PROCEDURE - Montgomery College **70001CP**

Chapter: Information Technology Modification No. 001

Subject: **Responsible Use of Emerging Technologies**

I. Scope and Applicability

A. These procedures establish expectations for the responsible use of all emerging technologies at the College, including Artificial Intelligence (AI), Generative AI (GenAI), machine learning, Augmented Reality (AR), Virtual Reality (VR), and future technologies not yet introduced.

B. Recognizing that each technology may present unique risks, benefits, and regulatory considerations, specific requirements are articulated in these procedures for GenAI due to its known applications and impact, including potential disparate impacts on underserved groups. However, unless otherwise specified, users should assume that the same responsible-use principles, safeguards, and expectations apply to all other emerging technologies in compliance with College policy, mission, ethical standards, and applicable law.

C. These procedures apply to all emerging technologies, regardless of cost or access method.

II. Definitions

A. Artificial Intelligence (AI): A branch of computer science dealing with the simulation of intelligent human behavior in computers. It involves creating algorithms that enable machines to perform tasks that would typically require human intelligence.

B. College Data: In accordance with 66002: Confidential Data Management and Security, College Data encompasses all data or information that is used by or belongs to the College, or that is created, processed, stored, maintained, transmitted, or copied using College IT Resources.

C. Emerging Technologies: Innovative tools, services, systems, applications, or platforms in early stages of adoption with potential to significantly impact College operations, teaching, or learning.

D. Generative AI (GenAI): An AI that can generate text, images, or other media in response to prompts. These systems can create new content based on patterns and data on which they have been trained.

E. Protected Data: Any data not considered public (low risk). This includes sensitive (moderate risk) and confidential (high risk) data as further defined in 66002: Confidential Data Management and Security.

F. Public Domain: Information, content, or creative works not protected by intellectual property rights whether due to copyright expiration, forfeit, or ineligibility, and are therefore freely available for use by the public and may be used, shared, modified, or reproduced without permission or payment, provided such use complies with applicable laws and ethical standards.

G. Users: Employees, students, contractors, and authorized individuals with access to College Technology.

III. General Guidelines

A. The use of emerging technologies brings with it risks including, but not limited to, those associated with information security and data privacy, intellectual property and copyright issues, trustworthiness of generated content, academic integrity, potential bias, accessibility barriers, and disparate academic outcomes, as well as the limits and opportunities such tools place on critical thinking, retention of material, and performance.

B. The College's use of emerging technologies will be guided by the goal of serving students, benefiting employees and the community, and ensuring that its benefits are aligned with the College's mission and goals. The use of any emerging technology should not cause or perpetuate harm or bias against any group or protected classes.

C. The College must protect its data, comply with relevant data laws, preserve data integrity, and protect emerging technology tools from attack and unauthorized access through cybersecurity controls.

D. Emerging technology may enable College business, but does not replace the judgment or accountability of College Users and departments. Users are always accountable for ensuring that the data they share with emerging technologies complies with relevant College policies and applicable laws and for ensuring the accuracy and appropriate use of the output they generate.

E. The College will be transparent with its use of emerging technology, including GenAI, by making it clear when individuals are interacting with AI, what content was produced by AI, and the role of AI in decision-making.

F. Recognizing that members of the College community have varying levels of digital literacy and access, the College will provide appropriate guidance and differentiated training, resources, and supports to enable responsible and effective use of emerging technologies.

IV. Acceptable Use of Emerging Technologies

A. All emerging technology use is governed by and must comply with Policy 66001: Acceptable Use of Information Technology and related procedures.

B. For specific examples of acceptable and prohibited use of GenAI, Users should also refer to the Use Case Guidelines maintained by the Office of Information Technology (OIT) and are encouraged to confer with OIT for any clarification before using GenAI in academic, administrative, or professional activities at the College.

C. Purchasing, developing, and installing technology tools

1. All emerging technology acquisitions and associated contracts, End User License Requirements, or terms of service must comply with Policy 63001: Procurement, Consultant Services, and Contracts including

review by the OIT for security of College Data and by the Office of General Counsel for legal sufficiency.

2. Any User wishing to purchase or otherwise acquire emerging technology tools or services must follow the Technology Request Process to ensure that all requests are reviewed for security, accessibility, and legal considerations.

3. Requests for emerging technology will be considered on a case-by-case basis and in accordance with College's policy.

4. Implementation of any technology that interacts with the College's network infrastructure must be coordinated with and approved by the Office of Information Technology. Installation of unauthorized technology, networked devices or services is prohibited.

D. <u>Privacy and Security of Data</u>

1. Users must comply with College policy 66002: Confidential Data Management and Security.

2. Users should safeguard all College Data, which everyone at the College is legally and ethically obligated to protect.

3. Only College Data already in the Public Domain, such as on the College's website, may be entered into any AI or other emerging technology.

4. No Protected Data may be entered into any AI or other emerging technology, except in cases where the College has an agreement with the solutions provider that assures data protection or the User has obtained appropriate approvals in compliance with 66002: Confidential Data Management and Security.

5. Users are responsible for safeguarding the privacy and security of College Data during any meetings with external entities that may use AI or other emerging technology.

E. <u>User Accountability and Compliance Requirements</u>

1. Users are responsible for the outcomes of the emerging technology tools they use and should review all output for accuracy and potential bias.

2. With appropriate supports as needed, for example for multi-lingual or neurodivergent users, all Users must be able to explain how the output was generated and accurately explain its meaning.

3. Code, programs, or applications generated by automated tools, including artificial intelligence systems, should only be used in institutional information technology systems and services with human oversight and review, and with the prior approval by Vice President of Information Technology and Chief Information Officer or their designee.

4. All members of the College community are expected to comply with federal copyright law and College policy 68101: Use of Copyrighted Materials.

5. Outputs from GenAI and other emerging technologies may include copyrighted or proprietary material drawn from large public datasets, making authorship difficult to determine. Users must therefore treat all output as potentially protected and verify originality prior to use, using College-provided guidance as applicable, and must obtain necessary permissions before incorporating any content that may be subject to copyright or intellectual property restrictions.

6. Users must ensure that the use of GenAI complies with all applicable external requirements, including but not limited to grant or funding agency policies related to the preparation of a grant proposal, accrediting bodies, and regulatory authorities.

F. Prohibited Content

Users may not use emerging technology to generate, disseminate, or support content or activities that are used for harm, including but not limited to content that is used to:

1. Help create or carry out malware, spam and phishing campaigns, social engineering, or other cyber scams that defraud or mislead others;

2. Infringe upon copyright, trademark, or other intellectual property rights;

3. Promote or enable harm to self or others, including violence, the development or use of weapons, the destruction of property, or unauthorized activities that violate the security of any service or system, or to promote violence, hatred, or the suffering others;

4. Enables or contributes to bias, harassment, threats, defamation, hostile environments, stalking, exploitation, or discrimination based on protected attributes;

5. Otherwise violate any federal, state, or local law or regulation, or any College policy including through the creation of content offensive to the College’s students, employees, or the public.

6. Create an image, video, or audio to mimic or replicate another person’s voice or likeness without their written permission, including but not limited to the creation of “deepfakes” or other synthetic media intended to impersonate an individual.

G. Disclosure and Attribution

1. Users must disclose and appropriately attribute the use of emerging technology, including GenAI, when the output substantially informs a final product or communication such that it could reasonably be interpreted as the original work of the User in the absence of disclosure, and when doing so is necessary to maintain transparency or clarity of authorship.

2. Disclosure should include what tool was used and verification that the output was reviewed for accuracy. A sample disclosure statement is: “This content was generated in part by <GenAI Tool> and was reviewed by the following College employees: <list names and titles>.”

3. Users should refer to the Use Case Guidelines maintained by the Office of Information Technology (OIT) for further guidance, including examples and exceptions (e.g., informal use for ideation or editing).

V. Roles and Responsibilities

A. All Users

1. When using third-party emerging technologies that are not administered by the College, Users should assume that there are no standard College security, privacy, or compliance provisions available for these technologies. Usage is governed by this policy and its procedures and any other related or relevant College policies and procedures.

2. Emerging technologies represent a fast-evolving field and so, in addition to complying with this and other College policies and procedures, all Users should, given equitable access to training, time, and support from the College, make reasonable efforts to know and understand the best practices and ethical guidelines for each technology’s use.

3. Users are responsible for consulting with Chief Information Security Officer / IT Policy Administrator if they have any questions about acceptable use of GenAI in a particular situation.

B. Office of Information Technology (OIT)

1. OIT will work with departments to advise on the various security and privacy rules impacting data and whether the data is appropriate for, and may be used legally with, emerging technology and GenAI.

2. OIT will serve as a resource for Users seeking the use of emerging technologies in their work, teaching, or learning.

3. As part of the Technology request process, OIT will review all requests for emerging technologies tools and solutions in the context of security, privacy, and accessibility.

C. Instructional Faculty

1. Faculty are expected to adhere to the most current academic guidelines issued by the Office of Academic Affairs regarding the use of GenAI and any other emerging technologies for academic purposes, including the use of GenAI detection tools. These guidelines shall be consistent with and issued in accordance with this policy and its associated procedures and shall help to ensure equity in assessment and student learning differences.

2. Instructors should disclose to their students any use of GenAI and any other emerging technologies to support teaching and learning.

3. Instructors can establish their own rules and expectations for student use of emerging technologies and AI but must clearly communicate these in the course syllabus and offer clarifications, as appropriate in assignments to support students’ compliance with the policy and to foster students continued learning about the ethical use of emerging technologies and AI.

4. Because AI detection tools can be biased or inaccurate, they should be used cautiously and never as a standalone measure but only as part of a broader academic-integrity strategy that includes human review.

VI. Monitoring and Enforcement

In compliance with 66001: Acceptable Use of Information Technology:

A. The College reserves the right to audit the network and related systems at any time for security and maintenance purposes and to comply with applicable laws.

B. Users are reminded that all information created or received for work purposes and/or contained in College computing equipment files, servers or electronic communications located on College property or in College managed cloud services or depositories are public records that are created and maintained by public funds, and are available to the public unless an exception under the Maryland Public Information Act applies. Thus, while the College respects the desire for privacy, it may monitor access to the equipment and networking structures and systems and inspect network traffic for such purposes as ensuring the security and operating performance of its systems and networks; reviewing employee performance; and enforcing College policies, procedures, standards, and applicable federal, state, and local laws.

C. Any member of the College community who learns of a potential breach of data protection or confidentiality—including through the use of an emerging technology tool or service—must report the incident to the IT Service Desk as soon as possible.

D. Users who violate this policy or procedures may be disciplined pursuant to applicable College policies and procedures and may be reported to law enforcement authorities as appropriate.

E. The College is committed to equitable enforcement of this policy and will periodically review relevant disciplinary data to ensure fairness across student and employee groups.

Administrative Approval: