

Introduction

As the use of artificial intelligence (AI) tools, such as chatbots, virtual assistants, and other emerging technologies (as defined in the Institutional AI Policy), becomes more prevalent, the University of New England (UNE) acknowledges the need for responsible and ethical use. In addition, UNE recognizes that AI tools come with serious security, accuracy, and legal risks. This policy outlines acceptable practices for AI tool use, emphasizing the protection of institutional, personal, proprietary, and sensitive information. Given the rapid evolution of AI, this policy will be reviewed annually and updated as needed. This policy should be read in conjunction with UNE's Institutional AI Policy, the AI Policy Guidance for Faculty, the AI Policy Guidance for Students, and the Guidance for the Use of Artificial Intelligence (AI) in Research.

All UNE community members must use AI tools responsibly and ethically, upholding University values and safeguarding sensitive information, and must comply with this policy in all instances unless an explicit exception is granted by the AI Governance Committee. The AI Governance Committee is responsible for reviewing and approving enterprise private AI tools for institutional use. Working with Information Technology Services, the Office of the General Counsel, the Office of the Registrar, the Office of Research and Innovation, Human Resources, the Center for Excellence in Teaching and Learning (CETL), and relevant academic units, the Committee also establishes and updates AI-related standards and guidelines, advises on high-risk or novel uses of AI, including agentic AI and AI used in high-stakes decision-making, and recommends updates to this policy as regulations, technologies, and institutional needs evolve.

General Usage of AI Tools

Enterprise Private AI Tools

Enterprise private AI tools are licensed by the University, contractually protected, and approved for institutional use, and community members access them with their UNE credentials. When an enterprise private AI tool is available for a task, community members should use it rather than a publicly available tool. The AI Governance Committee reviews and approves these tools and continues to refine the framework for evaluating and prioritizing new AI tool requests. Because the list of approved tools changes as that review continues, community members should confirm with Information Technology Services that a tool is approved before adopting it.

Publicly Available AI Tools

- Never upload high-risk data or any materials restricted by copyright, contract, or research agreements into publicly available AI tools.
- Only data classified as public or non-sensitive may be input into publicly available AI tools. Examples include information already published on UNE's public website, general research questions not involving confidential, proprietary, or regulated data, and non-identifiable, non-confidential educational content.
- Users should be aware that any information entered may become accessible to others or used without their knowledge or consent.
- It is the user's responsibility to confirm the classification of data prior to submitting it to any AI tool.
- Before using any such tool, users must carefully review its terms of service and data-handling policies. Do not use services that claim rights to your input or store sensitive materials without explicit UNE approval. Some publicly available AI tools offer an "opt-out" setting. Check whether this option is available, as it is critical for protecting confidential information. Information entered into these systems may otherwise become publicly accessible. To reduce this risk, enable the opt-out feature provided by many large language models (LLMs).

Prohibited Uses of AI Tools

The following uses of AI tools are strictly prohibited:

- Generating or manipulating content with AI tools in ways that compromise academic integrity, including plagiarism or misrepresentation of authorship.
- Using AI technologies for unauthorized personal data collection, surveillance, or monitoring of individuals without their consent. This does not apply to permitted activities such as students recording classroom lectures.
- Using AI to create, distribute, or promote content that is defamatory, lewd, illegal, violative of a person's legally protected privacy, or otherwise violative of any UNE policies, including policies against harassment and discrimination.
- Using AI tools for high-risk activities, such as employment decisions, admissions evaluations, or financial aid determinations, where the outcome would be determined solely by an automated system.

- Using generative AI tools to create malicious content, such as malware, viruses, worms, or trojan horses that could bypass access controls implemented by UNE or third parties to prevent unauthorized network access.

Academic integrity expectations and the use of AI detection tools are addressed in the AI Policy Guidance for Faculty and in the Code of Student Conduct.

For any high-impact decisions, including hiring, admissions, financial aid, promotion, or discipline, AI tools may be used only as a decision-support aid. Human decision-makers must retain full responsibility for the final decision and must be able to explain the basis for that decision without relying solely on AI output.

Consequences for Non-Compliance

Violations of this policy may result in disciplinary action. Individual legal liability may also arise if AI tools are used in ways that infringe copyright, compromise privacy, or violate applicable laws. Suspected misuse of AI tools should be reported to Information Technology Services, Human Resources, Student Conduct, or the Office of Research and Innovation as appropriate. Alleged violations will be addressed through existing disciplinary procedures and applicable handbooks and codes for students, faculty, and professional staff.

Additional Guidance

Procurement of AI Tools

AI tools that integrate with UNE systems or process institutional data may not be procured or implemented outside the established IT Services procurement, contract review, and security assessment processes. Individual faculty, professional staff, or departments must not independently sign terms of service or license agreements that bind UNE without appropriate review and approval.

If you or your department currently use an AI tool, you must ensure that it complies with UNE policies and effectively protects both organizational and personal information. For AI tools intended for sensitive functions, such as recruitment and admissions, academic evaluation, or financial decisions, consultation with the AI Governance Committee is required before adoption or use.

Ensure Accuracy of Outputs

You are ultimately responsible and accountable for your work product and any communications you send. You should understand that AI tools can often generate incomplete, inaccurate, or entirely fictitious content. This is sometimes referred to as “hallucination” and can occur even when AI tools sound confident or authoritative. You must take steps to ensure the accuracy and appropriateness of the work product and any communications that you produce with the assistance of an AI tool. All communications should be proofread and revised carefully. Generally, primary sources should be reviewed.

Disclosure and Citation

Disclosure and citation of AI use are generally not required for routine communications, such as emails or letters, unless authorship is significant. When appropriate, users should disclose and explain how AI was used to create a communication or work product. When in doubt, err on the side of disclosure.

Intellectual Property

Intellectual property (IP) laws were created with human creators in mind, and legal frameworks are still evolving to address how AI-generated content will be protected. Because the terms of use for many AI tools may grant the provider broad or irrevocable rights to use submitted data, users should exercise caution before entering such information into an AI tool. Many AI tools, particularly free ones, store or reuse user inputs to train their systems. Users should assume that any data submitted to AI tools may become publicly accessible or used without their consent.

To protect UNE and personal intellectual property, you must avoid inputting proprietary or sensitive information into AI tools unless explicitly approved by UNE. Only use tools whose terms you understand and that ensure appropriate data handling.

Do not input or reproduce materials that belong to others, including copyrighted, trademarked, or otherwise protected content, without authorization from the rights holder. Submitting third-party or UNE-owned materials without permission may violate intellectual property laws or institutional policy.

Confidential Information

AI tools often learn from user interactions, and many of them require you to consent to the storage and future use of your submissions, including the tools’ ability to share your input information with others. This is particularly true for publicly available AI tools.

To protect sensitive and confidential information, users must not input such data into any AI tools unless the tool is licensed by UNE or explicitly approved for use by the AI Governance Committee. Examples of confidential information include:

- Student records, as protected under FERPA
- Personnel records
- Data collected in a research project or University survey
- Information that UNE is obligated to keep confidential, such as in contracts, grant applications, or research disclosures
- Proprietary or non-public UNE information

Unless allowed by approved contracts and security controls, do not enter any student-identifying information into AI tools. This includes names, IDs, emails, education records, or descriptions of student work that could reveal identity.

Faculty and professional staff may require students to use publicly available AI tools until suitable University-approved enterprise private AI tools are available for academic use. When publicly available AI tools are required, faculty should clearly explain how data will be handled and should provide reasonable alternative arrangements if a student has a documented accommodation or another approved exception. Additional expectations and examples for instructional use are provided in the AI Policy Guidance for Faculty.

Patient, Research, or Client Data

Sharing patient, client, or research participant information with publicly available AI tools is prohibited under HIPAA, Maine privacy laws, professional ethical obligations, and UNE policy. These tools may use and share data without regard to disclosure restrictions or other protections. Therefore, individual patient data and patient data sets (even if de-identified) may not be exposed to open or public AI tools or services, absent specific, institutional approval.

Additional Resources

For Students

Because AI use rules can vary by course, review your syllabi and follow your instructors' instructions.

For Faculty

If you have questions about integrating AI tools into your teaching, contact the Center for Excellence in Teaching and Learning (CETL).

For Professional Staff

For guidance on using AI in administrative or operational workflows, contact Information Technology Services (ITS).

For Researchers

For guidance on using AI in research and grant activity, contact the Office of Research and Innovation (ORI).

Policy Review & Revision

This policy will be reviewed at least annually and updated as needed to reflect changes in regulations, technology, or University practices. Last updated August 20, 2026.