Acceptable Use Policy

This policy is designed to guide students, faculty, staff, and administrators in the acceptable use of computer systems and networks provided by Mount St. Mary's University. More importantly, it is meant as an application of the principles of respect and reverence for every person that are essential to Mount St. Mary's Catholic identity.

Guiding Principles

The Mount St. Mary's University community is encouraged to make innovative and creative use of information technologies in support of multiple learning experiences. Access to information representing a variety of views on current and historical issues should be allowed for the interest, information and enlightenment of the Mount St. Mary's University community. Consistent with other University policies, this policy is intended to respect the rights and obligations of academic freedom. The University recognizes that the purpose of copyright is to protect the rights of the creators of intellectual property and to prevent the unauthorized use or sale of works available in the private sector. Also consistent with other University policies, an individual's right of access to computer materials should not be denied or in any way limited because of race, creed, color, age, national origin, gender or disability.

Mount St. Mary's University computing and network resources are to be used only for University-related research, instruction, learning, enrichment, dissemination of scholarly information, and administrative activities. The computing and network facilities of the University are limited and should be used wisely and carefully with consideration for the needs of others. Computers and network systems offer powerful tools for communications among members of the community and of communities outside the University. When used appropriately, these tools can enhance dialog and communications. When used unlawfully or inappropriately, however, these tools can infringe on the work, rights or beliefs of others.

Responsibilities

The following are some examples of the responsibilities that accompany computer use at Mount St. Mary's and/or on networks to which Mount St. Mary's is connected.

1. Users are responsible for all use of their computer account(s). They should make appropriate use of the system and network-provided protection features and take precautions against others obtaining access to their computer resources.

2. Users may use only their own computer accounts. Users may not supply false or misleading information nor improperly obtain another's password in order to gain access to computers or network systems or data. The negligence or naiveté of another user in revealing an account name or password is not considered authorized use.

3. Users may not attempt to modify the University system or network facilities or attempt to crash systems. They should not tamper with any software protections or restrictions placed on computer applications or files. Users may not intercept network traffic without authorization.

4. Users may not encroach on others' use of computer resources. Such activities would include, but are not limited to, tying up computer resources for excessive game playing or other trivial applications; sending harassing messages; sending frivolous or excessive messages, including chain letters, junk mail, and other types of broadcast messages, either locally or over the Internet; using excessive amounts of storage; intentionally introducing any computer viruses; physically damaging systems; or running grossly inefficient programs when efficient ones are available.

5. The computer resources of Mount St. Mary's University may not be used to display or propagate materials (words or images) that are obscene, pornographic, fraudulent, abusive, racist, bigoted, or otherwise inappropriate to the mission of Mount St. Mary's University.

6. Users must remember that information distributed through the University's computing and networking facilities is a form of publishing, and some of the same standards apply. For example, anything generated at MSMU that is available on the Internet may be seen as representing MSMU and not just an individual. Even with disclaimers, the University is represented by its students, faculty and staff, and appropriate language, behavior and style is warranted. If an individual misuses computer resources, then the appropriate procedures that exist in University student, faculty, and staff policy handbooks will apply. Penalties may include the loss of all computer use privileges.

7. **Users are prohibited from installing or using network devices that are not owned by MSMU. This includes personal wireless access points, servers, hubs, switches, or any other networking equipment.**

Disclaimer

The University cannot protect individuals against the existence or receipt of text or images that may be offensive to them. As such, those who make use of electronic communications are warned that they may come across or be recipients of material they find offensive. Those who make information about themselves available on the Internet (through e-mail or some other means) should be forewarned that the University cannot protect them from invasions of privacy and other possible dangers that could result from the individual's distribution of personal information. Finally, while the University provides computer resources in its buildings and on its campuses this should not be interpreted as the University sanctioning the materials developed or propagated by the individuals using those resources.

General Security Principles

Users are expected to be aware of the security policies of the computers and networks which they access and to adhere to these policies. Users are individually accountable for their own actions and for all use of the resources assigned to them. The sharing of accounts, passwords, and other assigned resources is unauthorized.

A weakness in the security of any particular system or network is not a license to penetrate or abuse that system or network. The exploitation of software weaknesses to assume a false identity is not allowed. The unauthorized use of a computer or network is a violation of both our own campus computing policies and also Internet rules of conduct.

Users have the responsibility to employ the security mechanisms and procedures which have been made available to them in order to protect their own data as well as the systems and network they use. For systems which rely on password protection this means selecting good passwords, not sharing passwords, and changing passwords immediately upon suspicion that they have been compromised.

Password Security Guidelines

Do not set your password equal to your Username or any variation of your Username. Do not use a password consisting of all the same letter. Avoid passwords that would be easy to guess. Do not use your initials or first, middle, or last name or the name of any family member. Do not use as a password any information easily obtained about yourself such as license number, telephone number, address, social security number, etc.

Do not write your password down; memorize it instead. Never store your password in a file or document on the computer or send it in a Mail message.

Do not tell anyone your password and do not let other people use your account.

Copyrights, Licenses, and Content

The unauthorized copying of software which is licensed or protected by copyright is unethical and illegal. We do not condone unauthorized copying of software, or other any other copyrighted media. This would also include music and video files. Failure to observe copyrights or license agreements may result in disciplinary action or legal action by the copyright holder.

Respect for the intellectual work and property of others have traditionally been essential to the mission of colleges and universities. Plagiarism is not tolerated.

All institutional policies, including those concerning intellectual honesty, theft, and civility, are applicable to the use of the Internet.

Individuals are subject to sanction if they violate institutional policy, as well as to legal punishment if they violate the law.

Noncommercial Use

Computing facilities are intended to be used for academic and research purposes and to support the educational mission of the university. Computing facilities should not be used for unauthorized commercial purposes.

Many of the networks to which we are connected have Acceptable Use Policies. You should become acquainted with and adhere to the current Acceptable Use Policies of any network or remote system which you use.

Mount St. Mary's University is committed to providing computing resources to support the academic research, instructional, and administrative objectives for the students, faculty, staff, and administrative members of the University.

University Access and Disclosure

1. General Provisions

    a. To the extent permitted by law, the University reserves the right to access and disclose the contents of faculty, staff, students', and other users' electronic mail without the consent of the user. The University will do so when it believes it has a legitimate business need including, but not limited to, those listed in paragraph 3 (below), and only after explicit authorization is obtained from the appropriate University authority.

    b. Faculty, staff, and other non-student users are advised that the University's electronic mail systems should be treated like a shared filing system, i.e., with the expectation that communications sent or received on University business or with the use of University resources may be made available for review by any authorized University official for purposes related to University business.

    c. Electronic mail of students may constitute "education records" subject to the provisions of the federal statute known as the Family Educational Rights and Privacy Act of 1974 (FERPA). The University may access, inspect, and disclose such records under conditions that are set forth in the statute.

2. Monitoring of Communications

   The University will not monitor electronic mail as a routine matter but it may do so to the extent permitted by law as the University deems necessary for purposes of maintaining the integrity and effective operation of the University's electronic mail systems.

3. Inspection and Disclosure of Communications

   The University reserves the right to inspect and disclose the contents of electronic mail:

   - in the course of an investigation triggered by indications of misconduct or misuse,
   - as needed to protect health and safety,
   - as needed to prevent interference with the academic mission, or
   - as needed to locate substantive information required for University business that is not more readily available by some other means.

   The University will inspect and disclose the contents of electronic mail when such action is necessary to respond to legal processes and to fulfill the University's obligations to third parties.

4. Limitations on Disclosure and Use of Information Obtained by Means of Access or Monitoring

   The contents of electronic mail communications, properly obtained for University purposes, may be disclosed without permission of the user. The University will attempt to refrain from disclosure of particular communications if disclosure appears likely to create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

5. Special Procedures to Approve Access to, Disclosure of, or Use of Electronic Mail Communications

   Individuals needing to access the electronic mail communications of others, to use information gained from such access, and/or to disclose information from such access and who do not have the prior consent of the user must obtain approval in advance of such activity from the President or Executive Vice President.

   The Chief Information Officer will manage the electronic discovery and share the results only with those authorized.

6. Disciplinary Action

   Appropriate disciplinary action will be taken against individuals found to have engaged in prohibited use of the University's electronic mail resources or violated the privacy of the communications.