

Technology Department’s Guidance on the Use of Generative AI Tools

Version 1.6	Last Updated: 3-30-2026
Security Level: Public	Issued: 5/1/2024

Overview

Generative AI tools, including systems like ChatGPT, Google’s Gemini, and other AI-driven technologies, are rapidly transforming the landscape of digital interaction and content creation. The Technology Department acknowledges the potential for these tools to enhance educational practices, research, and administrative efficiency. This guidance document outlines our stance on the ethical and secure use of generative AI technologies within our community.

Examples of Acceptable Uses of Generative AI Tools

- Administrative Support: Generative AI may streamline administrative processes, including drafting communications or data analysis, **provided no sensitive university data is involved**. For questions about sensitive data, see the University [Written Information Security Program](#) or contact the information security team.

Unacceptable Uses of Generative AI Tools

- Handling Sensitive Information: Institutional data, particularly **personally identifiable information (PII) or other sensitive university data, must not be entered into public versions of generative AI tools or any non-sanctioned university software in alignment with the [University's Acceptable Use Policy](#)**. This prohibition includes, but is not limited to, student records, financial details, and confidential research data. For further guidance, please consult the [Written Information Security Program](#) or the [Data Classification Policy](#), which outlines how the university classifies confidential, sensitive, and public information.
- Intellectual Property Infringements: Inputting copyrighted material without permission, generating content that infringes on copyrights, or any other actions that violate intellectual property rights are illegal and violate [copyright law](#). See also Congressional Research Services’ [Generative Artificial Intelligence and Copyright Law](#) (September 2023).

Precautions and Data Protection

When utilizing generative AI tools, special attention must be paid to the security and confidentiality of the data being used. To protect sensitive and regulated data, adhere to the following best practices:

- **Data Security:** When utilizing generative AI tools, it is crucial to ensure that the data shared does not contain any information categorized as sensitive or regulated by the university. Please refer to our [Written Information Security Program](#) for details on sensitive data categories and definitions.
- **Anonymize Data:** Before using personal or sensitive data with AI tools, ensure that all identifiable information has been removed or obscured. This reduces the risk of data breaches and protects individual privacy.
- **Data Minimization:** Only use the minimum amount of data necessary for your task. Even in anonymized form, excessive data sharing can increase the risk of re-identification or unintended use.
- **Transparency:** It is essential to maintain openness about using generative AI in research or publications by disclosing its involvement in the intellectual process. Additionally, when recording or transcribing meetings, it is crucial to inform attendees about the use of these services to ensure that all participants are aware and can consent to this practice.
- **Verification of Content:** Be vigilant about the accuracy of information produced by AI tools, as these can generate incorrect or misleading content. Always verify facts and attribute the source when necessary.
- **Secure Applications:** It is crucial to ensure that any software application, including AI tools, especially those developed by third-party providers, is thoroughly evaluated for security compliance and adherence to university software licensing agreements. Before integrating new technologies, consult with the university's IT security team to ensure compatibility with the existing security infrastructure and compliance with the university's [Written Information Security Program](#).

Ethical Considerations

- **Responsible Use:** All interactions with AI tools should align with the university's core values of integrity and respect as outlined in the University's [Academic Integrity Policy](#).
- **Consent and Privacy:** It is crucial to respect privacy and seek consent when using generated content that may impact other individuals or their work.
- **Promoting Equity and Inclusivity:** AI tools should be carefully scrutinized for biases and trained with diverse datasets to mitigate discrimination. Establishing corrective measures for addressing any biased outcomes and actively engaging with diverse community groups to ensure inclusivity in AI deployment and usage is advisable.

AI-Powered Meeting Note-Takers and Wiretapping Guidelines

While convenient, AI-powered note-taking applications pose significant security, privacy, and legal risks. As of April 2025, Google's Gemini—accessed exclusively with your University-issued

credentials through the University's Google Workspace—is the only approved AI note-taker. All other AI software must be properly vetted, approved, and acquired through the [Software Purchase Request process](#) in accordance with the [System Acquisition and Development Policy](#). This ensures that any new or third-party solutions align with University standards, mitigate security risks, and comply with state and federal laws.

Massachusetts Wiretapping Law & Consent

Under Massachusetts law, all parties must provide explicit consent before any meeting or conversation is recorded, including through AI-powered note-takers or transcription tools. To comply, participants should be notified in advance that a session may be recorded (for instance, in the meeting invitation or agenda), and meeting organizers should reaffirm consent verbally at the start of the meeting. Recording must cease immediately if any participant objects or withdraws consent. All meeting invitations and agendas should include a disclaimer: *“Please be advised that recording meetings, by any means, including the use of any AI applications, without prior permission is strictly prohibited.”*

1. Meeting organizers and participants should remember that no meeting or conversation may be recorded or transcribed without permission from all involved parties.
2. Before recording, participants should be reminded at the outset of the meeting that a recording or transcription will be made, and that such material may be deemed a public record subject to disclosure.
3. Anyone who does not wish to be recorded should be allowed to opt out or leave the session.

AI-Powered Meeting Note-Takers - Handling Sensitive Information

All recordings and transcripts may fall under the Massachusetts Public Records Law, which could lead to their release in response to public records requests or subpoenas unless a statutory exemption applies. To minimize risks, individuals should avoid including personally identifiable (PI), confidential (CI), or other sensitive information in any recording or transcript. Any such materials must also comply with record retention requirements. **Unauthorized possession of recordings containing sensitive or confidential data may constitute a reportable breach under the Commonwealth's privacy laws, so employees should exercise discretion when discussing policy development, legal advice, or matters that could pose cybersecurity or physical security risks.**

Implementation and Resources

- Implementation: It is crucial to consult with the Technology Department before acquiring any new AI software, as our [System Acquisition and Development policy](#) mandates. This ensures that new technology aligns with our IT strategy, interfaces correctly with existing systems, and adheres to security and compliance standards. The Technology Department also assists in avoiding redundancy and achieving cost-effectiveness through competitive pricing and volume discounts. Please initiate new software

acquisition requests by visiting our [technology purchases page](#) on the Technology Department website.

- Training and Awareness: The Fitchburg State University Center for Teaching and Learning has curated a collection of resources to aid faculty in understanding and integrating AI tools. These resources, which include guidelines on incorporating AI into syllabi, AI and academic integrity, and more, are available on the Fitchburg State University [Center for Teaching and Learning Generative AI Website](#).
- Generative AI Pedagogical Resources: Explore the "[Generative AI and Its Use in Universities](#)" library guide, a valuable resource created by the CTL-sponsored Generative AI Pedagogical Discussion Group. The guide offers insights and practical applications of generative AI tailored to our campus community.

Fitchburg State University is committed to harnessing innovative technologies that enhance our educational mission while upholding our high data security and ethical integrity standards. As we expand our knowledge of artificial intelligence, we acknowledge the potential for yet undiscovered applications. These guidelines are designed to guide our ongoing exploration of this transformative technology, ensuring that we do so responsibly and ethically. Our objective is to promote the informed and conscientious use of generative AI tools, safeguarding the privacy and intellectual contributions of our entire community.

Revision History

Date of Change	Revision	Responsible	Summary of Change
5/1/2024	1	Stefan Dodd, CIO	Creation of AI Guidance
5/16/2025	1.1-1.5	Stefan Dodd, CIO	General Updates
3/30/2026	1.6	Stefan Dodd, CIO	Updated for accessibility.