

AI Guidance Framework

UNIVERSITY OF ILLINOIS SYSTEM

July 2026

Purpose

In July 2023, the University of Illinois System published its initial Generative AI Assessment and Recommendations Report in response to the rapid emergence of tools like ChatGPT. That foundational document established principles and identified opportunities and risks across teaching, research, healthcare, and operations.

This framework represents the next iteration of that guidance. As AI technology has matured and expanded beyond text-based chatbots, we have condensed and updated our approach to provide actionable, vendor-agnostic guidance. Rather than prescribing specific tools, which evolve rapidly, this document establishes principles and practices that enable innovation while managing risk. Each university should adapt this guidance to their specific context and needs. Developed collaboratively across the System, this framework serves as a shared baseline: universities and shared governance bodies are encouraged to tailor it locally and to channel feedback upward, so the guidance continues to improve.

Artificial intelligence is rapidly becoming a foundational capability for leading universities, shaping how knowledge is created, taught, discovered, and applied. For the University of Illinois System, effectively leveraging AI is essential to maintaining our competitiveness, advancing our public mission, and preparing students, faculty, and staff for an AI-enabled world. While managing risk, privacy, and ethical concerns is critical, our objective extends beyond avoidance of harm. We seek to enable excellence in teaching and learning, accelerate research and innovation, enhance healthcare delivery, and improve operational effectiveness through the responsible and strategic use of AI while ensuring its use remains aligned with our institutional values. This guidance applies to those who develop AI as well as our university communities who build AI systems, agents, or workflows share responsibility for sound development practices including training-data selection, bias mitigation, model governance, secure development, and responsible deployment.

Understanding AI Today

Artificial Intelligence (AI) is a machine-based system that can make predictions, recommendations, or decisions to achieve human-defined objectives. AI systems perceive their environment, process that information into models, and use those models to inform actions.

Sources: 15 U.S.C. § 9401(3); NIST AI Risk Management Framework (AI RMF 1.0); FDA Artificial Intelligence and Medical Products guidance.

Two Fundamental Approaches

AI systems can be categorized by how they produce outputs:

Deterministic AI: Produces consistent, predictable outputs given the same inputs. These systems operate on predefined rules or fixed mathematical relationships with no randomness. Examples include fraud detection systems, recommendation engines, and rule-based diagnostic tools. The same input always yields the same result.

Generative AI: Incorporates uncertainty and statistical inference, generating outputs based on probability distributions learned from data. The same input may produce different outputs. Generative AI (chatbots, image generators, code assistants) is the most prominent example. *Because outputs vary and can include errors or fabrications ("hallucinations"), human verification is essential.*

Many modern systems combine both approaches—using deterministic rules for structured tasks while incorporating probabilistic decision-making for adaptability.

Sources: Towards Data Science, "Deterministic vs. Probabilistic Deep Learning" (2025); Capgemini AI Futures Lab, "The Evolution of Hybrid AI" (2025); NIST AI 100-3 Glossary.

Common AI Categories

AI capabilities are often described by function. These categories are not mutually exclusive:

- **Generative AI:** Creates new text, images, audio, video, and code from prompts
- **Predictive AI:** Analyzes data to forecast outcomes and identify patterns
- **Computer Vision:** Interprets visual information from images and video (single-modality)
- **Multimodal AI:** Processes multiple data types (text, images, audio, video) simultaneously
- **Agentic AI:** Performs autonomous multi-step tasks with minimal human intervention
- **Embedded AI:** AI features integrated into existing software platforms

Sources: IBM, "What is Multimodal AI?" (2025); Roboflow, "Multimodal Models and Computer Vision" (2023).

Guiding Principles and Ethical Considerations

The University of Illinois System is committed to leveraging AI in ways that reflect our academic values, uphold public trust, and promote positive societal impact. Ethical use of AI means applying the technology responsibly, transparently, and with respect for the individuals and communities we serve. It requires thoughtful consideration not only of what AI can do, but what it should do in the context of our mission.

Principle	What This Means
Mission Alignment	Use AI in ways that advance the University's teaching, learning, research, healthcare, and public service missions while preparing our university communities for responsible participation in an AI-enabled society and workforce. When evaluating an AI use, consider how it serves these missions and our institutional values—not only whether it is permitted.
Human Oversight and Autonomy	You are responsible for all AI inputs and outputs you use or share. Verify factual claims, validate citations, and check for hallucinations and bias; maintain human review of consequential decisions. AI should support, not replace, human judgment, especially in academic, clinical, and administrative decision-making. As agentic AI acts with greater autonomy, accountability remains with the people

	and units that deploy it: ensure autonomous actions are auditable and traceable and maintain oversight of both individual outputs and the systems that produce them, including AI features embedded in software you may not directly control. Establish clear accountability and remediation procedures for harm or bias.
Transparency and Honesty	Disclose AI use when appropriate, especially in academic and clinical settings. When AI meaningfully contributes to academic, clinical, research, or administrative work, that role should be disclosed to maintain trust and academic integrity. Communicate the technology's capabilities, limitations, and potential biases to users and stakeholders. To the extent practical and appropriate provide transparency in algorithms and decision-making processes to enhance trust and accountability.
Privacy, Security, and Data Stewardship	Protect high-risk data. Never input sensitive, confidential, regulated, or proprietary information into non-approved AI tools. Protecting privacy and minimizing unnecessary data exposure is a core ethical obligation. Ensure AI systems incorporate privacy and security by design, comply with applicable laws, and implement strong privacy and security measures to prevent unauthorized access. Data used to train, refine, or prompt AI must be handled in alignment with university policies and legal requirements.
Fairness & Inclusion	Recognize AI can reflect biases from training data. Critically evaluate outputs, especially for decisions affecting people. AI must not be used in ways that create or reinforce discriminatory outcomes. Use inclusive design practices, identify and mitigate biases, and seek input from diverse stakeholders to prevent discrimination and address potential barriers or unintended consequences. Users should actively evaluate outputs for potential bias and engage diverse perspectives when deploying or interpreting AI systems.
Monitoring and Awareness of Impact	AI systems can degrade or drift over time. Regularly reassess deployed AI tools to ensure continued performance and accuracy. Initial validation does not guarantee ongoing reliability; periodic review is essential to maintain system effectiveness and identify emerging issues. AI tools can shape behaviors, decisions, and outcomes. Users should consider downstream impacts, including unintended consequences, and avoid applications that could cause harm or diminish equity, trust, or safety.
Continuous Learning and Reflection	AI technologies evolve rapidly and best practices continue to mature. Establish feedback mechanisms to capture user insights on system performance, emerging risks, and unintended consequences. Integrate feedback into ongoing governance processes to adapt policies and practices as the technology and our understanding advance. Users are expected to stay informed, reflect critically on their use of AI, and raise concerns when potential ethical issues arise.

Ethical use is not a static requirement—it is an ongoing commitment. By foregrounding ethical principles, the University of Illinois System ensures AI adoption that advances innovation, supports our institutional mission, and upholds the values of a public research university.

Data & Privacy

Using Non-University-Approved AI Tools

Public AI tools—such as consumer chatbots, free AI assistants, and publicly accessible generative AI services—have significant data privacy limitations. Information you enter may be stored, used for model training, or accessible to the vendor. The following guidance applies to these public tools:

- **You MAY input:** Publicly available information, general questions, non-sensitive drafts
- **You must NEVER input:** Student records (FERPA/GDPR), patient information (HIPAA), Social Security numbers, financial account data, research data with PII, proprietary/confidential information, export-controlled data

Important: This should be considered a minimum system-wide baseline. This list is **not exhaustive**. When in doubt, don't input it consult your university security, privacy office, or Digital Risk Office. Your university's [data classification](#) standards define categories of university data and their sensitivity; consult it to determine which uses and tools are appropriate for the data you are working with.

Using University-Approved AI Tools

Some AI tools have been vetted and approved by your university for use with certain types of non-public data. These tools have been reviewed by the university and have appropriate contracts, security controls, and data protection in place. *If your university has approved a specific AI tool for certain data types, that tool may be used for data that would otherwise be prohibited in public AI tools.*

Before using any AI tool with non-public data, verify: (1) the tool is on your university approved list, (2) the specific data types are permitted, and (3) you understand any usage restrictions.

To see what is currently approved please refer to: [Chicago](#), [Springfield](#), and [Urbana](#)

Intellectual Property and Ownership

AI raises unresolved questions about ownership and authorship. Under current U.S. Copyright Office guidance, purely AI-generated content may not be eligible for copyright protection, and entering unpublished scholarship, inventions, or other university intellectual property into AI tools may compromise ownership rights or confidentiality. Do not assume you own AI-generated outputs, and do not claim AI-generated work as solely your own. Follow university IP policy and applicable journal, funder, and professional authorship standards, and consult University Counsel or your Office of Technology Management for consequential matters.

AI Training and Literacy

Each university should develop and collaborate on AI skills training for faculty, staff, researchers, and students. Training should span institutional domains and be based on a maturity model of developing AI literacy, AI competency, and AI expertise. Wherever possible, training should be short, modular, and role-specific, with examples tied to real job functions. Suggested topics:

- **AI Fundamentals:** What AI is; deterministic vs. probabilistic; common categories
- **Data Privacy & Security:** What can/cannot be entered; permissions; approved tools; data retention
- **Data and Subject Matter Literacy:** Understand the nuances of the data being used
- **Critical Evaluation:** Verifying outputs; recognizing hallucinations; understanding bias
- **Effective Prompting:** Writing clear prompts; iterating for results

- **Ethical Use & Attribution:** Disclosure; academic integrity; IP implications
- **Role-Specific Applications:** Practical examples for teaching, research, healthcare, admin
- **Emerging Risks:** Deepfakes; AI-enhanced phishing; staying current

Consider making training a requirement for those working with sensitive data or procuring AI tools.

Domain Guidance

Teaching & Learning

- **Communicate expectations clearly:** Include AI use policies in syllabi
- **Teach AI literacy:** Help students and faculty understand AI capabilities and limitations
- **Rethink assessment design:** Focus on process and critical thinking
- **Use AI detection tools cautiously:** They produce false positives
- **Model appropriate use:** Demonstrate professional AI use in your field

Research

- **Follow funder requirements:** Adhere to sponsor policies on AI use
- **Secure data & infrastructure:** Coordinate with IT, especially for sensitive data
- **Document AI use:** Maintain records for reproducibility and traceability
- **Verify AI output:** AI can fabricate citations and misrepresent findings
- **Disclose AI use in publications:** Follow journal and professional authorship policies

Healthcare

- **Use only approved clinical AI tools:** Must be HIPAA-compliant and clinically reviewed
- **Maintain clinical judgment:** AI assists but does not replace decision-making
- **Never enter PHI into non-approved tools:** Violates HIPAA and university policy
- **Document AI-assisted decisions:** Note when AI contributed to clinical work
- **Report concerns:** Alert clinical informatics of concerning outputs

Operations & Administration

- **Leverage approved tools first:** Use existing vetted institutional solutions before procuring duplicates—this reduces risk, cost, and redundant reviews
- **Vet AI tools before procurement:** Work with IT security, privacy, and procurement
- **Understand AI in existing tools:** Many platforms now embed AI features
- **Start with low-risk use cases:** Draft communications, summarize documents
- **Protect university data:** Use non-public data in tools approved for that classification of data
- **Consult functional area experts:** Laws can prevent use of AI in operations and administration.

Potential Opportunities

When implemented thoughtfully, AI offers significant opportunities:

Domain	Opportunities
Teaching & Learning	Personalized tutoring; accessible learning materials; preparing students for AI workplaces
Research	Accelerated literature review; pattern discovery; novel hypothesis generation
Healthcare	Reduced provider burnout; faster diagnosis support; more time for patient care

Operations	Streamlined processes; improved service; better data-driven decisions
------------	---

Key Risks to Manage

Risk	Mitigation
Data Leakage	Use approved enterprise tools for sensitive work
Over Sharing	Always verify permissions granted to data sources and users
Inaccuracy/Hallucinations	Always verify AI outputs; check original sources
Bias & Fairness	Don't use AI as sole input for consequential decisions
Intellectual Property	Don't assume ownership of AI-generated content
Model Drift	Monitor performance; re-validate periodically
Deepfakes & Spoofing (Fraud)	Verify identity through multiple channels

Getting Started

1. **Develop AI skills training** for your university
2. **Review approved tools list** on your university IT website
3. **Start experimenting** with low-risk tasks using public data only
4. **Share what works** with colleagues
5. **Ask questions**, contact your contact your local IT support and/or your university IT teams

Questions & Resources

For tool vetting, security questions, or policy guidance:

- [University of Illinois Chicago Security & Privacy](#), security@uic.edu
- [University of Illinois Springfield Security & Privacy](#), securitysupport@illinois.edu
- [University of Illinois Urbana-Champaign Security & Privacy](#), securitysupport@illinois.edu

Intellectual Property and Ownership support:

- [University of Illinois Chicago Library](#)
- [University of Illinois Chicago Office of Technology Management](#)
- [University of Illinois Springfield Library](#)
- [University of Illinois System Legal Counsel](#)
- [University of Illinois Urbana-Champaign Library](#)
- [University of Illinois Urbana-Champaign Office of Technology Management](#)

This framework is intended for the U of I System as a whole. To support adoption, shorter audience-specific summaries, quick-reference materials, and role-based examples of appropriate and inappropriate use will be developed as companion resources for faculty, staff, administrators, researchers, and students.

This guidance will be updated as AI technology and best practices evolve.

Last Updated July 15, 2026