College of Business & Security Management (CBSM)

Guidelines on the Responsible and Ethical Use of Artificial Intelligence (AI)

The emergence of Artificial Intelligence (AI) and Machine Learning (ML) tools, including generative AI platforms, has created new opportunities for innovation, problem solving, and productivity. However, these tools also introduce significant concerns related to academic integrity, data privacy, critical thinking, and the development of core disciplinary competencies.

The AACSB 2020 Interpretive Guidance (Revision 2025) identifies responsible technology use as an essential component of business education. Specifically:

- "Schools should have policies to ensure the responsible use of technology, including the ethical use of artificial intelligence." (AACSB, p. 29)
- AACSB examples encourage the development of coursework and guidance that address machine learning, natural language processing, and the ethical use of AI in business settings. (AACSB, p. 7)

In alignment with these expectations, CBSM has established the following college-level guidance to ensure consistent, ethical, and secure student engagement with AI tools, in alignment with broader UAF guidance.

1. Purpose of These Guidelines

This guide is intended to set a minimum level of expectations for AI use within CBSM courses, complementing broader university policies (see Annex I) on academic integrity and data security. Individual instructors may go beyond this, but it aims to ensure that:

- Students are able to develop the analytical, research, communication, and discipline-specific skills needed for both academic and workforce success.
- When permitted, that AI is used ethically, transparently, and in ways consistent with both professional standards and academic goals.
- Instructors continue to retain the authority to tailor AI use expectations based on the learning objectives and needs of their courses.
- Students are able to understand the risks and responsibilities associated with AI use, including accuracy, privacy, ethical, and security-based concerns.

Based on this, it is recommended that individual instructors adopt one of the three approved models described below, and clearly identify which model is used within their syllabi.

2. Course-Level AI Categories

CBSM recognizes that what is considered appropriate use of AI may vary by course, based on individual or course-specific learning objectives and needs. To maintain consistency, instructors should classify their course AI policy under one of the following categories:

1. Prohibited

No use of AI tools is permitted in these courses. Courses designated as prohibited do not permit the use of AI for any components of course objectives.

2. Conditional

AI use is limited and is permitted only where explicitly defined or with instructor approval. Examples of this may include assignments where AI may only be used for brainstorming, debugging, or outlining, but not for full content creation. This list will be subject to individual instructors and their usage guidelines.

3. Broadly Permitted and/or Generally Encouraged

AI use is broadly allowed and may be used as a learning enhancer. All requirements on proper attribution and transparency (outlined later) still apply.

3. Student Responsibilities When Using AI

Regardless of whether AI is prohibited, conditional, or permitted, students are still responsible for the integrity and accuracy of all content submitted. This includes:

1. Source Verification

Students are required to ensure that all work, even when involving the use of AI, reflects legitimate, verifiable, and properly attributed sources, per all course requirements. The following uses are prohibited in all CBSM courses:

- Invalid or Fabricated Sources, including references to non-existent articles, authors, or data. This may be partial or whole (such as correct author lists but fake article names).
- Misattributed Claims, such as incorrectly attributing content or claims to a legitimate source, altering what the original source states, misquoting, etc.
- Plagiarism, such as directly copying from existing sources without proper attribution, including copying from AI outputs that reproduce copyrighted material, or include otherwise unattributed materials from other sources (including the AI itself). Failure to cite AI tools used in the generation of content may result in similar consequences.

2. Transparency and Attribution

When AI is permitted:

- Students must disclose how and to what extent AI was used.
- Students must follow proper citation practices for AI tools (based on the format required).
- Students may be required to submit an AI interaction log, including prompts and outputs, or other evidence of AI interactions, as required by the instructor.

Failure to properly attribute the inclusion and extent of use of such tools may constitute a violation of academic integrity.

3. Accountability

It is important to remember that AI-generated content is not exempt from academic integrity standards. As such, Students will remain responsible for:

- The factual accuracy of all work presented or submitted.
- The quality of any analysis involved in producing assigned products.
- Following ethical writing practices throughout their work.
- Compliance with all university and college-specific rules, as well as all applicable local, state, and national laws and regulations, as well as any contractual agreements that may exist relating to data utilized.

4. Cybersecurity and Data Privacy Requirements

Regardless of the course designation category (e.g., Prohibited, Conditional, or Permitted), students should adhere to the following data use standards:

1. No sensitive or personal data should be entered into AI tools. This includes:

- FERPA-protected student information.
- Personally Identifiable Information (PII).
- Proprietary data, whether internal to the university or through external sources.
- Confidential or internal university (or company) information.
- Secure assignment materials (e.g., exam questions, unpublished cases). These remain the intellectual property of Instructors and respective rightsholders.

2. Students should use institution-approved AI tools whenever possible. If outside or non-standard tools are used (when permitted):

- Students are responsible for reviewing privacy and/or legal policies, and ensuring they maintain proper protections for associated data.
- Students should be aware that any data entered into AI tools may be stored, reused, or made public by the provider, depending on those agreements, and may not follow safe data practices.

3. Students should avoid uploading course assignments into AI tools unless explicitly allowed. This reduces risks of:

- Unintentional plagiarism.
- The training of future AI models on course specific materials.
- Copyright exposure of instructor materials (which are the intellectual property of their respective owners).
- Data leakage (potential exposure of data to third parties).

4. For AI-Assisted Code and Software Development, students must ensure that:

- Code suggestions do not include insecure or malicious components.
- Copyrighted or licensed code is not improperly reused or unintentionally produced.
- All outputs are checked for compliance with course and project requirements.

5. Additional Notes

1. To ensure consistency and transparency, instructors are expected to:

- Select one of the three AI guidance categories (Prohibited, Conditional, Permitted) and include it in their syllabus. These may vary by individual courses, but should be clearly delineated.
- Clearly communicate expectations for attribution, any allowable tools, and permitted uses.
- Provide examples of permitted or restricted use (e.g., "AI may be used for proofreading but not drafting paragraphs"). This helps provide clarity to students and reviewers.
- Coordinate with Program Directors when implementing new or experimental AI guidelines, as necessary, and seek guidance from colleagues where appropriate.
- Report violations under academic integrity procedures as required.

2. Alignment with AACSB Standards. This guidance supports AACSB's expectations by:

- Establishing a college-wide standard for ethical AI use.
- Reinforcing the development of student competencies in critical thinking, analysis, and ethical reasoning.
- Encouraging responsible engagement with emerging technologies in line with industry expectations.
- Ensuring transparency, fairness, and accountability in the assessment process.

AACSB Standards:
2020 Interpretive Guidance for AACSB Business Accreditation (Revision 2025):
https://www.aacsb.edu/-/media/documents/accreditation/2020-interpretive-guidance-feb-28-2025.pdf

Annex I: AI and the UAF Student Code of Conduct:

https://www.uaf.edu/orca/student-conduct/academic-misconduct.php

Here is some information regarding AI as it relates to the student code of conduct.

Work that is created by an artificial intelligence engine is covered by the student code of conduct. The student code of conduct was written to address behavior, not technologies. In addition, work submitted for credit that was created by AI-engines can be addressed using the academic misconduct portion of the student code of conduct.

Depending on the provisions in the course syllabus and/or the program's standards, portions of the academic dishonesty regulation can apply to the use of unauthorized use AI under the following examples:

- utilizing devices not authorized by the faculty member;
- using sources (including but not limited to text, images, computer code, and audio/video files) not authorized by the faculty member;
- acting as a substitute or utilizing a substitute;
- deceiving faculty members or other representatives of the university to affect a grade or to gain admission to a program or course;
- violating the ethical guidelines or professional standards of a given program.

Student code of conduct violation determinations are made upon a finding of the evidence through the student conduct process. Student conduct administrators consider all evidence presented, however, because the reliability of AI detection tools is undetermined, findings of responsibility will not be solely based on AI detection software at this time. For reference OpenAI warns their detection software is " not fully reliable" and "it should not be used as a primary decision-making tool, but instead as a complement to other methods of determining the source of a piece of text." According to GPTZero, "Overall, our classifier is intended to be used to flag situations in which a conversation can be started (for example, between educators and students) to drive further inquiry and spread awareness of the risks of using AI in written work."

In order to determine a violation occurred additional evidence of unauthorized use of AI must be available. Examples of evidence include: other writing examples, unexplained advanced techniques, prior work completed by the alleged individual, admissions of use, etc.

---

*This policy was developed with the assistance of AI-based tools via outlining and structural organization. (OpenAI ChatGPT 5.2)