University of Utah AI Office | ai.utah.edu | July 18, 2025

Guidance on the Use of Artificial Intelligence in Research

Purpose

This guidance illustrates how University of Utah policies and associated rules and guidelines (collectively, "University Standards") apply to the use of generative AI enabled technology, Software Applications, generative AI tools, and agentic AI (collectively "AI Tools"), in research at the University. As discussed below, questions about acceptable use of AI Tools can, in many instances, can be resolved through application of existing University Standards.

Background

AI Tools are evolving rapidly and have the potential to advance research activities, increase innovation, and decrease the burden of simple administrative tasks for the faculty, students, and staff, who engage in or support research at the University. Use of AI Tools also raises important questions about how those AI Tools might repurpose or result in the disclosure of University data, along with questions about whether the output of the AI Tools is reliable, free from bias, and otherwise fit to be included in research results or analysis. Relatedly, because end users lack visibility into how AI Tools were created, questions may also arise regarding whether the output of AI Tools improperly relies on the work of others, whether the AI Tools generate output using the level of rigor expected from scholarly work, and whether reliance on the output of AI Tools meets applicable legal, professional, or regulatory requirements. Existing University Standards designed to protect University data and research projects also apply when users enter University data into AI Tools and when users rely on the output of AI Tools. In some instances, clarification regarding the application of those University Standards may be helpful to address specific issues related to use of AI Tools. As the academic, professional, and legal landscapes related to AI Tools change over time, specific revisions, or development of new University Standards, may be important to help users meet University expectations.

Scope

This guidance applies to Research Activities at the University that use devices or information subject to established University Standards. The guidance applies to any University employee, including faculty, students, staff, and in some cases to University affiliates, (collectively "University Personnel"), who participates in a Research Activity.

Guidance

Accountability. University Personnel must comply with University Standards when participating in a Research Activity, engaging in University business functions, or using University IT Resources and Information Assets. Use of any AI Tools on University IT Resources or with University Information Assets or Institutional Data, is subject to University Policy. University employees may only use approved Software that was properly Procured under University Policy and subject to requirements based on the

classification of the data and conditions of use placed upon it by the Data Steward and University Standards.

Procurement. University Personnel must use established University Procurement processes when purchasing AI Tools, including when purchasing through UShop, Archer, Accounts Payable or University Purchasing, and also including sole source purchases and renewals. University Personnel should not sign documents on the University's behalf. Procurement Contracts associated with AI Tools may pose significant legal risk to the University if the underlying Services will access, manipulate, create or store University data or interface with University IT Resources. Accordingly, software with AI Tools must undergo appropriate evaluation prior to use. Depending on the nature of scope of the intended use of the Software, such evaluation may include University review of a completed Educause Higher Education Community Vendor Assessment Toolkit (HECVAT) review of additional internal risk documents, and review for relevant legal, contract, IT and security, and information privacy considerations. A failing score during the evaluation will result in the software not being approved for acquisition and unapproved software will not be used on University IT Resources.

Security. Use of AI Tools with University IT Resources, Information Systems, or Assets, shall be limited to appropriate and legal use only as authorized by the University and in the manner and to the extent authorized. This means University Personnel can only install or distribute AI Tools that are appropriately licensed and meet University security requirements. University Personnel may not violate the rights of any person, organization, or company protected by trade secret, patent, Intellectual Property rights, or similar laws or regulations. University Personnel are responsible for complying with related terms of use in product contracts and licenses and applicable federal and state laws.

Data Privacy. University Personnel should understand the type of data being used with AI Tools and take reasonable precautions to maintain privacy of data subjects. All use is subject to University Standards, including protecting Institutional Data and IT Assets and following conditions of use and Best Practices issued by the Data Steward. Users shall not use Restricted Data or Sensitive Data in any way that would cause unauthorized disclosure under University policy or applicable state and federal law.

Honesty. University Personnel should declare that they are using AI Tools and adequately describe the purpose and extent of use in compliance with University Standards, and applicable state and federal law. If notices and consent to data subjects are required, University Personnel shall provide notice and obtain consent before any University data are accessed, used, viewed, or manipulated by AI Tools.

Governance. Using AI Tools in Research Activities may be subject to multiple governance processes at the University, including the Institutional Review Board ("IRB"), Data Governance Committee, or Clinical Data in AI Subgroup. University Personnel should be transparent throughout the IRB application, purchasing, or procurement process, alerting University stakeholders, and starting the governance process. University IT maintains an inventory of approved AI Tools, and University Personnel are encouraged to communicate with University IT to assess existing Software before working with third parties to purchase new AI Tools.

Monitoring. Use of AI Tools is subject to Signature-based Detection and Automated Monitoring activities to ensure compliance with local, state, federal, and University regulations and contractual obligations. Maintaining records of how AI Tools were used may be included in the Research Record to evaluate compliance with University Standards and this guidance.

Education. The Office of Research Education (REd) (in the Office of Research Integrity & Compliance) in collaboration with University Policy owners should develop and maintain annual training summarizing Acceptable Use of AI Tools in Research Activities consistent with University Standards and this guidance. University Personnel who are experts on AI Tools should develop classes for the University Campus. These classes can be shared across Utah Higher Education Institutions, as needed.

Compliance and Enforcement. This Guidance applies University Standards to the use and procurement of AI Tools for Research Activities. Violations of University Standards – including the improper use of AI Tools – may result in sanctions and other enforcement actions.

Policy Application Statements

Policy 4-001: Institutional Data Management Policy

Use of Institutional Data or Information in AI systems is subject to the conditions of use and Best Practices established by the Data Steward over the Institutional Data or Information. The Data Steward should create conditions of use that permit access to Institutional Data without further review. Absent approval outlined in the relevant conditions of use, a Data User must submit a request to the Data Steward for approval or denial before Institutional Data or Information is used in a way not specifically contemplated by the conditions of use. Data Stewards are responsible for ensuring the Data User abides by the conditions of use, best practices, and in compliance with university policy, state and federal law.

Policy 4-004: University of Utah Information Security Policy

Use of AI with University IT Resources, Information Systems, or Assets, shall be limited to appropriate and legal use, including legitimate patient care, instructional, research, administrative, public service, and approved contract purposes, only as authorized by the University and in the manner and to the extent authorized. This means Users shall only install or distribute AI software that is appropriately licensed for use by the University and Users may not violate the rights of any person, organization, or company protected by trade secret, patent, Intellectual Property rights, or similar laws or regulations. Users are responsible to comply with all federal, state, and other applicable laws; all applicable University regulations; and applicable contracts and licenses.

Rule 4-004A: Acceptable Use

A user may only use AI, Generative AI, Local AI, Agentic AI, or Agentic AI Workflows, that is approved by the university and for the approved use it was approved. All Illegal Behavior with AI is strictly prohibited. Users shall abide by the University's Ethical Standards and Codes of Conduct when using AI, including to protect the University's Restricted and Sensitive Data. Users may not perform actions with AI that are detrimental to Electronic Resources or that negatively affect other Users' ability to perform their assigned duties. Users may not waste University Electronic Resources or prevent others from using them.

Rule 4-004C: Data Classification and Encryption

Users must protect the University's Restricted and Sensitive data classification types when using AI, Generative AI, Local AI, Agentic AI, or Agentic AI Workflows. If Data is classified as Restricted Data or Sensitive Data, a User can only provide access to authorized individuals with approved access, a business need to know, and with the appropriate confidentiality agreement in place. In the case of third-party Software Applications and Information Systems, Users must verify with IT and Data Stewards that the Institutional Data is used only as permitted by the conditions of use. Most AI Software Applications are not appropriate for Restricted Data or Sensitive Data, and Users should confirm with the Data Steward, and as applicable, the Privacy Office, IT, ITS, and Office of General Counsel for approval before use.

Policy 4-050: University Software Policy

AI can be integrated into any type of Software, including: Systems Software, Programing Software, and Application Software, each as defined by Rule 4-050B. It is in the best interests of the University to appropriately manage the acquisition or development of University Software, its use, and its replacement. To this end, enterprise-level Data Stewards should establish Best Practices and Conditions of Use to decide when AI may be used in Software.

Rule 4-050A: University Enterprise Software

Before purchasing, leasing, developing, or other acquiring University Enterprise Software with AI, Generative AI, Local AI, Agentic AI, or an Agentic Workflow, that University administrative or academic unit is required to complete the current version of the University's technical Request for Proposal (RFP) document, which must then be evaluated by University of Utah Hospitals and Clinics Information Technology Services (ITS) for Hospitals and Clinics software or University Information Technology (UIT) for campus and health sciences software. Each acquisition of a University Enterprise Software application with AI, Generative AI, Local AI, Agentic AI, or an Agentic Workflow, however acquired, must be approved by the appropriate governance committee.

When any University Enterprise Software with AI, Generative AI, Local AI, Agentic AI, or an Agentic Workflow, is proposed to be purchased or leased from, or developed (written) by, an external party or vendor, there must be a three-year TCO form completed and approved by the appropriate Dean or Administrative Director, and the University of Utah Hospitals and Clinics CIO for University of Utah Hospitals and Clinics software or the University CIO for campus and health sciences software, before the purchase or lease is finalized.

When any University Enterprise Software is proposed to be developed (written) for the University by an internal University unit, there must be a three-year TCO form completed and approved by both the appropriate Dean or Administrative Director and the University of Utah Hospitals and Clinics CIO for University of Utah Hospitals and Clinics software or the University CIO for campus and health sciences software, before substantial development work begins.

Rule 4-050B: University Software

Before purchasing, leasing, developing, or otherwise acquiring University Software that includes AI, Generative AI, Local AI, Agentic AI, or an Agentic Workflow, that will access manipulate, create or store Restricted Data, as outlined in Rule 4-004C, the University unit is required to complete the Educause Higher Education Community Vendor Assessment Toolkit (HECVAT) and any mandatory questions document(s), which must then be evaluated by UIT for campus and health sciences software and University of Utah Hospitals and Clinics Information Technology Services (ITS), if the Software is for University Hospital or Clinics. This includes University software purchased through UShop, Archer, Accounts Payable or University Purchasing as well as sole source and renewals. A failing score during the evaluation will result in the software not being approved for acquisition.

It is also recommended that software that before purchasing, leasing, developing, or otherwise acquiring University Software that includes AI, Generative AI, Local AI, Agentic AI, or an Agentic Workflow, that will access manipulate, create or store Sensitive Data, as outlined in Rule 4-004C, follow this same review.

Policy 3-100: University Procurement

Organizational Units shall procure Supplies and Services, including those with AI, Generative AI, Local AI, Agentic AI, or Agentic Workflow, through the University's designated Procurement system, Purchasing Cards, or other processes approved by the Purchasing Department. Procurement Contracts associated with AI, Generative AI, Agentic AI, or an Agentic Workflow may pose significant legal implications to the University if, for example, the underlying Services, University Software, or Enterprise Software, will access manipulate, create or store Restricted Data or Sensitive Data, as outlined in Rule 4-004C. If so determined, these Procurement Contacts require review by the Office of General Counsel prior to contract execution (see also Policy 3-004).

Rule 3-100E: Restricted Purchases and Special Procurement

All new Software purchases, including Software with AI, Generative AI, Local AI, Agentic AI, or Agentic Workflow, regardless of Procurement method or dollar value, are subject to the requirements as detailed in Rule R4-050A. UIT approval is not required for existing software maintenance or existing software subscription renewals. All purchases of IT-related hardware and data encryption requirements, regardless of Procurement method or dollar value, are subject to the requirements and limits as detailed within University Rule 4-004C.

Policy 7-001: Policy for Research Misconduct

Relying on output from AI as part of a Research Record may constitute Research Misconduct if the output introduces errors—whether through AI hallucinations or simple inaccuracies generated by the AI Tools. It is the responsibility of Research Personnel to verify the accuracy and integrity of all information included in a Research Record and failure to do so—including when relying on AI Tools—could result in an investigation for, and finding of, research misconduct.

Policy 7-020: Determining Authorship in Scholarship or Scientific Publications

AI does not meet the accountability requirements to be identified as an author in scholarship or scientific publications. The human author must take accountability and responsibility for Generative AI output, including verifying the content and ensuring the material is appropriate and accurate. More information is available here: https://integrity.research.utah.edu/ai-research-statement.php.

Glossary

“Agentic AI” means AI systems that can autonomously or semi-autonomously make complex decisions and take actions towards specific goals with limited human oversight.

“Agentic Workflow” means multiple Agentic AI, whether from one single source or multiple sources, operating in collaboration to make complex decisions and take actions towards specific goals with limited human oversight. Agentic Workflows typically require read and write access to data held in a variety of locations to accomplish goals.

“Artificial Intelligence” means an artificial program, developed and trained in a computer system, software, hardware, or other context, that is designed or trained to think or act like a human, without human oversight.

“Asset” is defined in Policy 4-004 and means any University-owned Information Asset or IT Resource that is a part of University business processes.

“Best Practices” means accepted management and access procedures that Data Custodians, Data Administrators and Data Users, as defined by Policy 4-001, follow to ensure security, accessibility, and integrity of Institutional Data. Data Stewards are responsible for specifying Best Practices and identifying adequate resources that enable Data Custodians and Data Administrators to implement Best Practices. Best Practices change as technology, procedural improvements, and the nature of the data change.

“Data Steward” is defined in Policy 4-001 and means a University official who has planning and policy-level responsibilities for access and management of Institutional Data in his or her functional areas. A Data Steward is appointed by the Vice President who is responsible for the Data Steward's functional area.

“Electronic Communication” is defined in Policy 4-004 and means for exchanging digital messages. This includes, but is not limited to, email, Teams, Zoom, etc.

“Electronic Resource” is defined in Policy 4-004 and means any technology used for Electronic Communication. This includes, but is not limited to, internet, email, and social media.

“Generative AI” means a type of artificial intelligence that can generate new content based on the interpretation of an input against the information it was trained on.

“Local Artificial Intelligence” means Artificial Intelligence, Generative Artificial Intelligence, Agentic AI, or any Agentic Workflow” that is developed by a University operating unit, for use by that operating unit. “Developed” includes writing, and training or tuning Artificial Intelligence systems, whether purchased, open source, or leased.

“Information” is defined in Policy 4-001 and means Institutional Data that is grouped and/or organized for use in a context required by Data Users. For example, student Institutional Data may be grouped and organized to provide information in the form of enrollment reports or other contextual information required by Data Users.

“Information Asset” is defined in Policy 4-004 and means data or knowledge stored in any electronic manner and recognized as having value for the purpose of enabling the University to perform its business functions.

“Information System” is defined in Policy 4-004 and means an IT Resource used to electronically create, store, process, or transmit any University data or Information Asset.

“Institutional Data” is defined in Policy 4-001 and means Data that are acquired or maintained by University functional areas in the performance of official administrative job duties. Specifically excluded from the definition of Institutional Data are: personal medical, psychiatric, or psychological data for both employees and patients seen at University Hospitals or Clinics; notes and records that are the personal property of individuals in the University community; research notes, data, and materials; and instructional notes and materials; and otherwise restricted by institutional policy or State or Federal guidelines.

“IT Resource” is defined in Policy 4-004 and means a Server, Workstation, Mobile Device, medical device, networking device, web camera, monitoring device, or other device/resource that matches one or more of the following criteria:

a. owned by the University;
b. used to conduct University business regardless of ownership;
c. connected to the University’s network; or
d. creates, accesses, stores, or transmits Information Assets.

“Mobile Device” is defined in Policy 4-004 and means a portable, handheld electronic computing device that performs similar functions as a Workstation (e.g., iPhone, Android phone, Windows phone, Blackberry, Android tablet, iPad).

"Procurement" is defined in Policy 3-100 and means buying, purchasing, renting, leasing, or otherwise acquiring any Supplies, Services, or Construction. Procurement includes all functions that pertain to the obtaining of any supply, Service, or Construction, including description of requirements, selection, and solicitation of sources, preparation and award of a contract, and all phases of contract administration using University funds.

“Purchaser” is defined in Policy 3-100 and means anyone that has Procurement authority, whether direct or delegated. Other University employees may participate in the Procurement process.

“Purchasing Card (PCard)” is defined in Policy 3-100 and means an institutional credit card administered by the Purchasing Department, billed directly to, and paid by the University of Utah, designated for the direct Procurement of non-travel small purchases made by a University employee.

“Research” means Research as defined by 45 CFR 46.102(l), which is “a systematic investigation, including development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.” Research includes obtaining information, biospecimens, or other data through interventions or interactions with human subjects or live animals.

“Research Activity” means an activity related to Research as defined by 45 CFR 46.102(l)

“Research Record” means any biodata, data, document, computer file, computer diskette, flash drive, or any other written or non-written account or object that reasonably may be expected to provide Evidence or information regarding the proposed, conducted, or reported Research that constitutes the subject of an Allegation of Misconduct. “Research Record” includes, but is not limited to: a grant or contract application, whether funded or unfunded; grant or contract progress and other reports; laboratory notebooks; notes; correspondence; videos; photographs; X-ray film; slides; biological materials; computer programs, files and printouts; manuscripts and publications; equipment use logs; laboratory procurement records; animal facility records; human and animal subject protocols; consent forms; medical charts; patient research files; and any documents and materials provided to the U.S. Department of Health and Human Services or an institutional official by a Respondent in the course of the Research Misconduct proceeding.

“Server” is defined in Policy 4-004 and means the hardware and software used to provide information and/or services to multiple Users.

“University Software” is defined in Policy 4-050 and means any software that is purchased, leased, or developed, or otherwise acquired by a University of Utah administrative or academic unit, for use by that University unit. It does not include software that is developed or acquired by an individual member of the University community (including any student, employee, or volunteer) without use of University funds or resources, for such individual person’s private use.

“University Enterprise Software” is defined in Rule 4-050A and means University Software that will have broad institutional impact, affecting the operations of more than one University unit, and/or will require integration with PeopleSoft or other enterprise software applications currently in use at the University.

“User” is defined in Policy 4-004 and means any person, including students, staff, faculty, permanent and temporary employees, contractors, vendors, research collaborators, and third-party agents, who accesses any University Electronic Resources, Information Systems, and/or IT Resources.

“Workstation” is defined in Policy 4-004 and means an electronic computing device, terminal, or any other device (e.g., desktop computer, laptop, Windows tablet) that performs as a general- purpose computer equipped with a microprocessor and that is designed to run commercial software (such as a word processing Application or internet browser).