Acceptable Use Policy

1. Introduction

This document constitutes a university-wide policy designed to ensure the availability of computers, data networks, services and other computer-related resources to students, faculty and staff of Mount Saint Mary's University ("MSMU" or the "University"). The policy reflects the standards of the University community and indicates in general, what privileges and responsibilities are characteristic of the University computing environment. Because some networks operate in environments in which certain specific items in this policy do not apply, system administrators are free to create policies that are at a variance (although not inconsistent) to this one. In such cases the departmental system administrators should make relevant variances known to their users. The following policy, rules and conditions apply to all users of MSMU computing resources and services. Violations of this policy are possibly unlawful. Violations may result in disciplinary action that could result in expulsion from the University, dismissal from a position and/or legal action.

2. Terminology

A number of terms used below have very specific meanings within the context of this document. We define them as:

- Networked Computer: A computer system that is connected to any MSMU data network.
- Shared Computing Resource: A networked computer and its peripherals that can be used by more than one person; i.e., a server.
- Central Facilities: Refers to networked computers and peripherals purchased, maintained, and operated by the Office of Information Technology and made available to the entire University community.
- Departmental: Refers to networked computers and peripherals purchased by University departments or other administrative units, primarily for the use of the unit's personnel.
- Individual: Refers to networked computers purchased for use by an individual member of the University community.
- System Manager: The person or group responsible for the operation and security of one or more networked computers (the person or group with system privileges).
- System Administrator: The person having executive authority over one or more networked computers.

3. General Policies

Computer use has become an essential part of many University activities. While much computing is now done on departmental or individual computers (personal computers, workstations, and mobile devices) most information sources, software and data-networking systems reside on shared, central computers or use shared networks. The Office of Information Technology ("OIT") has responsibility for providing and maintaining shared computing tools. Mount Saint Mary's University works to create an intellectual environment in which students, faculty and staff may feel free to create and collaborate with colleagues both on and off campus without fear that the products of these intellectual efforts will be violated by misrepresentation, tampering, illegal access, destruction or theft. General policies regarding the resources the University provides are outlined in this document.

3.1 Indemnification of Liability

Users of University computing resources agree that neither the University nor OIT will be responsible for any direct, indirect, consequential, special or punitive damages or losses users may incur in connection with University computing resources, data or other materials transmitted through or residing on University systems, even if the University has been advised of the possibility of such damage or loss. In addition, users agree to defend and indemnify the University and hold the University harmless from and against any and all claims, proceedings, damages, injuries, liabilities, losses, costs and expenses (including reasonable attorneys' fees)

relating to any acts by user or materials or information transmitted by such user in connection with the University's systems leading wholly or partially to claims against the University and its systems by other users or third parties.

3.2 Access

MSMU strives to provide privacy and a fair share of technical resources to all members of the University community whose work requires it. Fees may be charged for some services. All computer users have the responsibility to use these resources, as they would any public resource of the University, in an efficient, effective, respectful and lawful manner. Computer users may not use MSMU's computer resources in any way that may be seen as insulting, defamatory, obscene, harassing, discriminatory, threatening, disruptive or offensive to other persons. When using MSMU's computer resources, individuals must comply with MSMU's rules and policies, the mission of the University, as well as all federal, California, and other applicable laws, regulations and ordinances.

3.3 Availability

MSMU will make its computing resources and networks available to users with the fewest interruptions as possible.

4. Specific Policies

Specific applications such as e-mail and circumstances demand policies to regulate usage.

4.1 E-mail Attachment Policy

In an attempt to reduce problems caused by virus-infected e-mail attachments, we have begun intensive scanning of all inbound and outbound e-mail. We are no longer allowing the following file types to be sent or received through the e-mail system or stored in your mailbox:
***.SCR *.PIF *.COM *.EXE *.CMD *.BAT**

These file types are often used to spread viruses and not typically associated with ANY word processing, spreadsheet or database application and do not represent any type of image or graphic file. If an attachment is found, the e-mail will be dropped and the file deleted based solely on the attachment having one of these six extensions.

If you need to send or receive a legitimate file with one of these six extensions, you will need to rename the file to a different extension — or have the sender rename the file — and provide instructions on returning it to its original type/extension after downloading it to your desktop.

As a result of this policy and scanning capability, you should see far less "spam" or junk mail appearing in your mailbox. As always, if you have any questions or concerns, please contact the IT Service Desk at x2970.

4.2 E-mail Communication Policy

Upon admittance, all students are assigned an official University e-mail address that will be maintained on the University's e-mail directory for at least one term after the student's last enrollment at the University. Students are allocated 50GB of storage space for their respective e-mail accounts and are encouraged to manage their mail volume and archiving so as not to exceed this limit

All official University communications will be sent to your official University student e-mail address: username@msmu.edu. Students may forward their e-mail from the official University e-mail address to another e-mail address of the student's choice. The University, however, is not responsible for e-mail forwarded to another e-mail address, and students who do so, do so at their own risk.

4.3 Music/Video File Downloading Policy

OIT decision makers block, to the best of our ability, downloading and sharing music and video files. This is based solely on the legality questions surrounding this issue.
.

4.4 Connecting to the Internet from your Dorm Room

Each dormitory room is configured with a phone line and a data line. However, the phone line cannot be used as a modem line. The data line is an Ethernet connection to which you can connect your PC or Macintosh to access the University's Internet connection and e-mail services. In order to use the Ethernet connection, your PC or Macintosh must be equipped with a 100/1000mb network interface card. A network cable is also needed.

4.5 Other Networking

Note: the following items are not permitted for use by faculty, staff or students without the written consent of OIT:

- Network Hubs\Routers\Firewalls
- Network Switches
- Wireless Hubs
- Wireless Switches
- Mobile Hotspots
- Other networking devices

5. Security

MSMU will help users of its central computing resources protect the information they store on those resources from accidental loss, tampering, or unauthorized search or other access. Appropriate information on the security procedures implemented on each central or campus resource will be made available by the system administrator. In the event of inadvertent or non-malicious actions resulting in the loss of or damage to that information, OIT will make a reasonable effort to restore the lost or damaged information. In most cases, however, ultimate responsibility for prevention and resolution of such problems rests with the individual computer user.

All computer system users are to assume there is no security of text and data files stored in "public" volumes on shared or personal computer resources accessible by the campus community as a whole. Users may request that arrangements be made to protect information stored on such resources. These requests will be honored within limitations of the systems administrator managing the resource.

The system administrators of shared and individual computing resources are responsible for the security of information stored on those resources, for making appropriate information on security procedures available to users of those systems, and for keeping those systems free from unauthorized access.

Internet linkages allow national and international communications, file transfer and computer processing. Use is appropriate only for purposes permitted in networking guidelines and acceptable use policies.

Although it may be possible to connect to other systems through the network, this ability does not imply the right to make use of these systems without proper authorization. All users of any networking resources should be cautious when downloading files to protect one's confidentiality and security and to guard against computer viruses.

6. Confidentiality

OIT will attempt to maintain the security and appropriate confidentiality of all information stored on their computing resources. Users have no right to expect information stored on computing resources will remain confidential from those who need to know for reasons of operational necessity or in instances where the University has reason to believe the user is using these resources in a way inconsistent with the University's institutional purposes or mission or in an illegal manner.

For the purpose of this policy statement, electronic communications includes but is not limited to electronic mail, electronic files, internet services, voice mail, audio and video conferencing sent or received by faculty, staff, students or other authorized users of University computing resources. The University reserves the right to access and disclose as necessary, all messages sent over its systems, without regard to content and without permission from employees and students.

If any computing resource user has evidence of the fact that his or her privacy or other rights have been infringed upon by another user, the affected party may ask for monitoring or inspection through the appropriate University office or legal authority. All individuals involved in authorizing the monitoring must keep permanent copies of requests.

7. Censorship

Free expression of ideas is central to the academic process. MSMU computer System Administrators will not remove any information from individual accounts or from electronic bulletin boards maintained on them unless the appropriate System Administrator finds that:

- The presence of the information on the bulletin board involves illegality (e.g., copyrighted material, software used in violation of a license agreement, etc.);
- The information in some way endangers computing resources or the information of other users (e.g., a computer worm, virus or other destructive or malicious program);
- The information is inappropriate because it is unrelated to or is inconsistent with MSMU’s rules and policies, the mission of the University, and/or federal, California, and other applicable laws, regulations and ordinances (e.g. policies, laws and regulations prohibiting harassment, discrimination, retaliation; and/or violation of individuals’ privacy rights); or
- The information is not in compliance with the Restrictions on Usage listed in the section, "Responsibilities of the User."

OIT may remove from shared computers any information that is inappropriate, as defined above. Specific guidelines for appropriate use of each MSMU bulletin board system will be available on that system. Users whose information is removed will be notified by the systems administrator of the removal as soon as is feasible. Users who wish to appeal such removal of information may do so through an appeal board made up of the governing body appropriate to the system and status of the user. If no appeal board exists, then in such cases, the appeal may be made to the Vice President of Strategic Initiatives and Strategic Initiatives & Chief Technology Officer (CTO)

8. Responsibilities of the User

Access to computing resources is a privilege made available to all University faculty, staff and students, not a right. Certain responsibilities accompany that privilege, and understanding them is important for all computer users.

8.1 Institutional Purposes

Use of MSMU computing-related resources is for purposes related to the University's mission. We all must be responsible stewards of these resources. All classes of computer service user (faculty, staff and students) may use computing resources only for purposes related to their studies, their instruction, the discharge of their duties as employees, their official business with the University and their other University-sanctioned activities. The use of MSMU computing resources for academically related but commercial purposes is permitted only with approval of the Provost and the VP of Strategic Initiatives & Chief Technology Officer (CTO). When faculty or staff utilize computing and technical resources not owned, managed or maintained by the University to conduct University business such as teaching and/or other administrative tasks, faculty and staff will abide by the terms and conditions contained within this Acceptable Use Policy. Furthermore, faculty and staff will engage in such usage with permission from Chairs, Deans or Departmental Supervisors/Managers.

8.2 Security

The user is responsible for correct and sufficient use of the tools each computer system provides for maintaining the security and confidentiality of stored information. For example:

- Computer accounts, passwords and other types of authorization are assigned to individual users and must not be shared with others. Each user is responsible for making authorized use of resources only for intended purposes, and is responsible for all transactions made under the assigned account number.
- The user must select an obscure account password and change it frequently.
- The user must understand the level of protection each computer system automatically applies to files and supplement it, if necessary, for sensitive information.
- The microcomputer user must be aware of computer viruses and other destructive computer programs and take steps to avoid being their victim.

8.3 Restrictions on Usage

Computing resources may be used to further the mission of the University in any way associated with teaching, learning, research, administrative or public services. Users must comply with all federal, California, and other applicable laws; all generally applicable University rules and policies; and all applicable contracts and licenses. Such laws, rules, policies, and licenses include, for example, the laws of libel, privacy, copyright, trademark, harassment, discrimination, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking," "cracking," and similar activities; the University's Code of Student Rights and Responsibilities; the University's Anti-Harassment and Sexual Harassment Policies; and all applicable software licenses. Users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

Examples of usage which would violate these restrictions include:

- Obtaining unauthorized access to computers or network resources or using improperly obtained computer accounts, access codes, or network identification numbers;
- Intentionally destroying or damaging facilities, equipment, software or data belonging to the University or other users;
- Intentionally disrupting or unauthorized monitoring of electronic communications;
- Committing fraud or engaging in forgery; or
- Unauthorized copying of copyrighted material. Computer software protected by copyright is not to be copied from, into, or by using campus computing facilities except as permitted by law or by the copyright contract. This means that such computer software may be copied only in order to make backup copies if permitted by the copyright owner. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users in a department, University or the University exceeds the number of original copies purchased by the department, or University.

Computing resources should be used in accordance with the standards of the University community. Examples of this misuse follow, some of which would also violate the restrictions contained in the preceding paragraph:

- Violations of computer system security. This includes all software, files, passwords and accounts;
- Intentional use of computer networking facilities in ways that necessarily impede the computing activities of others (randomly initiating interactive electronic communications or E-mail exchanges, overuse of interactive network utilities, initiating or perpetuating chain letters and so forth);
- Use of computing facilities for commercial or personal advertisements, solicitations, promotions, political material or other purposes unrelated to the mission of the University or University life.
- Academic dishonesty (plagiarism, cheating);
- Disruptive conduct within lab facilities;
- Violation of campus or Internet network or host usage policies and regulations;
- Violation of another user's privacy. A user must obtain written permission from the owner of a file to alter or copy a file. The ability to read, alter or copy a file does not imply permission to read, alter or copy that file;
- Waste of computing facilities and resources;
- Failing to honor departmental or unit laboratory and system procedures, policies, and/or protocol;
- Allowing access to computing resources by unauthorized users;
- Unauthorized use of passwords, documents or technology;
- Intentionally introducing viruses;
- Illegal duplication of software or its related documentation;
- Plagiarism and copyright infringement;
- Creating or sustaining files to run a personal business at the University without authorization; or
- Harassment, discrimination or retaliation via technology.

Student and employee Internet pages are the responsibility of the individual maintaining them. The individual, not the University, is liable for all claims or actions resulting from a violation of any of the above Restrictions on Usage. Notwithstanding the foregoing, the University retains the right to remove or block any information that is inappropriate and/or in violation of this Acceptable Use Policy.

8.4 Harassment

No student, faculty or staff member should use computers, e-mail, voice mail, or other technology to harass, discriminate against, retaliate against, or threaten others, disrupt classes or offices, or transmit data that does not qualify as academically protected freedom of speech. When using MSMU's computer resources, individuals must comply with MSMU's rules and policies, the mission of the University, as well as all federal, California, and other applicable laws, regulations and ordinances. (Examples of forbidden transmissions include sexually-explicit messages; unwelcome propositions; ethnic or racial slurs; or any other message that

can be construed to be harassment or disparagement of others based on any characteristic protected by federal, state, or local law, ordinance or regulation.)

8.5 Procedures Regarding Violations

- Student violations will be reported to Student Affairs.
- Staff violations will be reported to Human Resources.
- Faculty violations will be reported to the Provost.

If necessary, the Provost may direct the case to the Academic Freedom Committee or a Sexual Harassment Grievance Officer for further review. The Academic Freedom Committee will review claims regarding constitutionally protected freedom of speech. The case will be closed if it is protected by freedom of speech. Any violations involving unlawful harassment, discrimination or retaliation will be referred to one of the Grievance Officers (see MSMU Sexual Harassment Policy for policy and procedures). In both cases, any decisions or further action on the case will be reported back to the Provost. The Provost will then determine if further action is required.

Users who violate the policy may face restriction of technology access or more severe sanctions, if circumstances warrant.

8.6 Facilitative Usage

Computing resource users can facilitate computing in the MSMU environment in many ways. Collegiality demands the practice of facilitative computing. It includes:

- Regular deletion of unneeded files from one's accounts on central machines.
- Refraining from overuse of connect time, log in sessions, information storage space, CPU cycles, software licenses or printing facilities.
- Refraining from overuse of interactive network utilities (such as high bandwidth audio or video applications).

8.7 Reporting Violations

Violations of this policy should be reported immediately to the systems administrator or department chair of a departmental system, or the Office of Information Technology. The University will make every effort to maintain confidentiality to the extent consistent with legal, ethical and other policy obligations. It must be remembered that in the event that the University has reason to believe that the user is using University resources in an illegal manner, or in some way inconsistent with the institution's purposes or mission, the user has no right to confidentiality and such information may be subject to sanctions as described in the section (“10. Sanctions”).

9. Social Media

9.1 Blogs, Forums, Facebook, Twitter and Wikis.

The same principles and guidelines that apply to student, faculty, or staff member activities in general, as codified in the MSMU policies and guidelines, also apply to their activities online. This includes forms of online publishing and discussion, such as Web logs, or blogs, Discussion Forums, School Sponsored Facebook and Twitter pages, and Wikis. Any online tool that individuals use to share their insights, express their opinions and communicate within the context of a globally distributed conversation have proper and improper uses. While MSMU encourages all of its student, faculty, and staff members to join a global conversation, it is important for those who choose to do so to understand what is recommended, expected and required when they

discuss ideas or persons related to or affiliated with MSMU. All student, faculty, and staff members who choose to participate should abide by the following rules or face possible disciplinary proceedings:

- Abide by MSMU's other policies and guidelines. Postings should not contain anything contrary to MSMU's rules and policies, or the mission of the University.
- Be respectful of others. Do not post anything that may be seen as insulting, defamatory, obscene, harassing, discriminatory, disruptive, or offensive to other persons, or which would infringe upon the privacy rights of other persons. Ensure you do not post anything that would contribute to a hostile environment, or which would violate University policy, federal or state harassment, discrimination and retaliation laws, or laws which protect the privacy interests of all individuals.
- Respect copyright and fair use laws. For MSMU's protection as well as your own, it is critical that you show proper respect for the laws governing copyright and fair use of copyrighted material owned by others, including MSMU's own copyrights and brands. You should never quote more than short excerpts of someone else's work. And it is good general practice to link to others' work.
- Use a disclaimer. Whether you are publishing to your own page or participate in someone else's, make it clear that what you say there is representative of your views and opinions and not necessarily the views and opinions of MSMU, its students, faculty or staff. At a minimum, you should include the following standard legal disclaimer language: "The postings on this site are my own and don't necessarily represent the opinions of MSMU, its students, faculty or staff."
- Use your best judgment. Remember that there are always consequences to what you write. If you're about to post something that makes you even the slightest bit uncomfortable, review the suggestions above and think about why that is. If you're still unsure, feel free to discuss your proposed post with MSMU's administration. Ultimately, however, you have sole responsibility for what you choose to post.

9.1 Video

MSMU makes use of film, photography, video and audio tape to advertise, express, and share experiences on our campuses both in the classroom and out. Students, Faculty, and Staff should be aware that if they appear, or are on camera, at an MSMU sponsored event or class, their likeness, voice, and biographical material in connection with these recordings may appear in advertisements, including but not limited to, printed brochures and publications, the MSMU Website, the MSMU Facebook page, YouTube, iTunesU, and other online outlets. Mount Saint Mary's reserves the right to exhibit or distribute such recordings using a private digital video network, or other mechanisms, in whole or in part without restrictions or limitation for any educational purpose which Mount Saint Mary's University of Los Angeles California, a public corporation, and those acting pursuant to its authority, deem appropriate, as well as to copyright the same in its name or any other name it may chose. Individuals appearing in any film, photograph, video or audio tape, can claim no payment or compensation.

All employees, agents, and members of the Board at Mount Saint Mary's University of Los Angeles California, are free of any and all claims and demands arising out of or in connection with the use of such photographs, film or tape, including but not limited to any claims for defamation or invasion of privacy, pursuant to the consent provisions of the Family Educational Rights and Privacy At, 20 U.S.C. 1232 et.seq.

10. Sanctions

Violations of the policies described above for legal and ethical use of computing resources will be dealt with seriously. Violators will be subject to the normal disciplinary procedures of the University and, in addition, the loss of computing privileges may result. Illegal acts involving MSMU computing resources may also be subject to prosecution by local, state and federal authorities.

11. Review Timeline

Recommended by: Academic Technology Committee 2/28/06
Approved by: Student Life Policy Board 5/16/2006
Approved by: Office of Information Technology 5/19/06 Approved by: Human Resources 8/7/06

Modified: 11/16/2009

Modified: 1/1/2015 Name change to Mount Saint Mary's University (MSMU)

Updated: 10/2018 by OIT Leadership Team