POLICY

Title: RESPONSIBLE USE OF ARTIFICIAL INTELLIGENCE (AI)	Code: E0202-2
Authority: Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99; Titles VI and IX of the Civil Rights Act, the Americans with Disabilities Act of 1990, 42 U.S.C. § 12101 et seq. (1990), and the Higher Education Act of 1965, 20 U.S.C. § 1001 et seq. See Also: MATC Policy C0700, District Employee Code of Ethics; Board Minutes, 08/27/24	Original Adoption: 08/27/24 Revised/Reviewed: Effective: 09/01/24

POLICY STATEMENT

MATC is committed to providing a safe and secure computing environment for employees, students, and affiliates. This policy establishes guidelines for the responsible, ethical, and confidential use of AI Technology within the college community when performing work and using MATC systems and data. Establishment of this policy seeks to ensure safeguards for institutional data in compliance with FERPA, HIPAA and other applicable federal and state laws.

Artificial Intelligence (AI) refers to the development of computer systems that can perform tasks that typically require human intelligence. These tasks include learning, reasoning,

problem-solving, perception, language understanding, and decision-making. These tools can write and revise text on command, offering new ways for students to learn but also raising questions about academic integrity. The best-known example of a generative AI chatbot is ChatGPT, built by OpenAI and accessible through Bing AI, but other tools, such as Google Bard, exist and are rapidly improving.

AI can be categorized into two main types: narrow or weak AI, which is designed to perform a specific task, and general or strong AI, which aims to possess the ability to understand, learn, and apply knowledge across various domains.

SCOPE

This policy applies to all users of MATC systems and data including employees, students, contractors, and affiliates, whether on campus or from remote locations. MATC systems and data must be used appropriately and in accordance with local, state and federal laws. Users will be held accountable for inappropriate or unlawful acts as outlined in this policy.

POLICY

PERMISSIBLE USE OF MATC DATA WHEN USING AI TOOLS

Entering data into most AI applications or web platforms (i.e. Google search, Grammarly, etc.) is similar to posting that data on a public website. By design, these AI tools collect and store data from users as part of their learning process. Any data you enter into such a tool could become part of its training data, which it may then share with other users outside the college and may:

- subject the college to the likelihood of increased hacking or data breach.
- lead to privacy issues and possible exposure for MATC under federal and state privacy laws.
- result in loss of confidentiality.
- constitute copyright infringement.
- harm MATC’s reputation and put the college at legal risk.

For these reasons, all college employees (including contract employees), students, and affiliates may enter institutional data into AI tools or services only when:

- The information is classified as public (low risk) and does not include any internal, sensitive, or restricted data; or
- The AI tool or service being used has undergone appropriate internal review by IT based on the AI Activity type:

Data Classifications and AI Use

In accordance with MATC Administrative Procedure H101-1, college data is classified as follows:

Data Classification	Definition
Restricted Users must not enter this type of data into AI tools.	Information protected by federal or state statutes or regulations (such as FERPA, HIPAA), college regulations or contractual language. Restricted Data may be disclosed to individuals on a need-to-know basis only. By way of illustration only, some examples of Restricted Data include: 1. Credit Card Information 2. Protected Health Information 3. Social Security numbers 4. Student and prospective student information 5. HR employee data and information including hiring, promotion, discipline, or termination of employees. 6. Legal documents including contracts, compliance reports, or other legal or regulatory activities with potential legal implications.
Sensitive Data Users must not enter this type of data into AI tools.	Information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a criminal or civil statute requiring this protection. Sensitive Data is information that is restricted to members of the college community who have a legitimate purpose for accessing such data. By way of illustration only, some examples of Sensitive Data include: 1. Internal memoranda and electronic mail, and non-public reports, budgets, plans, and financial information. 2. Information covered by non-disclosure agreements 3. Donor contact information and non-public gift amounts.
Public Data Users may enter this type of data into AI tools.	Information that is open to the general public and is not named in one of the two categories above.

POLICY

Title: RESPONSIBLE USE OF ARTIFICIAL INTELLIGENCE (AI)	Code: E0202-2

USER RESPONSIBILITY
Users will be held accountable for appropriate and ethical use of AI tools and are responsible for ensuring:

1. *Data Privacy and Security.*
   Data entered into AI tools complies with all privacy, cybersecurity, education laws such as the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99, and institutional policies.
2. *Confidentiality.*
   Data entered into AI tools is capable of being reverse engineered, so use of AI must not result in the college breaching a duty of confidentiality.
3. *Bias and Discrimination.*
   The output from using AI tools does not result in bias and/or discrimination against any student, employee, and/or other individual.
4. *Plagiarism.*
   The output does not result in plagiarism.
5. *Copyright Infringement.*
   The output does not result in copyright infringement.
6. *Misinformation.*
   The use of AI does not result in the college producing a public document that contains incorrect, inaccurate, or misleading information.

Violations of this policy will subject employees and students to their respective disciplinary processes and other measures up to and including expulsion from the College or loss of employment. Illegal acts involving IT Resources may also subject violators to prosecution by local, state, and/or federal authorities. This policy and its enforcement is subject to the terms and conditions of the College’s Employee Handbook and the Student Code of Conduct.

APPROVAL AUTHORITY: Information Technology; Office of General Counsel

POLICY MANAGER: Information Technology