POLICY Board of Trustees - Montgomery College **76001**

Chapter: Information Technology Modification No. 004

Subject: **Acceptable Use of Information Technology**

I. Information technology is critical to carrying out the mission of the College. This policy, and its associated procedures, establish acceptable use of information technology resources made available to students, faculty, and staff, and any non-College individuals and entities specifically authorized to use these resources.

II. The same standards for all Users regarding the acceptable use of facilities, equipment and tools, as well as acceptable standards of behavior toward individuals while using these resources, apply to the use of information technology resources as well. The ability to use these resources is a privilege, not a right or guarantee, based on Board of Trustees' priorities and available funding. No one can or should assume that because this policy is silent on a particular act or behavior, or that just because one is capable of doing something, that it is then acceptable, condoned, or legal. The same disciplinary actions that apply to the misuse of other resources and behaviors may be applied to misuse of information technology resources.

III. All Users who request and/or are given access to College-owned and operated information technology resources agree to use those resources in a manner consistent with the mission of the College and in compliance with this and other policies, as well as all applicable federal, state, and local laws, procedures, rules and regulations.

IV. This policy and its associated procedures apply to use of the College's informational technology resources regardless of location, i.e., on site, at a remote work location, or while traveling domestically or internationally.

V. The Board of Trustees authorizes the president to establish any procedures necessary to implement this policy.

_____

Effective Date: July 21, 1997 (Interim Policy).
Modification Date(s): February 19, 2001; April 28, 2014, April 21, 2025.
Last Review Date: April 21, 2025.

I. Information Technology Resource ("IT Resources")

IT Resources include all electronic equipment, facilities, technologies, and data used for information processing, transfer, storage, display, printing, and communications by Montgomery College or its Users. These include, but are not limited to, computer hardware and software, computer labs, classroom technologies such as computer-based instructional management systems, and computing and electronic communications devices and services, email, networks, telephones, voicemail, facsimile transmissions, video, multi-function printing devices, mobile computer devices, data, multimedia and instructional materials. This definition also includes services that are owned, leased, operated, provided by, or otherwise connected to Montgomery College resources, such as cloud computing or any other connected/hosted service.

II. User Responsibilities

Users are expected to comply with legal, policy and procedure requirements and standards related to the use of IT Resources. These requirements include:

A. The User is expected to abide by College security requirements and will:

1. Use the College's IT Resources legally and in accordance with any required authorization.

2. Neither endanger the security of any College computer or network facility nor willfully interfere with others' authorized computer use.

3. Connect to College networks, including wireless networks, only with equipment/computers, including desktops, laptops, tablets, and smartphones or any other equipment, that meet any applicable Montgomery College Office of Information Technology (OIT) technical and security standards.

4. Provide reasonable security to one's passwords and respect the privacy and security of others' passwords.

5. Recognize that confidential information must be protected appropriately and in accordance with College policy. The College cannot guarantee the privacy of computer files, electronic communications, or other information stored on or transmitted by a computer or other device.

B. The User is expected to:

1. Abide by law in not participating in computer theft, computer trespass, invasion of privacy, computer forgery, password disclosure, or misleading transmittal of names or trademarks.

2. Abide by the laws of copyright and/or license agreements.

3. Understand that the College will not defend the User against any charges of criminal acts outside of the scope of employment involving the use of College-owned IT Resources.

4. Use the College's IT Resources for College business and mission purposes and limit other uses to occasional occurrences; such other uses must not have undue impact on the operation of the College's IT Resources, adversely affect the work or mission of the College, whether performed by the User or others, or violate any other provisions of policy or practice standards of the College.

5. Take responsibility for the materials they transmit through the College's electronic communications system and other College provided IT Resources and not violate College policy with such transmission.

6. Not harass, threaten, or otherwise cause harm to specific individuals through electronic communication; and not create what a casual observer might reasonably perceive to be an atmosphere of harassment, including sexual harassment. A casual observer may be anyone such as a fellow student, employee, or visitor.

C. Users shall adhere to a standard of behavior that is not disruptive to the business of the College and will:

1. Not impede, interfere with, impair or otherwise cause harm to the activities of others.

2. Not download or post to College computers, or transport across College networks, material that is illegal, proprietary, subject to copyright protection, in violation of College contracts or third party intellectual property rights, or that otherwise exposes the institution to liability.

3. Not use the College's electronic communication facilities to attempt unauthorized use or interfere with others' legitimate use of any computer or network facility anywhere.

4. Share computing resources in accordance with policies set for computers involved.

5. Use caution in downloading or distributing information and shall not create, install, or knowingly distribute computer malware or other destructive program on any IT Resource, regardless of whether any demonstrable harm results.

6. Use available software and hardware "as is" without attempting to modify or reconfigure the software or hardware of any IT Resource.

7. Report then delete phishing e-mails, spam, and other types of electronic fraud, and do not open or redistribute any suspicious items.

8. Follow College policy, procedure, and associated guidelines regarding the use of college email.

D. Users will be good stewards in the care and safeguarding of files and records and will:

1. Assure appropriate, responsible, and ethical care and use of College data.

2. Recognize that these responsibilities extend beyond the confines of any employment or contractual relationship with the College, and that any attempt to destroy or alter College records for purposes other than routine maintenance, whether hard copy or electronic, will be subject to disciplinary/legal action.

3. Comply with periodic requests to alter/change passwords and any training requirements associated with continued use and access to the College's resources.

III. Network Infrastructure

The College has built a very large and complex network, which includes wired, wireless, and external connections. Any uncoordinated installation of network infrastructure could cause unintended disruption to this network. Only Network Service Providers authorized by the Chief Information Officer are allowed to implement network infrastructure, including hubs, switches, routers, network firewalls, and wireless access points. Users are not allowed to offer alternate methods of access to MC's IT Resources, including by means such as modems and virtual private networks (VPNs) or network infrastructure services such as Domain Name System (DNS) and Dynamic Host Control Protocol (DHCP).

IV. College Responsibilities

A. The College is expected to adhere to industry standards and other best practices with regard to computer and telephone systems to provide adequate access to these resources with the optimum service levels possible, in accordance with legal requirements, Board of Trustees' policy, and within the approved budget. The Vice President of Information Technology/Chief Information Officer ("VP/CIO") is charged with directing and managing these efforts.

B. The College makes no warranties of any kind, either express or implied, that the functions or services provided by or through technology resources will be error free or without defect. The College will not be liable for any damage Users may suffer, including but not limited to loss of data, service interruptions or failure to deliver services. In addition, the College makes no representation or warranties, either express or implied, for data, information and materials obtained over the Internet and will not be liable for any damage Users may suffer as a result of relying upon such data or information.

V. Privacy Issues of Computer Use and Communications

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 are depositories and 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, Users should not have any expectation of privacy with regard to communications passed through the network or stored on computers that use it. The College 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 laws.

C. Examination, access, or the grant of access to current Users' files, electronic communications, or network transmission contents by OIT staff or its contractors, must be authorized beforehand by written approval from the Vice President of Information Technology and Chief Information Officer or their designee.

VI. College Web Servers/Electronic Publishing

A. The development and maintenance of a departmental or unit internet site and/or social media account is permitted through the College's computing resources as long as it complies with college policies, procedures, and guidelines including but not limited to 22003: Public Information, Communications, and Marketing.

B. In accordance with 22003: Public Information, Communications, and Marketing, personal internet sites and/or social media accounts that are operated by College employees, students, or consultants shall not represent that such accounts are being officially sanctioned, sponsored, or provided by the College. Such accounts shall not use the College's trademarks and logos without permission. If the content of the website makes reference to the College and/or can reasonably be used to connect the individual to the College, the website shall contain a disclaimer stating "that the page/site is not endorsed, sponsored or provided by or on behalf of Montgomery College."

VII. Policy Assurance

The IT Policy Administrator (ITPA), in conjunction with the Office of the General Counsel, is charged with ensuring compliance with policies and procedures applicable to information technology.

A. The ITPA is responsible to investigate on behalf of the Office of General Counsel (OGC) all reported violations and keep a record for OGC of each one. In the case of an alleged intellectual property infringement notification, the ITPA will respond in writing to the party sending the notification after conducting an investigation, maintaining a copy in ITPA files, subject to other instructions from the OGC.

B. The ITPA's investigation in coordination with OGC will include gathering

information, determining the likelihood that a violation has occurred, notifying all appropriate parties affected, and addressing IT system damage and repair actions. The ITPA will assess each situation and involve other College staff and/or external agencies as necessary to protect and repair the IT Resources of the College.

C. The ITPA will adhere to College policies and procedures in the investigation and disposition of each incident. Investigations may include such activities as:

1. A written notice to the supervisor of a person alleged to have committed a violation, with a request for appropriate actions;

2. A written notice to the Vice President of Human Resources, Development, and Engagement, requesting appropriate actions;

3. A written notice to the General Counsel requesting directions and guidance, including instances in which the ITPA recommends the involvement of law enforcement agencies or any other entity that may have jurisdiction.

D. The ITPA will submit a report to the President of the College or designee with a summary of incidents related to violation of the Acceptable Use Policy from time to time, but no less often than annually.

E. The ITPA has the authority to remove or restore access to IT Resources to any User who is believed to have violated the Acceptable Use Policy and/or procedures of the Acceptable Use Policy. Written notice must be given to the User, the User's supervisor, and the General Counsel when this action is anticipated. No further sanctions are within the ITPA's authority.

F. Appeals concerning the decision and actions of the ITPA are permitted. The appeals process is:

1. All appeals must be addressed to the VP/CIO, within ten (10) days of the decision of the ITPA.

2. Appeals must be in writing, stating specifically the basis of the appeal.

3. The VP/CIO will make a decision regarding the appeal within ten (10) days of receipt of the appeal.

4. The decision of the VP/CIO regarding an appeal will be in writing.

5. Nothing in this process prevents the User whose access to IT Resources has been restricted from pursuing other avenues of appeal that may be available under College policy or law.

Administrative Approval: February 19, 2001; August 27, 2001; March 25, 2004; April 28, 2014; December 1, 2021; April 2, 2025.