

MONTCLAIR

STATE UNIVERSITY

Responsible Use of Computing	
Responsible Office:	Information Technology
Policy Summary:	Outlines the standards for acceptable use of University computing and information technology resources
Effective Date:	
Last Revision Date:	

I. Purpose

As a part of the physical and social learning infrastructure, Montclair State University acquires, develops, and maintains computers, computer systems and networks. These computing resources are intended for University-related purposes, including direct and indirect support of the University's instruction, research, and service missions; University administrative functions; student and campus life activities; and contributions to knowledge, the profession and the educational environment of the University through the free exchange of ideas among members of the University community and between the University community and the wider local, national and international communities.

Computer systems and networks owned or operated by Montclair State University provide access to resources on and off campus. Such open access is a privilege and imposes upon users certain responsibilities and obligations. Access is granted subject to University policies, and local, state, and federal laws. Use of these resources must be consistent with professional standards and University policies; reflect the principles of academic integrity; show restraint in the consumption of shared resources; and adhere to law and University policy in regard to intellectual property, ownership of data, copyright, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment.

The rights of academic and political freedom and freedom of expression apply to the use of University computing resources. So, too, however, do the responsibilities and limitations associated with those rights. Therefore, legitimate use of a computer, computer system, or network does not extend to whatever is technically possible. Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

All information, records and material maintained on the University's computers and computing systems by University employees is the property of the University. Notwithstanding the above principle, the University acknowledges that faculty members may have an expectation, consistent with general practice in American higher education and any applicable collective bargaining agreement, of a proprietary interest in their scholarly and research materials, similar to the same interest they would have in handwritten materials produced within the scope of their employment.

This policy outlines the standards for acceptable use of University computing and information technology resources, which include, but are not limited to, equipment, software, networks, data and telephones, whether owned, leased or otherwise provided by Montclair State University.

II. Applicability

This policy applies to all users of computing and information technology resources owned or managed by Montclair State University, including resources available to the University through outsourced and applications service provider arrangements. Individuals covered by this policy include, but are not limited to, faculty, staff, students, guests, external individuals or organizations and individuals accessing the University's information resources through external network services, such as the Internet.

Computing resources include all University owned, licensed or managed hardware and software, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

This policy applies to technology administered in individual departments and resources administered by central administrative departments, such as the University Library and Office of Information Technology. Additional policies may apply to specific computers, computer systems, or networks provided or operated by specific units of the University or to uses within specific units. Users must consult the managers of the specific computer, computer system or network for further information.

III. Definitions (as applicable)

IV. Policy

Preserving access to information resources is an effort that requires each member of the University community to act responsibly and guard against abuses. Therefore, anyone who accesses or uses the University's computing resources in any way is obligated to abide by the following standards of acceptable and ethical use.

All users of university computing resources must:

- Comply with all federal, New Jersey and other applicable laws; all University rules and policies; and all contracts and licenses. Examples of such laws, rules, policies, contracts and licenses include the laws of libel, privacy, copyright, trademark, obscenity and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and

Abuse Act, which prohibit various activities; the University's code of student conduct; the University's sexual harassment policy; and all applicable software licenses. Users are responsible for ascertaining, understanding and complying with the applicable laws, rules, policies, contracts, and licenses governing their computing activities.

- Use only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized. Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the University.
- Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. The ability to access other persons' accounts does not imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.
- Respect the finite capacity of computer resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. Although there is no set bandwidth, disk space, or other limit applicable to all users of University computing resources, the University may require users to limit or refrain from specific uses in accordance with this principle, and users are required to constrain their use to reasonable limits. The reasonableness of any particular use will be judged in the context of all relevant circumstances.
- Refrain from using computing resources for personal commercial purposes or for personal financial or other gain. Limited, occasional personal use of University computing resources is permitted where such use does not constitute commercial activity or activity for financial or other gain and when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other University responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures and as clarified in the State of New Jersey's Uniform Code of Ethics and the Student, Faculty and Employee Handbooks published by the University.
- Refrain from stating or implying that they speak on behalf of the University and from using University trademarks and logos without authorization to do so. Affiliation with the University does not, by itself, imply authorization to speak on behalf of the University nor does it permit members of the community to use the University's trademarks and logos without the prior approval of University Counsel or the Vice President for University Advancement. Please consult the University Code of Ethics and Policy #1.5.97 for further clarification of requirements regarding disclaimers on expressive personal opinions and the use of University trademarks and logos.

Security and Privacy

The University employs various measures to protect the security of its computing resources and of users' accounts. Users should be aware, however, that the University cannot guarantee such security. Users should, therefore, be resolved in their efforts to establish appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly.

Users should also be aware that their uses of University computing resources are not completely private. While the University does not routinely monitor individual usage of its computing resources, normal operation and maintenance require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and similar activities that are necessary for the provision of service. The University may also specifically monitor the activity and accounts of individual users, including individual login sessions and communications, without notice, at its discretion, when (a) the user has voluntarily made them accessible to the public, as by posting to a web page; (b) the University requires access to information regarding the individual's use of the computing resource; (c) it reasonably appears necessary to do so to protect the integrity, security or functionality of the University or other computing resources or to protect the University from liability; (d) there is reasonable cause to believe that the user has violated, or is violating, University policies; (e) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or (f) it is otherwise required or permitted by law. Any such individual monitoring, other than that specified in "(a)", required by law, or necessary to respond to perceived emergency situations, will be authorized in advance by the President, Vice President for Academic Affairs or the Vice President for Information Technology, or their designees. All records of these authorizations will be maintained in a secure file by the Vice President for Information Technology as this is the unit that actually implements such requests.

The University, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate University personnel or law enforcement agencies and may use those results in appropriate University disciplinary proceedings. Communications made by means of University computing resources are also generally subject to New Jersey's Open Public Records Act to the same extent as they would be if made on paper. Further clarification regarding the Open Public Records Act may be obtained at (<http://www.njarchives.org/links/pdf/circular-letter-03-10-st.pdf>).

Policy Addenda and Notifications

The University will, through appropriate administrative procedures, periodically amend this policy and generate addenda to it. When available, general notification will be made to the University community by means of electronic distribution lists and the University's web page. In addition, in order to ensure that all Users have an opportunity to read and proactively affirm their acceptance of University computing policies, on an annual basis the University will deactivate all user accounts. Reactivation will be contingent upon a review by all Users of all applicable computing policies and affirmation that these policies have been read, understood, and acknowledged.

V. Procedure (as applicable)

Enforcement

Violation of this computing policy threatens the atmosphere for the sharing of information, the free exchange of ideas and the secure environment for creating and maintaining information. Such violations of the University Computing Policy are treated like any other ethical violation as outlined in the Student Handbook, relevant contractual agreements, and applicable faculty and staff handbooks. Violators may also be subject to prosecution under applicable Federal and New Jersey Statutes.

The University may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures at its discretion and when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of University or other computing resources or to protect the University from liability. The record of such action consists of a written request to the Vice President for Information Technology and a copy to the University Counsel.

The University may also refer suspected violations of applicable law to appropriate law enforcement

VI. References