

# Mount Mercy Acceptable Use Policy

## Acceptable Use Policy

Mount Mercy University encourages computer use as a tool to further its teaching, scholarly research, and service goals. Mount Mercy University provides faculty, students, and staff with equipment and facilities that provide access to campus and global information resources. Computing resources are to be used in an ethical, courteous and fair manner.

Use of Mount Mercy University computing facilities is restricted to current faculty, staff, students, and other employees. With permission of lab supervisors, alumni and non-University individuals may be permitted to Use Mount Mercy University technology resources. This latter access will be granted on a case by case basis.

The purpose of this policy is to extend these expectations to include acceptable uses of information technology resources. Furthermore, the policy extends these expectations to cover circumstances in which the interests and rights of others must be protected and preserved. These guidelines apply to all Mount Mercy faculty, staff, and students using Mount Mercy University information technology resources. These policies also extend to alumni and non-University individuals and entities that access information through Mount Mercy University technology resources.

Information technology resources are those facilities, technologies, and information resources required to accomplish information processing, storage, and communication, whether individually controlled or shared, stand alone or networked. Included in this definition are the Busse Computer Center, departmental/building technology centers, classroom technologies, equipment, personal computers used on campus owned by students, staff, and faculty, and computing and electronic communication devices and services.

Specialized computer labs within the University community may define conditions of use for facilities under their control. These statements must be consistent with this overall policy, but may provide additional detail, guidelines, and/or restrictions. In addition, any network traffic exiting the University is subject to the acceptable use policies of the University's national and international network connectivity providers.

Student violation of these policies constitutes computer abuse and disciplinary actions will be governed as outlines in *The Good Book*. Computer abuse by faculty and employees of Mount Mercy University will be handled by appropriate administrative channels. The campus computer director's role in the process will be to call attention to the situation, gather and validate pertinent information and forward the information to the appropriate dean, vice-president or supervisor. Violations of courtesy are to be referred to the Director of Campus Computing or supervisor of the individual lab or electronic device.

## E-Mail Acceptable Use Policy

Persons using electronic mail with Mount Mercy University information technology resources are expected to treat the contents of electronic files as private and confidential. Inspection of electronic files and electronic mail, and any action based upon such inspection, will be governed by all applicable United States and Iowa laws. The University community is advised that all files stored on main systems, including electronic mail, are backed-up regularly and may be subject to subpoena.

Mount Mercy University cannot monitor and does not control the information available through the Internet. Parents or guardians are responsible for monitoring the materials accessed by minors.

Information technology resources may be used for the following purposes:

- Class assignments
- Campus community and public service projects
- Campus publications and announcements
- Academic research and investigation
- Computing for personal and professional advancement

Administrative and instructional support  
Staff and faculty consulting, subject to University policies

Computer users must not engage in unauthorized or inappropriate conduct on the University network, e-mail, or Internet. Examples of such activities include, but are not limited to:

Using or sharing another person's login ID to access computing facilities at Mount Mercy or another Internet facility. This includes permitting others to use one's own login ID.  
Unauthorized tampering with or modification of network resources.  
Using any means to crack or access systems, whether on campus or off, in an unauthorized or inappropriate manner.  
Using Mount Mercy technology or facilities to engage in illegal or criminal activities.  
Using Mount Mercy technology or facilities to threaten or harass another person.  
Attempting to read or access another person's electronic mail or protected files  
Copying or distributing software in a manner which violates copyright laws, license agreements, and intellectual property as outlined in the *Copyright Law of the United States of America*, revised March 1, 1989, in Title 17 of the United States Code, Section 117.  
Knowingly distributing or actively developing a computer virus, worm, or Trojan Horse.  
Repeated use of Mount Mercy technology or facilities in a discourteous manner.

### **Information regarding Mount Mercy University network accounts and email accounts:**

Access to the Mount Mercy University network will be granted with the direct supervisor or VP approval. All employees of the University are required to have a network account and a campus email account.

Access to the Mount Mercy University network and email is also governed by the Acceptable Use Policy with the same restrictions and punishments applicable if misused.

***No one should give out their user name and password.*** Each user is assigned an account and will be held accountable for the activity on that account. Do not share your user name and/or password.

If another user requires access to your PC and/or account, they need to contact the Campus Computing Department at 319-363-8213 extension 4357. With proper justification, Campus Computing will determine if access is needed and will reset the user password to gain access to an account. Campus Computing does not know any user passwords so the password will need to be reset if it is determined access permissions are necessary.

You are using a university PC and accessing the university's network and email. Allowing others to access your email account or network information is in violation of the Acceptable Use Policy.

Please contact Campus Computing with any questions or concerns.