly publication or submitted to any organization, publication, or body that requires authorship disclosure unless attribution is specifically prohibited by sponsor.
- Review AI-generated output regularly for accuracy and suitability, and revise or update it as needed to ensure it meets the intended purpose.

- Ensure safeguards against bias or discrimination if the AI System processes PII or makes decisions that could affect an individual's legal rights or physical safety. In such cases, the system must be regularly tested to confirm compliance with applicable laws.

For AI Systems used in University Operations - including academic functions, administrative processes, health & safety, infrastructure & services, and strategic resource management- faculty and staff must also adhere to the following:

- If the system (i) processes Confidential Information, PII, or Restricted Research Data, or (ii) performs actions that may affect legal rights or physical safety:
  - Undergo an information security review through OTS Cybersecurity process, applicable to either vendor-provided or internally developed systems.
  - Ensure that the university retains ownership of both data and Intellectual Property (IP), even after it is processed by an AI tool.
  - Ensure that using the AI service does not transfer ownership of research ideas, drafts, inventions, or creative work to the AI service or vendor.
- Faculty and students should understand that uploading IP to an AI tool may expose it to licensing risks unless the university has a contract that protects ownership.
- If the University does not own the data that will be analyzed by AI, obtain the prior express written permission of the data owner before processing such data.

**Contact:** for questions or guidance related to this policy, please contact [CTS@illinoistech.edu](mailto:CTS@illinoistech.edu) .

**Review Frequency:** Please note that this policy is continuously in development, as technology, laws, and the university and research communities evolve.