

 Wharton County Junior College	ADMINISTRATIVE PROCEDURE		
WCJC Title: Acceptable Use of Artificial Intelligence / Machine Learning Tools	Section C: Business and Support Services	Pages: 3	
Policy Title: Technology Resources: Artificial Intelligence		Policy: CRB (Local)	
Subtitle: Acceptable Use of Artificial Intelligence / Machine Learning Tools		Date Adopted: 03/31/2026	

Purpose

Wharton County Junior College (“WCJC” or “College”) Information Security has a responsibility to protect College computing resources, including College data. There is a unique potential for negligent disclosure of College data when interacting with large language models (AI, GenAI) and machine learning (ML) solutions that are not approved by or provided by WCJC Information Security. Some AI/ML models capture data submitted to their system and use that data for future training. In some circumstances, the raw data can be recovered by another user of the system after the AI/ML system is trained with that data. When providing data to an AI/ML model or system, it opens the risk that the data shared is exposed to parties that are not authorized to access that data.

This Administrative Procedure describes and limits the types of AI/ML models and software that can be used with various classifications of College data. This procedure also provides user responsibilities for the use of AI/ML. AI/ML includes 1) the deep learning models that produce content, for example, text, images, or video from patterns in data that are provided to the model; and 2) any systems that use AI/ML models (e.g., ChatGPT, Claude, Grammarly, Notion AI, Microsoft Copilot). Users are responsible for guarding against the inappropriate disclosure of protected College data when using AI/ML.

Definitions

GenAI Tool: Software interfaces, such as Microsoft Copilot and OpenAI ChatGPT, mine information sources for various creative, problem-solving, and decision-making purposes. GenAI Tools may be standalone or integrated with other applications and services (for example, Copilot for Microsoft 365 can be accessed from the Windows desktop or through Microsoft Office 365 applications). This integration is not limited to Microsoft products. Public GenAI Tools are those readily available on the general market to anyone, whether free of charge or through a paid subscription. It is important to note that AI technology is rapidly evolving, and new products and applications are emerging quickly.

College AI/ML Tools: Tools specifically approved for use with College data. These tools approved for handling College private or restricted data interact with private College large language models (LLMs) that do not share this data with other entities or the public.

Users: Students, faculty, staff, contractors, guests, and any members of the general public granted permission to access and use College computing resources.

Machine Learning: A type of artificial intelligence that enables systems to learn from data and improve their performance or predictions without being explicitly programmed.

AI Agent: A software system that uses artificial intelligence to perform tasks, make decisions, or provide recommendations on behalf of a user or organization.

Procedure

This standard applies to Wharton County Junior College faculty, staff, and students providing data to AI/ML models and systems in connection with learning, research, business, and other activities.

Use of AI/ML Tools

Private and Restricted College data may only be used in conjunction with College AI/ML Tools designated as approved for use with these classifications. Public data may be used with any AI/ML model or system. Users must verify the approval status and data classifications permitted for any AI/ML Tool before use. Users must request an evaluation of AI/ML tools that have not yet been approved by contacting WCJC Information Security and initiating the Vendor Security Risk Assessment process.

Users must also be aware of their responsibilities as outlined in the College's Acceptable Use Policy, which provides governance on prohibited activities and security of College computing resources.

AI/ML Use Responsibilities

When using any AI/ML Tools, including approved College tools, users are responsible for:

- Being accountable for the use of their own output from AI/ML and verifying the accuracy of all output obtained from AI/ML.
- Using AI/ML Tools only for legitimate purposes. Uses such as creating media impersonating or representing others without their permission or falsifying presentations of research data and/or research results are not legitimate uses.
- Refraining from malicious activities including disinformation, deception, or harassment of others.

Public AI/ML Use Responsibilities

When using Public GenAI Tools, users are also responsible for:

- Safeguarding the privacy of all individuals who have provided the College with personal information (including, but not limited to, students, faculty, staff, community members, and research subjects) as well as respecting the intellectual property rights of others.
- Following all applicable laws, regulations, and College policies and Administrative Procedures.

Exercise due diligence in identifying the intellectual property rights of others (including when creating derivative works) and follow the rules of fair use before using AI/ML tools in any manner that could violate others' rights.

Noncompliance

Users must comply with this Administrative Procedure, College policies, and all applicable laws and regulations. Noncompliance could lead to corrective action and possible suspension or loss of access privileges in accordance with College Policy, the Staff Handbook, the Faculty Handbook, or the Student Code of Conduct. Concerns regarding noncompliance may be reported to the WCJC Information Security team and will be referred to the appropriate College authorities for review.

Date Prepared/Revised: 02/01/2026 (KV)