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, Los Angeles ("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 (for example, 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 or computing resources.
- Electronic Communications: For the purpose of this policy statement, electronic communications includes but is not limited to email, digital files, internet services, voice mail, audio and video recordings that have been sent or received by faculty, staff, students, or other authorized users of University computing resources

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 Video

MSMU makes use of film, photography, video, and audio recordings to advertise, express, and share experiences on our campuses both in and out of the classroom. 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 University 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 recording, 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 recordings, 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.

3.3 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.

3.4 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 email, and special circumstances require policies to regulate usage.

4.1 Email Attachment Policy

In an attempt to reduce problems caused by virus and malware, all inbound and outbound email is automatically scanned. The following file types are not allowed to be sent or received through the email system or stored in a University mailbox: ***.SCR *.PIF *.COM *.EXE *.CMD *.BAT.** These file types are often used in phishing attempts, are 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 email will be quarantined 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.

4.2 Email Communication Policy

Refer to OIT Policy 100-10 Email Communications.

4.3 Music/Video File Downloading Policy

Downloading and streaming music from sites authorized by the owners of the copyrighted music, whether or not such sites charge a fee, is permitted on the Mount Network. Downloading unauthorized music from pirate sites (web or FTP) or peer-to-peer systems or making unauthorized copies of music available to others (that is, uploading music) on peer-to-peer systems is not allowed and may be a violation of copyright and intellectual property laws. OIT will blacklist pirate sites and attempt to block downloads of music and video files.

5. Connecting to the Internet from Residence Halls

High-speed access to the Mount campus network is provided to students residing on campus. Each dormitory room is configured with an Ethernet connection and wireless network access. The Ethernet connection can be used to physically connect a computer or other devices to the University's Internet and email services. In order to use the Ethernet connection, a network cable is required, and a computer must be equipped with a 100/1000mb network interface card.

The main Wireless network is “MSMU Wireless,” which should be used by students for the best experience. The MSMULA Guest wireless network has limited speed and requires MSMU sponsorship. Students may sponsor their guest on campus. Guest access must be renewed after 24 hours.

Residents may not set up wireless access points in residence hall rooms. Personal routers and wireless hotspots are prohibited and will be disabled by OIT.

Gaming devices (such as Xbox, PlayStation, and Wii) should be used with wired connections only. Personal printers may be used with wired connections only. Wireless printing functions must be disabled.

Students are responsible for actions originating from their network devices, computers, printers, and University accounts. Devices found to be interfering with the Mount network will be blocked and accounts will be disabled, if necessary.

5.1 BYOD Devices

MSMU allows students to connect and use personal electronic devices for educational purposes inside the Residence Hall areas. It will be the students' responsibility to follow the rules for safe and responsible use. Students assume all risk for their electronic devices. The university will not be held responsible for lost, stolen, misplaced or damaged devices.

Students who log into the MSMU Wireless network, are accepting the terms of MSMU Acceptable Use Policy and agreeing to abide by these rules and conditions. BYOD devices are permitted to connect to the Mount network using individual student, faculty, or staff accounts only. Connecting with Group Wireless credentials is not allowed and will result in sanctions.

The following devices WILL NOT work and are not supported on the MSMU wireless network:

- Chromecast
- Grace Digital Internet Radio
- Roku
- Amazon Fire stick
- Personal wireless access points (e.g. Apple Airport Express , Google Wifisystem, Netgear, TP-Link, Ubiquiti, AirLock, smart wifiplug, EnGenius)
- Apple TV (supported over Ethernet / hard wire only)
- Element TV brands (supported over Ethernet / hard wire only)
- XBOX (supported over Ethernet / hard wire only)
- PS4 (supported over Ethernet / hard wire only).
- All other of the following types of networking devices not listed above:
    - Network Switches\Hubs\Routers\Firewalls
    - Wireless Hubs\Switches/Access Points/Routers
    - Mobile Hotspots

6. Security of Shared Resources

MSMU will assist users of its central computing resources to protect the information that is stored on those resources from accidental loss, tampering, or other unauthorized access. Security measures implemented on each central or campus resource can be requested from the system administrator. In the event of data loss or damage due to inadvertent or non-malicious actions, OIT will make a reasonable effort to restore the data. The ultimate responsibility for protecting digital information and data rests with the data owners and individual computer users.

All computer system users are to assume there is no privacy of 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 provide additional protection for 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.

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 viruses and malware.

7. Confidentiality

OIT will attempt to maintain the security, privacy, and appropriate confidentiality of all information stored on University computing resources. However, there are legitimate reasons for persons other than the account holder to access files, computers, or network traffic: including ensuring the continued integrity, security, or effective operation of University computing systems; to protect user or system data; to ensure continued effective departmental operations; to ensure appropriate use of University computing systems; or to satisfy a lawful court order. Users should not expect information stored on central computing resources to remain confidential from those who need to know for reasons of operational necessity, or in instances where the University has reason to believe the resources are being used in a way that is inconsistent with the University's institutional purposes or mission or in violation of University policies.

On the computer network, every user is assigned an individual account, which is for the exclusive use of the owner. Messages and email transmitted to other users should always identify the sender. Obscenities should not be transmitted. 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 faculty, staff, and students. However, it will do so only to prevent or correct improper use, satisfy a legal obligation, or ensure proper use of the email system.

If any computing resource user has evidence 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.

8. Censorship

Free expression of ideas is central to the academic process. MSMU computer system administrators will not remove any information from individual accounts or applications unless the appropriate system administrator discovers that:

a. The presence of the information is illegal (e.g., copyrighted material, software used in violation of a license agreement, etc.), or in violation of 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);
b. The information in some way endangers computing resources or the information of other users (e.g., a computer worm, virus, malware, or other destructive or malicious program);
c. The information is inappropriate because it is unrelated to or is inconsistent with MSMU's rules and policies, the mission of the University; or
d. 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 or applications any information that is inappropriate, as defined above. Specific guidelines for appropriate use of each MSMU application will be available on that system. Users whose information is removed will be notified by the system 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)

9. 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.

9.1 Institutional Purposes

Use of MSMU computing-related resources is for purposes related to the University's mission. All members of the community must be responsible stewards of these resources. Each user 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 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, using the University network, they will abide by the terms and conditions contained within this Acceptable Use Policy.

9.2 Security

Each computer user is responsible for the correct use of the applications and tools provided for maintaining the security and confidentiality of stored digital information. For example:

- Computer accounts, passwords and other types of authorization belong 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 their assigned account.
- The user must select an obscure account password and change it frequently.
- The user must understand the level of protection each computer system automatically provides for files and supplement it, if necessary, for sensitive information.
- The computer user must be aware of computer viruses, malware, and phishing schemes, and take steps to avoid being their victim.

9.3 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:
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:

- Unauthorized access to computers or network resources or using improperly obtained computer accounts, passwords, 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;
- 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 (cheating);
- 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 university, departmental or unit laboratory and system procedures, policies, and/or protocol;
- Intentionally introducing viruses or malware;
- Plagiarism and copyright infringement, including software or its related documentation;
- Creating or sustaining files to run a personal business at the University without authorization; or
- Harassment, discrimination, or retaliation via technology.

Department internet and intranet 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.

9.4 Harassment

No student, faculty, or staff member should use computers, email, 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.

9.5 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 Title IX Sexual Misconduct 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 Title IX Officers (see MSMU Zero Tolerance Policy and Title IX Compliance 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 this policy may face restriction of technology access or more severe sanctions, if circumstances warrant.

9.6 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. 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”.

10. Social Media

The same principles and guidelines that apply to student, faculty, or staff member activities in general, also apply to online activities. This includes online publishing and discussion activities, such as blogs, discussion forums, and University-sponsored Social Media pages (including Facebook, Instagram, and Twitter). 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 to understand what is recommended, expected, and required when discussing 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. 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 individual’s, it is critical to show proper respect for the laws governing copyright and fair use of copyrighted material owned by others, including MSMU’s own copyrights and brands. Never quote more than short excerpts of someone else's work without permission. Remember to give credit and provide links to others' work.

- Use a disclaimer. Whether publishing to personal pages or participating 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, 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."

11. 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. In addition, devices may be blacklisted, accounts disabled, and privileges to the network or wireless may be removed. Illegal acts involving MSMU computing resources may also be subject to prosecution by local, state, and federal authorities.

12. 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

Updated: 6/2019 by OIT Leadership Team