Colby

MEMORANDUM | GUIDANCE DOCUMENT

TO: Colby College Users of Generative Artificial Intelligence Tools
FROM: Richard Uchida, Vice President, General Counsel, and Secretary of the College
Elizabeth Teague, Assistant General Counsel
DATE: August 11, 2025

Using Generative AI at Colby College - A Legal Perspective

This memorandum is an exploration of the powerful capabilities of generative artificial intelligence tools and the transformative potential they hold for the work and life of our community. While these tools are a catalyst for innovation and creativity, it is important to understand the unique landscape of legal considerations that accompany their use. Our aim is to provide thoughtful guidance that goes beyond the classroom and the College's day-to-day academic environment, helping you navigate the exciting opportunities of generative AI, at Colby and beyond.[1]

Tip: The more you learn about AI, the better you will become in leveraging its potential. The AI@Colby site (https://sites.google.com/colby.edu/explore-ai/home) offers comprehensive guidelines and resources, developed through a collaboration among Academic Technology Services, the Davis Institute for Artificial Intelligence, the Library, the Center for Teaching and Learning, and the Writing Department. It supports the Colby community in exploring and using AI in human-centered and ethical ways.

Generative AI works by training from a massive amount of data, but it does not "know" facts. It predicts what to produce or generate based on information and patterns it has seen or been provided. This means the output it produces can be biased, outdated, or inaccurate. It may also contain information or material that was never intended to be, or shouldn't be, a part of the data in that AI platform. Understanding these considerations is a key step to using AI tools thoughtfully, safely, and responsibly. It is these same considerations that have led federal and state lawmakers, regulators, and private industry to pay greater attention to the use of AI, especially when it is used in important decisions about people's lives.

Here is an overview of key legal considerations to understand, along with practical tips on prudent use to protect yourself, your work, and the College. These are considerations only, and should not

[1] This document does not constitute legal advice. It is intended for general guidance, only. The Office of General Counsel is prepared to provide specific legal advice on generative artificial intelligence issues that you may encounter. This document will be updated from time to time based on new developments, including news and updates on the legal issues impacted by artificial intelligence technology.

discourage you from exploring and using artificial intelligence, much as you have employed other technologies to enhance and support your work.

Privacy and Data Security Considerations

One of the most important things to remember is that generative AI platforms store and train from the information users provide or that those platforms are instructed to review, monitor, and incorporate into their models (news, books, social media, popular culture posts and information, public records, and other data and materials from multiple sources.) Thus, significant legal considerations arise when sensitive, confidential, or proprietary data is loaded or posted into a public or unapproved AI tool that also stores and trains from that data. This might include student records, personally identifiable information about you or others, training data, employee files, health records, financial data, and other confidential or proprietary information. In addition, doing so can violate federal and state privacy laws such as the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA), as well as a variety of College policies.

- **Tips**: When using AI for College-related work, assume that anything you post, load or input into a public AI platform is permanently recorded and can be used to train future AI models. To avoid this, it is wise to use only the platforms approved by the College (like Google Gemini and NotebookLM (with your colby.edu login, *not* the public versions). The College has contracted with these vendors to restrict the availability of data provided to those platforms. Even then, do not post, input or load sensitive, confidential, personally identifiable, or proprietary data without checking with a College official (your manager or director, a dean or faculty member, a College officer, this office) first.

Employment and Discrimination Considerations

When AI is used in areas such as hiring, performance reviews, or admissions, it can unintentionally amplify biases found in its training data. This can create legal considerations under federal and state anti-discrimination and privacy laws. Using AI as a significant basis for decisions and judgments requiring human analysis, evaluation, assessment, and oversight is increasingly drawing scrutiny from federal and state lawmakers, as well as regulatory agencies. For example, if an AI tool is trained on historical hiring data that was developed at a time when bias against particular classes of people was pervasive, the tool may produce results that discriminate against those same classes of people years later.

- **Tip**: You should not rely on AI tools to make or substantially influence critical decisions about people's lives, such as hiring and promotions, employee evaluations, admissions, or compensation. AI can help you organize information, but the final decision should be made using one's own judgment, knowledge, and expertise, adhering to institutional policies.

Hallucinations and Unreliable Content Considerations

As noted above, generative AI models are trained using massive amounts of data from multiple sources. However, current versions are not able to discern the truth or accuracy of the data it gathers in any reliable way. Numerous instances have occurred where individuals have been criticized, and even sanctioned, for relying on or sharing inaccurate outputs generated by AI systems. As a result, relying on facts generated by AI is risky, especially when the material you have submitted relies heavily on the accuracy and completeness of that output.[2]

Moreover, data can be easily manipulated. The rise of deepfakes, AI-generated videos, photos, and audio that are nearly indistinguishable from reality, raises significant legal considerations. They can be used to manipulate or deceive by imitating an individual's voice or likeness without their consent. Emerging federal law and a patchwork of state laws can provide some recourse for a person whose identity was used without authorization. However, more important is the need to exercise vigilance in the review, evaluation, assessment, verification, and oversight of the material generated by AI, given the ability to manipulate data.

- **Tips**: Verification of the output from an AI platform is crucial. Likewise, disclosing where and how AI was used in work product you produce creates an additional safeguard to avoid hallucinations or reliance upon "false facts". Besides proper attribution of AI-generated materials, such disclosure can alert a cautious reader to verify the accuracy of those materials identified in the disclosure. Be aware of the power of AI to generate deceptive or fake videos, photos, or audios, or other false information, including unauthorized use of your own identity. See more guidance below.

Intellectual Property (IP) and Ownership Considerations

AI's impact on intellectual property (IP) law presents several key challenges, from copyright and patent protections to infringement risks. A top concern for creators who seek legal protection for work they have created using AI, is the uncertain legal status of AI-generated content. The U.S. Copyright Office has clarified that to be eligible for copyright protection, a work must contain "sufficient human creativity." This means if you use AI to create work and are seeking such protection, you need to add your own creative input to the work to be eligible for registration. However, there are no definitive thresholds on what constitutes sufficient human creativity to transform the work into a piece eligible for protection. Similarly, U.S. patent law requires a human inventor. The U.S. Patent and Trademark Office (USPTO) has issued guidance confirming that inventions created solely by AI cannot be patented; rather, patents may be granted

A note on "Fair Use" and AI: "Fair use" is a legal defense in copyright law that allows for the limited use of copyrighted material without permission. Courts have recently ruled that using legally acquired copyrighted materials to train AI models can be considered fair use. However, the legal landscape is still evolving. Training AI on pirated content is generally not fair use.

[2] Moreover, there does not appear to be a First Amendment/free expression defense to protect AI-generated content that is defamatory or harmful.

on some inventions that human inventors make with AI assistance.

IP infringement is also a top consideration implicated by AI. Generative AI tools are trained on content from the internet, which often includes protected material. When you use AI to create a document or image, the output might unknowingly incorporate IP elements (photos and video, written pieces, audio, etc.) which may have been included in the data the tool trained from. This can lead to liability claims about whether your use of such material infringes upon another's intellectual property rights.

Additionally, as noted in the previous section on data privacy, loading or posting your work product or that belonging to others, such as research, data sets, drafts of articles, etc., that you intended to protect or may be protected intellectual property of the person who created such material, may result in not only a waiver of any rights to protect that material, but also expose all of that work product for use by others.

- **Tips**: When using AI, you are ultimately responsible for ensuring your output does not infringe on existing copyrights or other intellectual property protections. You are also responsible to ensure that the information, data, or material you load or post on an AI platform is not intellectual property of another that you are providing without their consent. If you are seeking to protect your invention or content from use by others through a patent filing or copyright registration, be aware of the importance of human involvement to qualify such work for protection.

Antitrust and Anti-Competitive Considerations

Using AI tools to analyze and evaluate sensitive institutional strategy, like financial planning models, compensation or salary structures, employment or admissions assessments/information or criteria, can create a potential for inadvertently facilitating or inviting collusion or anti-competitive practices, especially if it appears that such data is shared among those in the same industry sector. Anti-competitive behavior can lead to intense regulatory scrutiny and has become the increased focus of federal and state (and even private) anti-trust investigations and prosecutions.

- **Tip**: Be cautious when using AI to handle sensitive data about institutional strategy. Such inputs can enable organizations to subtly collude on pricing, market allocation, or other competitive behaviors, leading to reduced competition and ultimately impacting consumers through higher costs or diminished choices. If such information must be loaded, utilize one of the platforms identified in the "Privacy and Data Security" section to restrict the broader dissemination of that information.

Cybercrime Considerations

Cybercriminals are increasingly exploiting generative AI to enhance their illicit activities. From crafting convincing phishing emails, texts, and other communications to developing sophisticated malware, generative AI has been a boon to cyber-criminals because of the massive

amounts of information and data that users post, both intentionally and unintentionally, on these platforms. Every year, numbers of Colby students, faculty, and staff fall victim to cybercrime - sometimes without any recourse for the loss, injury, or harm they suffer.

- **Tip**: Be on the lookout for unusually well-written or personalized phishing attempts. These might be crafted by AI to appear legitimate. Be especially careful when clicking links or downloading attachments. Watch for notices and warnings from the College's ITS department about phishing attempts and other instances of cybercrime or cyber-mischief. Report suspicious communications and questionable AI output to ITS.

What Should I Do? Guidelines for AI Use

Here are some guidelines that might help avoid the risks identified above when considering the use of AI:

- **Credit and Verify Original Sources:** When using AI, it's crucial to understand that AI tools are prone to "hallucinate" information, including sources. You must never simply trust a source that AI provides without verifying the source itself. Instead, track down the original publication or dataset yourself. Once you have confirmed the source and the accuracy of the information, you can then cite the original source directly, not the AI tool. This practice protects intellectual property, ensures accuracy, and demonstrates your commitment to professional integrity.

- **Disclose AI Involvement**: When you use AI in your work, think about your audience and their expectations. If you are creating something for an academic setting, research, or a public report, the recipient(s) may expect you to disclose how and where you used AI. Adding a disclaimer or disclosure explains your process and helps maintain integrity and transparency. In your disclosure, consider explaining not only where and how you used AI but also how you verified its output. For example, you could write, "I used an AI tool to help summarize background information for this report. I then verified all facts and sources against reputable sources, which I can produce upon request." This builds trust with the recipient of your work and shows that you maintained human oversight.

- **Require Disclosure of AI Involvement.** Likewise, when working with a third party, such as a vendor, contractor, or other "outsiders", require them to disclose whether they will use AI in the delivery of their work, and if so, how and where. Also, if that third party, in turn, will rely on a separate party who will use AI to assist them in the work they will deliver, require that the disclosure cover the third party and the party assisting them. Request a written agreement that the third party (and others working with third party) will adhere to the College's protections on data privacy and confidentiality.

- **Be Careful About What You Load or Post to an AI Model.** Because of the ways AI models train and then provide output, there are a host of reasons, described above, why you should be very careful about what information and material you elect to provide those models.

- **Avoid AI for Critical Decisions**: Do not use AI to make decisions which require human judgment, such as admissions, hiring, grading, or employee evaluation.

- **Uphold Institutional Values**: All College policies regarding employee conduct and academic integrity apply to AI-related work. Never use AI to engage in discriminatory, unethical, or illegal activity. If in doubt about your use, please ask.

Institutional Guidance

- **Information Technology Services (ITS)**: Guidance on secure platforms and data storage, as well as questions about the appropriate use of artificial intelligence. [Colby College ITS]

- **Davis Institute for AI**: Pedagogical and research-related questions, including classroom use, curriculum design, and academic exploration of AI [DavisAI]

- **Human Resources (HR)**: Policies for AI use in recruitment, evaluation, and employee data. [Colby College HR]

- **Office of the Provost:** Oversight of academic policy and institutional priorities related to AI integration in teaching, learning, and scholarly work. [Colby College Provost's Office]

- **Center for Teaching and Learning:** Support for faculty in incorporating AI tools into pedagogy while maintaining educational integrity and equity. [Colby College CTL]

- **Dean of Studies Office**: For AI use in academics, especially in advising, academic accommodations, and student support services. [Dean of Studies Office]

- **Office of the General Counsel**: Questions on data privacy, legal considerations involving confidential or protected information, intellectual property, vendor contracts, the implications of laws, including civil rights and other laws that impact AI use. [Colby College Office of the General Counsel]

Additional Resources

- Colby Data Privacy Guidelines

- Colby College Policy on Acceptable Use of Digital Resources

- Davis Institute for AI programming and workshops

- MuleChat

- White House Blueprint for an AI Bill of Rights

- "America's AI Action Plan"

Key Takeaway: Generative AI is a powerful tool with significant potential to enhance our work. The Office of General Counsel is committed to supporting the community in its navigation of the legal issues implicated by the use of artificial intelligence. Please reach out (207-859-4609 or legal@colby.edu) with questions or to have this office evaluate specific situations.