

UNIVERSITY OF UTAH

Artificial Intelligence Use Guidelines

Responsible Office: Office of Artificial Intelligence

Guidance Officer: Chief AI Officer

Effective Date: September 2026

Last Revised: September 2026

Version: 1.0

1. PURPOSE

The University of Utah is committed to the responsible advancement and use of artificial intelligence (AI) to support research, scholarship, creative activity, education, clinical care, administration, and service. The University recognizes AI literacy as an increasingly important dimension of undergraduate, graduate, and professional education, and research activities. Students and researchers should have opportunities, appropriate to their disciplines and programs of study, to develop the capacity to use AI critically, ethically, transparently, and effectively; to evaluate AI-generated information for accuracy, bias, and reliability; and to understand when AI use enhances—and when it may undermine—human judgment, creativity, learning, and professional responsibility.

The University affirms that AI systems must be developed and deployed responsibly to advance human well-being, academic freedom, learning and knowledge production, equity, transparency, and public trust. The University views AI not merely as a tool but as essential infrastructure — including data, models, systems, software, and hardware — that fosters innovation and the social good. Furthermore, the University seeks to ensure that AI platforms are safe, secure, reliable, and beneficial for the University community.

This guidance establishes institutional standards and expectations governing the acquisition, development, and deployment of AI technologies across the University. The goal of this guidance is to help members of the University community to balance innovation with privacy, security, compliance, integrity, responsible use, and public trust.

2. SCOPE

This Guideline applies to:

- All University faculty, staff, students, researchers, contractors, affiliates, and agents (“University individuals”);
- All AI tools or systems used in connection with University business, including in research, instruction, clinical operations, administration, and process improvement;
- AI capabilities embedded within licensed or enterprise software;
- Locally developed AI systems;
- AI use that involves University information technology resources or Institutional Data.

This guidance is intended to govern the use of AI in connection with University business or the use of University resources or Institutional Data. It is not intended to regulate an individual’s personal use of AI tools outside the scope of University activities, except where otherwise governed by applicable University regulations.

This guidance supplements, and does not replace, applicable University policies and rules, including, but not limited to:

- [Policy 4-001: Institutional Data Management](#)
- [Policy 4-004: University Information Security](#)
- [Rule R4-004A: Acceptable Use](#)
- [Rule R4-004C: Data Classification and Encryption](#)
- [Policy 3-100: Procurement](#)
- [Policy 4-050 and related rules: University Software](#)
- [Policy 7-001: Research Misconduct](#)
- [Policy 7-020: Determining Authorship](#)
- [Policy 6-410 Academic Integrity](#)
- Applicable federal and state law, including but not limited to [HIPAA](#), [FERPA](#), and [GRAMA](#)

For clarification or novel use cases not addressed in this guidance, contact Alsupport@utah.edu

3. DEFINITIONS

For purposes of this guideline, the following definitions apply. In the event of any inconsistency between a definition in this guideline and a definition in University regulations, the definition set forth in the applicable University regulation shall prevail.

Artificial Intelligence (AI): A machine-based system designed to perform tasks that typically require human intelligence, including but not limited to generating content, making predictions, analyzing data, or executing actions.

Generative AI: AI systems capable of producing new content (e.g., text, images, audio, code, or other outputs) based on information learned from training data.

Agentic AI: AI systems capable of planning, making decisions, and executing tasks toward defined goals with varying degrees of human direction and oversight

Responsible AI: AI that is developed and used in a manner that protects privacy, security, civil rights, and civil liberties, and promotes fairness, accountability, transparency, and appropriate human oversight.

Institutional Data: Data acquired or maintained by University functional areas in the performance of official administrative job duties, as defined in [Policy 4-001](#).

Restricted Data / Sensitive Data: Data classifications defined in [Rule R4-004C](#).

Approved AI Tool: An AI tool for which the required University review processes have been completed and that is listed on the official inventory maintained at <https://ai.utah.edu/tools/index.php>.

High-Risk AI Use: An application of AI that may materially affect an individual's rights, privacy, opportunities, academic standing, employment, financial interests, access to University services, or other significant interests, and therefore requires heightened review, oversight, and accountability.

Consequential Decision: A decision that materially affects an individual's academic standing, admission, financial aid, employment, access to University programs or services, or disability accommodations.

Meaningful Human Review: Review by a qualified individual with sufficient authority and understanding of the relevant information, the AI system's role, capabilities and limitations,

and the process used to produce the output recommendation, enabling that individual to exercise independent judgment and modify or overturn the outcome when appropriate.

4. GUIDANCE STATEMENT

Members of the University community may develop and/or use AI tools to advance the University's mission, provided such development/use:

1. Complies with applicable laws, regulations, contracts, and sponsor requirements;
2. Adheres to [University data classification and security standards](#);
3. Uses [reviewed and approved AI tools](#) when conducting University business;
4. Maintains meaningful human oversight and ensures that final decision-making authority remains with qualified individuals, particularly in high-risk or consequential contexts
5. Upholds academic integrity and education and research standards;
6. Protects privacy, intellectual property, and institutional interests.
7. Promotes responsible AI.

4.1 AI Use Decision Framework

Prior to deploying or using AI in connection with University business, individuals should evaluate the following:

- **Purpose and Use Case** – What is the intended use? Does the intended use align with University mission, applicable policies, and the intended business or academic purpose?
- **Data Classification** – What type of data will be used (e.g., Public, Sensitive, Restricted)? Is the AI tool approved for that data classification and intended use?
- **Tool Approval** – Is the AI tool included on the University's approved inventory? If not, it must be submitted for review and approved before use.
- **Risk Level** – Does the proposed use present minimal, moderate, or high risk? Could it materially affect an individual's academic standing, employment, financial interests, access to University services, or other significant interests?
- **Human Oversight** – What level of human review is appropriate? If the AI use could influence a high-risk or consequential decision, is meaningful human review in place before any final decision or action is taken?

The level of review and oversight should be proportionate to the reasonably foreseeable risks and potential impacts of the proposed use of AI. Where uncertainty exists regarding

data classification, risk level, tool approval, or appropriate oversight, individuals should consult the Office of Artificial Intelligence or the appropriate Data Steward, or other relevant University offices prior to implementation.

5. GOVERNANCE AND RESPONSIBILITIES

5.1 Office of Artificial Intelligence (OAI)

The Office of Artificial Intelligence provides institutional leadership for AI strategy, governance, and best practices, and for the coordination of University AI guidance. Specifically, OAI:

- Develops and maintains AI guidance and best practices;
- Coordinates University-wide AI standards;
- Maintains the approved AI tools inventory;
- Leads AI literacy, training, and community engagement initiatives;
- Facilitates strategic partnerships with industry and government; and
- Promotes responsible and innovative AI adoption across the institution.

5.2 [University Information Technology \(UIT\)](#)

- Conducts technical and security evaluations of AI tools;
- Manages enterprise AI configurations;
- Maintains operational oversight of approved tools; and
- Provides technical support through the [UIT](#) and [DLT](#) Help Desks.

5.3 [Information Security Office \(ISO\)](#)

- Conducts security risk assessments;
- Oversees incident response involving AI systems; and
- Monitors compliance with security requirements.

5.4 Data Stewards

Data Stewards are defined in [4-001](#).

5.5 Office of Research Security and Compliance

The Office of Research Security and Compliance oversees AI use within research activities, including compliance and sponsor-related obligations.

5.6 Advisory and Coordination

The OAI coordinates with relevant University stakeholders, including the AI Leadership Team, Office of General Counsel, University Information Technology, Purchasing, Health Sciences, the Office of the Vice President for Research, the Offices for Faculty, the Graduate School, Undergraduate Studies, and other academic and administrative areas, to support responsible AI adoption, risk management, and compliance with institutional, contractual, and legal requirements.

The AI Leadership Team provides strategic advice and promotes cross-institutional alignment for University AI initiatives.

6. APPROVED AI TOOLS AND PROCUREMENT

6.1 Use of Approved Tools

When conducting University business using AI with Institutional Data, University individuals must use University-approved AI tools whenever required by the applicable data classification, institutional regulation, or University guidance. Approved enterprise tools are configured to safeguard University data and prevent unauthorized training on institutional data.

The current inventory is maintained at:

<https://ai.utah.edu/tools/index.php>

6.2 Requesting New Tools

If a required AI tool is not listed in the current inventory:

- University individuals must complete the [AI Tool Form](#).
- The tool will undergo review by the Office of Artificial Intelligence, University Information Technology, Information Security, and other appropriate University offices based on the proposed use and associated risks.

- Use is not permitted until approval is granted.

All acquisitions must comply with [Policy 3-100](#) and related procurement rules and processes, including coordination with University Purchasing Services.

6.3 AI Impact Assessments (AIA)

High-risk AI initiatives may require completion of an AI Impact Assessment before deployment, as determined by the Office of Artificial Intelligence in coordination with relevant University offices.

The assessment may evaluate:

- Purpose and intended outcomes;
- Data sources and classification;
- Potential bias or disparate impacts;
- Privacy, security, and cybersecurity risks;
- Accessibility and potential impacts on individuals with disabilities, where applicable;
- Human oversight and meaningful human review;
- Transparency, explainability, and communication to affected individuals, where appropriate; and
- Appeals, recourse, or existing University review processes for affected individuals.

The OAI, in coordination with relevant units, will determine when an AIA is required. Additional guidance, examples, and implementation resources for AI tool reviews and AI Impact Assessment are available through the OAI.

7. AI DATA USE REQUIREMENTS

University individuals should review [Rule R4-004C](#) to determine the applicable data classification, apply data minimization principles, and follow the data governance requirements outlined in [Policy 4-001](#).

Only the minimum data reasonably necessary to accomplish the approved purpose should be provided to an AI system.

These requirements apply to any AI use conducted in connection with University business, Institutional Data, or enterprise AI services, regardless of the device used to access the system.

7.1 Approved Use with Public Data

University-approved enterprise AI tools are currently approved for use with public data, unless explicitly designated otherwise.

Approval of an AI tool does not imply authorization to use sensitive or restricted data within that tool.

Public data is defined in R4-004C and generally includes information intended for public disclosure or approved for release without restriction. Examples may include:

- Public-facing website content;
- Published research;
- Course descriptions available through the Course Catalog;
- Marketing materials; and
- Public reports.

University-approved AI tools may be used with public data unless otherwise restricted.

7.2 Sensitive and Restricted Data — Authorization Required

Sensitive or Restricted data are defined in R4-004C and may only be used with AI tools that are explicitly approved for that classification and only under approved contractual, technical, and governance safeguards.

Most AI tools are not appropriate for Sensitive or Restricted data.

Use of unapproved AI tools with protected data may expose the University to security, regulatory, contractual, or reputational risk.

7.3 Required Safeguards for Sensitive or Restricted Data

Sensitive or Restricted data may only be entered into AI systems when:

- The AI tool is explicitly approved for that classification;
- Approval is obtained from the appropriate Data Steward and, where required, the Chief Data Officer or Data Trustee;
- Required contractual safeguards are executed;
- Technical security controls meet University standards; and
- Data storage locations comply with institutional security requirements.

- Only the minimum amount of Sensitive or Restricted data necessary for the approved purpose should be shared with an AI tool.

Where applicable:

- Business Associate Agreements (BAA) must be in place;
- Data Use Agreements (DUA) may be required;
- Vendors must contractually prohibit training on University data unless expressly authorized; and
- Vendors must provide sufficient transparency into model capabilities, data-handling practices, and limitations to enable institutional risk evaluation.

7.4 AI Training and Model Development Using Institutional Data

Use of Institutional Data for AI model training, fine-tuning, evaluation, or development — whether internal or through third-party vendors — requires documented review and approval consistent with [Policy 4-001](#).

Requests must identify:

- Purpose and intended use of the model or AI application;
- Data elements and classification;
- Data minimization practices;
- Governance and oversight mechanisms; and
- Model lifecycle considerations including retention, retraining, access controls, and retirement, where applicable.

Institutional Data may not be used for AI training without explicit authorization.

Questions regarding tool approval, data classification, or high-risk AI use should be directed to the OAI and the Chief Data Officer prior to implementation.

8. AI IN RESEARCH

AI may be used in research activities subject to University standards and sponsor requirements. This section applies both when AI is used as a research tool and when AI systems, outputs, interactions, or societal effects are themselves the subject of research.

Researchers must:

- Confirm data classification and governance requirements;
- Verify sponsor policies regarding AI use;
- Ensure the accuracy and integrity of AI-generated outputs;
- [Document AI usage](#) where appropriate; and
- Maintain responsibility and accountability for the accuracy, integrity, and originality of all research content, regardless of whether AI tools are used.

AI tools may support but may not replace substantive intellectual contributions required for grant proposals or scholarly work.

AI does not qualify for authorship under [Policy 7-020](#).

[Researchers are responsible for complying with applicable University policies](#), sponsor requirements, publisher requirements, and disciplinary standards regarding the disclosure of AI-assisted content. Failure to comply with applicable disclosure requirement may constitute research misconduct or other policy violations, as determined under existing University policies and procedure.

9. AI IN TEACHING AND LEARNING

Faculty retain authority to determine whether and how AI tools may be used in their courses, consistent with University regulations. Expectations for AI use should be clearly communicated in course syllabi and, where appropriate, in assignment instructions. For guidance on course policies, assignments, and responsible instructional use of AI, faculty and instructors should consult the [Martha Bradley Evans Center for Teaching Excellence](#).

Faculty and out instructors are encouraged to model the responsible and transparent use of AI in teaching, course development, assessment, and other educational activities, while remaining accountable for the accuracy, quality, and integrity of instructional materials. Students using AI must comply with academic integrity rules and course expectations.

Students may use non-approved tools for personal study purposes. Coursework involving Institutional Data or University business, however, must use approved tools or otherwise comply with applicable University requirements.

The University seeks to prepare graduates to thrive in an AI-enabled world by fostering AI literacy appropriate to their disciplines. Students should have opportunities to understand AI capabilities, limitations, verification practices, ethical considerations, bias risks, and appropriate use.

AI-detection tools should not be treated as conclusive evidence of academic misconduct. Academic integrity determinations should be based on the totality of available evidence and established University procedures. Instructors should not upload student work to unapproved third-party AI detection services.

9.1 Transparency, Disclosure, and High-Risk Academic Uses

Academic and administrative areas deploying AI systems in high-risk academic or student-impact contexts should ensure affected individuals are informed and protected.

High-risk contexts are those in which AI materially influences decisions that affect a person's academic standing, employment, access to opportunity, finances, or legal rights. Examples include, but are not limited to:

- AI-assisted grading or academic evaluation;
- Academic integrity determination processes;
- Admissions, scholarship, or financial aid decisions;
- Decisions affecting student progression, standing, or dismissal;
- Decisions affecting employment; and
- Student placements, or disability accommodation determinations.

When AI systems materially inform or influence such decisions, affected individuals should be informed of:

- The use of AI in the decision process;
- The role and scope of human review and oversight; and
- How to request meaningful human review, correction, or appeal consistent with applicable University requirements and procedures.

9.2 Expectations for AI Use in Grading and Assessment

When AI is used to support grading or feedback, instructors retain full responsibility for grades and must follow the [Guidelines for Responsible Use of AI in Grading](#). Key expectations include:

- **Human authority & oversight:** AI may assist instructors by supporting grading activities (such as preliminary rubric scoring, draft feedback, or pattern identification), but instructors remain solely responsible for evaluating student work and assigning final grades.

- **De-identification & privacy:** Student work processed by AI should be de-identified unless the approved AI tool and specific use case have been expressly authorized to process identifiable student information. Gradebooks or identifiable student datasets should not be uploaded except as expressly authorized.
- **Approved tools only:** Instructors should use only institutionally approved AI tools for grading and feedback. Instructors should not use personal/consumer AI accounts for grading tasks.
- **Validation & monitoring:** Instructors should pilot and validate AI assistance before course-wide use (e.g., compare AI suggestions to human grading on representative samples), periodically spot-check for drift or bias, and document the tool used and validation approach.
- **Transparency with students:** Instructors should disclose the use of AI in course materials, describe its intended role in grading or feedback, explain applicable privacy protections, and inform students how they may request meaningful human review through established University processes.
- **Appeals & documentation:** Instructors should maintain documentation of AI use and provide students access to established grade appeal processes; instructors should be able to explain how final grades were determined.

10. AI IN ADMINISTRATIVE OPERATIONS

AI tools may be used to improve administrative processes, communications, and operational efficiency, provided such use:

- Employs approved tools where required;
- Protects institutional data;
- Maintains appropriate human oversight;
- Ensures that AI does not serve as the sole basis for consequential administrative decisions affecting individuals; and
- Complies with records retention obligations.

11. AI IN MEETINGS AND COLLABORATION

Approved AI meeting tools currently include only:

- Microsoft Teams Premium
- Zoom AI Companion

When a non-University host or attendee introduces an AI assistant into a meeting, University participants should consider whether sensitive or restricted information may be discussed. If sensitive or restricted information is reasonably expected to be discussed, participants should request that the AI assistant be disabled for that portion of the meeting or otherwise take appropriate steps to protect University information.

12. RECORDS AND PUBLIC DISCLOSURE

AI interactions conducted as part of University business may constitute government records under the Utah Government Records Access and Management Act [GRAMA](#).

In certain circumstances, records associated with federally funded research, federal contracts, or shared federal data may also be subject to applicable federal disclosure laws.

University individuals must exercise care when entering information into AI systems and ensure compliance with record retention and disclosure obligations under state and federal law. The retention of AI-generated prompts, outputs, summaries, and related records should be determined by their business purpose and applicable records retention requirements, not by the fact that AI was used.

13. SECURITY AND INCIDENT REPORTING

Suspected data exposure, misuse, or security incidents involving AI tools must be reported promptly to:

University of Utah Information Security Office
iso@utah.edu
801-587-1925

Hallucinations, inaccurate outputs, or other AI performance issues should be reported through this process only when they result in, or reasonably could result in, a security, privacy, safety, legal, discriminatory, or material operational risk.

14. PROHIBITED USES

The following uses of AI are prohibited:

- Deployment of AI systems that discriminate on the basis of protected characteristics under federal or state law;

- Use of AI to knowingly deceive, impersonate, or create synthetic content for University business in a manner that misrepresents identity, authority, or official University communications;
- Fully autonomous decision-making in high-risk contexts without human review;
- Use of AI systems that conflict with academic freedom, civil rights, or established University regulations or guidance;
- Use of AI tools to fabricate research data in violation of [Policy 7-001](#): Research Misconduct, falsify academic records, or misrepresent authorship; and
- Circumventing institutional data protections through unauthorized AI services.

Any other use that violates federal or state law or university regulations.

15. INFRASTRUCTURE EFFICIENCY AND RESOURCE STEWARDSHIP

The University recognizes that AI systems require significant computational, storage, and network resources. The University evaluates the efficiency, performance, and operational demands of AI technologies to support responsible resource stewardship, sustainability, cost management, and long-term institutional resilience.

Efforts include:

- Coordinated planning for AI-related infrastructure and compute capacity;
- Modernization and optimization of cyberinfrastructure;
- Enterprise management of AI platforms to reduce redundancy and unmanaged tool proliferation;
- Operational efficiency practices at the Center for High Performance Computing (CHPC); and
- Consideration of energy efficiency and sustainable use of computing resources, where appropriate.

16. MONITORING AND ENFORCEMENT

AI use conducted in connection with University business, Institutional Data, and University enterprise systems may be subject to monitoring or review—consistent with applicable law, University regulations, academic freedom, civil rights and liberties, and reasonable expectations of privacy—to ensure compliance with contractual, legal, security, and

institutional requirements. Monitoring and review should be proportionate to the purpose and risks involved.

Failure to comply with this guidance or applicable University policies may result in suspension of access to AI tools, disciplinary measures consistent with applicable University regulations, or other appropriate administrative action.

17. REVIEW AND UPDATES

This guidance will be reviewed at least annually and updated as necessary to address evolving technology, regulatory requirements, institutional priorities and regulations, and emerging best practices. Material revisions will be communicated to the University community, and the OAI will consult with appropriate academic and administrative stakeholders when revisions substantially affect institutional responsibilities or academic practices.