

**ADDITION OR REVISION OF AN ADMINISTRATIVE PROCEDURE OR BOARD POLICY
TRANSMISSION COVER SHEET
JANUARY 2011**

Title/Issue

Administrative Procedure

Board Policy

AP 3720	Use of Technology and Information Resources
----------------	--

New Revision of Existing CCLC Recommendation Legal Counsel

Originated by: _____ Ext. _____ Date: _____

**Send transmission cover sheet (as part of the proposal) to the Vice President, Instruction electronically.
It will be reviewed at the next Academic Mutual Agreement Council (AMAC) meeting.**

Academic or Professional Matter

Reviewed by AMAC on 1/10 /2011

Is this an Academic & Professional Matter? yes no

Details of what Academic & Professional matters include (according to Title V, Article 2, Section 53200) are on the following page.

Institutional Review Matter

Distributed on _____ / _____ / _____

to:

Is this an Institutional Review Matter? yes no

Assigned Administrator	Date
Audrey Yamagata-Noji	3/21/2011
Council/Committee Approval	Approved as presented? Date
SP&S	Yes 4/18/2011
Academic Senate	Approved as presented? Date
College President	Approved as presented? Date
AMAC Academic Mutual Agreement Council	Approved as presented? Date
Returned completed copy of cover sheet to originator and assigned administrator.	Date

Assigned Administrator	Date
Council/ Committee Approval	Approved as presented? Date
Bargaining Agents (if applicable) Please respond to the assigned administrator within 30 days of receipt or it will be deemed approved as presented.	Approved as presented? Date
College President	Approved as presented? Date
PAC President's Advisory Committee	Approved as presented? Date
Returned completed copy of cover sheet to originator and assigned administrator.	Date

APPLICABLE TO BOTH ACADEMIC AND NON-ACADEMIC MATTERS:

Sent to the President's Office	Date
Sent to Webmaster for posting to the Web	Date

Board of Trustees (Board Policies)	Approved as presented?	Date
Confirmed that posting is complete	Date	

Assigned Administrator –
NOW THAT THE POLICY HAS CHANGED...did you?

Make a campus announcement via email regarding the change?

Check to make sure that any **forms** used to carry out this policy have been changed?

Contact the person(s) responsible for changing the language in the catalog and schedule?

Contact IT if programming changes are needed to implement policy?

COMMENTS:

1/10/11-Reviewed at AMAC-Audrey assigned as administrator and take to SP&S.

Academic & Professional matters include: (according to Title V, Article 2, Section 53200)

1. Curriculum, including establishing prerequisites and placing courses within disciplines
2. Degree and certificate requirements
3. Grading policies
4. Education program development
5. Standards or policies regarding student preparation and success
6. District and college governance structures, as related to faculty roles
7. Faculty roles and involvement in accreditation
8. Policies for faculty professional development activities
9. Processes for program review
10. Processes for institutional planning and budget development
11. Other academic and professional matters as mutually agreed upon between the governing board and the academic senate

Chapter 3 – General Institution

AP 3720 ~~Computer and Network~~ Use of Technology and Information Resources

References:

Education Code Section 70902; 17 U.S.C. § 101 et seq. (Copyright Act); Penal Code Section 502

The College ~~Computer and Network systems~~ technology systems and tools are the sole property of Mt. San Antonio College. They may not be used by any person without the proper authorization of the College. The ~~Computer and Network systems~~ technology systems and tools are for College instructional and work related purposes.

This procedure applies to all Mt. San Antonio College students, faculty, and staff and to others granted use of College information resources. This procedure refers to all College information resources whether individually controlled or shared, stand-alone, or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the College. This includes personal computers, workstations, ~~mainframes, minicomputers,~~ and associated peripherals, software and information resources, regardless of whether used for administration, research, teaching or other purposes.

Conditions of Use

Individual units within the College may define additional conditions of use for information resources under their control. These statements must be consistent with this overall procedure but may provide additional detail, guidelines and/or restrictions.

Legal Process

This procedure exists within the framework of the College Board Policy and State and federal laws. A user of College information resources who is found to have violated any of these policies will be subject to disciplinary action up to and including but not limited to loss of information resources privileges; disciplinary suspension or termination from employment or expulsion; and/or civil or criminal legal action.

Copyrights and Licenses

Computer users must respect copyrights and licenses to software and other on-line information.

- Copying - Software protected by copyright may not be copied except as expressly permitted by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any College facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.
- Number of Simultaneous Users - The number and distribution of copies must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.
- Copyrights - In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright, **including Fair Use** and other laws. ~~Copied material must be properly attributed.~~ Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited.

Integrity of Information Resources

Computer users must respect the integrity of computer-based information resources.

- Modification or Removal of Equipment - Computer users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization.
- Unauthorized Use - Computer users must not interfere with others access and use of the College computers. This includes, but is not limited to: the sending of ~~chain letters~~ or excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs, running grossly inefficient programs when efficient alternatives are known by the user to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a College computer or network; and damaging or vandalizing College computing facilities, equipment, software or computer files.
- Unauthorized Programs - Computer users must not intentionally develop or use programs which disrupt other computer users or which access private or restricted portions of the system, or which damage the software or hardware components of the system. Computer users must ensure that they do not use programs or utilities that interfere with other computer users or that modify normally protected or restricted portions of the system or user accounts. The use of any unauthorized or destructive program will result in disciplinary action as provided in this procedure, and may further lead to civil or criminal legal proceedings.

Unauthorized Access

Computer users must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access.

- Abuse of Computing Privileges - Users of College information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the College. For example, abuse of the networks to which the College belongs or the computers at other sites connected to those networks will be treated as an abuse of College computing privileges.
- Reporting Problems - Any defects discovered in system accounting or system security must be reported promptly to the appropriate system manager so that steps can be taken to investigate and solve the problem.
- Password Protection - A computer user who has been authorized to use a password protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the system manager.

Usage

Computer users must respect the rights of other computer users. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of College procedure and may violate applicable law.

- Unlawful Messages - Users may not use electronic communication facilities to send defamatory, fraudulent, harassing, obscene, threatening, or other messages that violate applicable federal, State or other law or College policy, or which constitute the unauthorized release of confidential information.
- Commercial Usage - Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions (see Commercial Use,

below). Some public discussion groups have been designated for selling items and may be used appropriately, according to the stated purpose of the group(s).

- Information Belonging to Others - Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users, without the permission of those other users.
- Rights of Individuals - Users must not release any individual's (student, faculty, and staff) **personal** information to anyone without proper authorization.
- User identification - Users shall not send communications or messages anonymously or without accurately identifying the originating account or station.
- Political, Personal and Commercial Use - The College is a non-profit, tax-exempt organization and, as such, is subject to specific federal, State and local laws regarding sources of income, political activities, use of property, and similar matters.
- Political Use - College information resources must not be used for partisan political activities where prohibited by federal, State or other applicable laws.
- Personal Use - College information resources should not be used for personal activities not related to appropriate College functions, except in a purely incidental manner.
- Commercial Use - College information resources should not be used for commercial purposes. Users also are reminded that the ".cc" and ".edu" domains on the Internet have rules restricting or prohibiting commercial use, and users may not conduct activities not appropriately within the those domains.
- **Captioning / Closed Captioning – All video media posted to the Internet or Intranet must be captioned, or sub-titled, or sub-titled for deaf and hard of hearing.**
- **Remote Access – Remote access to sensitive College systems is provided by Virtual Private Network (VPN) based on critical business need. Faculty and staff may request VPN access by completing the VPN request form and obtaining the appropriate approval signatures. Request for VPN access must be approved by the CTO. Mt. SAC reserves the right to audit all VPN client systems and all communications between VPN client systems and Mt. SAC's network for compliance with all applicable security requirements.**

All Mt. San Antonio College related email communications must be conducted using an email address assigned by the College. This restriction is necessary because email originating at the College may contain proprietary information regarding students, staff, or internal College business. The College is responsible for the security of this information and cannot assume that other email providers will provide adequate levels of data backup, security, and virus protection. ~~Therefore, forwarding of email from a Mt. San Antonio College email address to a non Mt. San Antonio College email address is not authorized or allowed.~~ Additionally, **Therefore**, users may not configure any email program or service to use an automated process for forwarding Mt. San Antonio College email to any other email address.

~~Employees must not use their personal electronic mail accounts with an Internet Service Provider (ISP) or any other third party provider while using Mt. San Antonio College computers. To do so would circumvent logging, anti-virus scanning controls, and backup controls that the College has established.~~

Social Media

Social networking includes networking sites that communicate via the Internet and networking sites that use SMS text or mobile technologies. All genres of social networking sites or media will be referred to below as social media. Currently popular examples of social media include Facebook, MySpace, and Twitter.

Social Media Responsibility

College employees are responsible for the content they post to social media. The College will not indemnify employees for anything they write on a social media associated with the College, or on any other social media.

- College Coursework - Faculty utilizing social media to enhance instruction can act as their own site administrator in accordance with these procedures.
- College Departments - Social media for a College department requires prior approval from the department administrator. An email or written proposal or approval will suffice. Social media for College departments will have a minimum of two site administrators assigned. If a site administrator leaves the College, the department administrator will assign another in their place and the account password will be changed.
- College Clubs and Organizations - Social media for college clubs and organizations cannot be affiliated with the College without prior approval from the College club sponsor/advisor or other college employee. Social media for college clubs and organizations should have two site administrators of which at least one is a College employee. Those site administrators can optionally authorize and assign student site administrator(s), and revoke those privileges if the student site administrator(s) is not acting in accordance with these procedures.

The site administrator(s) shall post their name and a contact method prominently on the site. Site administrators for social media agree to check their pages regularly.

The following types of content are prohibited from social media officially affiliated with Mt. SAC and may be removed by the site administrator upon discovery:

- Derogatory language that can reasonably be interpreted as harassing or threatening any third party
- Language or images encouraging or depicting sexual harassment, vandalism, stalking, drinking, drug use, criminal activity, or other behavior prohibited by the Student Standards of Conduct
- Content that violates State or federal law, including online gambling and the use (without permission) of copyrighted material
- Information that is obviously libelous
- Pornography or patently obscene material as defined by law

Nondiscrimination

All users have the right to be free from any conduct connected with the use of the Mt. San Antonio College network and computer resources which discriminates against any person on the basis of BP

3410. No user shall use the College network and computer resources to transmit any message, create any communication of any kind, or store information which violates any College procedure regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

Disclosure

No Expectation of Privacy – Mt. San Antonio College reserves the right to monitor all use of the College network and computer to assure compliance with these policies. Users should be aware that they have no expectation of privacy in the use of the College network and computer resources. Mt. San Antonio College will exercise this right only for legitimate College purposes, including, but not limited to, ensuring compliance with this procedure and the integrity and security of the system.

Possibility of Disclosure - Users must be aware of the possibility of unintended disclosure of communications.

Retrieval - It is possible for information entered on or transmitted via computer and communications systems to be retrieved, even if a user has deleted such information.

Public Records - The California Public Records Act (Government Code Sections 6250 et seq.) includes computer transmissions in the definition of “public record” and nonexempt communications made on the College network and computer must be disclosed if requested by a member of the public.

Litigation - Computer transmissions may be discoverable in litigation.

Dissemination And User Acknowledgment

All users shall be provided copies of these procedures and be directed to familiarize themselves with them.

~~Users shall sign and date the acknowledgment and waiver included in this procedure stating that they have read and understand this procedure, and will comply with it. This acknowledgment and waiver shall be in the form as follows:~~

~~Employee Acceptable Use Agreement~~

~~Mt. San Antonio College (hereinafter also referred to as the “College”) provides broad access to its computing, communications and information resources. These resources support the delivery of the College's academic mission and, accordingly, they must be used responsibly. These resources include the physical data communications network and all computers, printers, scanners and other hardware attached to that network, as well as all system software, telephone systems, and means of access to the Internet.~~

~~With regard to the computing, communications and information resources of Mt. San Antonio College, it is understood and agreed that:~~

- ~~• Mt. San Antonio College's computing, communication and information resources are provided for the support of its educational and service goals and the use of such resources for other purposes is prohibited. However, incidental personal use is permissible so long as: (a) it does not consume more than a trivial amount of system resources; (b) it does not interfere with the productivity of other campus employees, and (c) it does not preempt any College activity.~~
- ~~• The College and its employees are to abide by this policy along with any local, State, and federal laws that may apply. All users are subject to both the provisions of this agreement, as well as any policies specific to the individual systems they use.~~

- ~~• The confidentiality of student and staff information is protected under federal and State law and/or regulations. Any information regarding students or staff that an employee (acting alone or on behalf of the College) might access in the course of a work assignment through a computer, student file, or other documentation, is to be used strictly to perform job duties and may only be shared with those who are authorized to have such information. Employees (acting alone or on behalf of the College) may not change, alter, copy, or divulge any such information unless it is required to carry out a Mt. SAC job assignment.~~
- ~~• To protect the integrity of computing resources, passwords, access codes or account names must not be shared with others. Additionally, passwords may be subject to complexity requirements and employees may be required to change their passwords periodically.~~
- ~~• Most educational materials (both commercial and faculty-created, including software) are protected under copyright. Any violation of the rights of a person or entity protected by copyright law is prohibited. The unauthorized duplication, installation, or distribution of computer software utilizing the College's computing, communications and information resources is specifically prohibited.~~
- ~~• Unauthorized software installed on College owned computers will not be supported and may be removed if deemed necessary.~~
- ~~• Employees may not connect any system or install software which could allow any user to gain access to the College's system and information without written approval from the Chief Technology Officer or his/her designee.~~
- ~~• Employees may not use Mt. San Antonio College resources for conducting a private business or for personal financial gain.~~
- ~~• Intentionally sending or accessing pornography or patently obscene material other than for authorized research or instructional purposes is prohibited. The definitions of "pornography" and "obscene" shall be as determined by law.~~
- ~~• Employees found in violation of the College's computer use policies are subject to proper disciplinary action, including the reporting of such activity to the appropriate authorities as required by law. Employees must consider the open nature of information transferred electronically, and should not assume an absolute guarantee of privacy or restricted access to such information. The College provides the highest degree of security possible when transferring data, but disclaims responsibility if these security measures are circumvented and the information is compromised.~~
- ~~• Mt. San Antonio College is not responsible for loss of data, time delay, system performance, software performance, or any other damages arising from the use of College computing resources. Therefore, employees are encouraged to secure backup copies of their own files.~~
- ~~• Authorized College personnel may, while performing routine or investigative operations have access to data, including electronic mail, web browser information, and any other personal data stored on College computers. However, the College shall not routinely or arbitrarily monitor incidental personal use of college resources. Neither the College nor any of its employees (acting alone or on behalf of the College) shall disclose the contents of observed personal data to any other person or entity except as required by law or Board Policy.~~

- ~~Activities that place excessive strain on network resources, (e.g.: net radio, other similar streaming media, or online gaming) are not allowed without written approval from the Chief Technology Officer or his/her designee.~~

Selected Examples of Unacceptable Use:

- ~~Revealing passwords to others, or allowing someone else to use one's account.~~
- ~~Utilizing network or system id numbers/names that are not assigned for one's specific use on the designated system.~~
- ~~Attempting to authorize, delete, or alter files or systems not created by oneself without authorization from the Chief Technology Officer or his/her designee.~~
- ~~Watching Internet videos or listening to Internet radio on one's computer without authorization from the Chief Technology Officer or his/her designee.~~
- ~~Not complying with requests from designated personnel to discontinue activities that threaten the integrity of computing resources.~~
- ~~Attempting to defeat data protection schemes or to uncover security vulnerabilities.~~
- ~~Registering a Mt. San Antonio College IP address with any other domain name.~~
- ~~Unauthorized network scanning or attempts to intercept network traffic.~~
- ~~Malicious disruptions such as intentionally introducing a computer virus to the campus network.~~
- ~~Harassing or threatening other users of the campus network.~~
- ~~Connecting unauthorized equipment directly to the campus network. (Devices such as PDAs, printers, and USB drives that connect to a computer and not directly to the network are acceptable.)~~

~~The above stated provisions and terms constitute the entire agreement between the College and employee as to their agreed upon rights and duties as such relate to the utilization of the Computing, Communications and Information Resources at Mt. San Antonio College. These terms are subject to change only upon mutual written agreement between the College and the Faculty Association. The College shall make the current version of this document available at <http://infosecurity.mtsac.edu>. All Parties are put on notice that a violation of the above terms and provisions may result in civil, criminal, or other administrative action.~~

~~As an employee of Mt. San Antonio College, I certify that I have read and have received a copy of this agreement.~~

~~Name: _____ Date: _____~~