Background:

As an institution of higher learning, the University both uses information technology and supplies it to the members of the university community. This policy sets forth the general rights and responsibilities common to all uses of information technology, from the simple stand-alone PC to the complex systems that create virtual classrooms, workplaces and recreational facilities in the University.

The primary guiding principle is that the rules are the same for information technology as for other aspects of university life. The rights and responsibilities governing the behavior of members of the University community are the same on both the virtual and physical campuses, and the same disciplinary procedures will be followed when the rules are violated. There is nothing special about the virtual campus that makes it distinctly different.

The University has a strong commitment to the principles of free speech, open access to knowledge, and respect for a diversity of opinions. The rights as well as the restrictions governing these principles on the physical campus apply fully to the virtual campus.

Policy:

Resource Limits

Information technology resources are often limited; what is used by one person is no longer available to others. Many systems have specific limits on several kinds of resources, such as storage space or connect time. All users must comply with these limits and not attempt to circumvent them. Moreover, users are expected not to be wasteful of resources whether or not there are specific limits placed on them. Unreasonable use of resources may be curtailed.

Privacy

Members of the University community shall not attempt to access the private files of others. The ability to access a file does not, by itself, constitute authorization to do so. The University does not routinely monitor or inspect individual accounts, files, or communications. There are situations, however, in which the University has a legitimate need to do so: (1) system managers may access user accounts, files, or communications when there is reason to believe that the user is interfering with the performance of a system; (2) authorized investigators may access accounts, files, or communications to obtain relevant information when
there is a reasonable suspicion that the user has violated either laws or University policies; (3) co-workers and supervisors may need to access accounts, files, or communications used for university business when an employee becomes unavailable; and (4) when required by law. All monitoring and inspection shall be subject to authorization, notification and other requirements specified in the IT Management Policy.

Though the University will attempt to prevent unauthorized access to private files, it cannot make any guarantees. Because the University is a public entity, information in an electronic form may be subject to disclosure under the Ohio Public Records Act just as paper records are. Information also can be revealed by malfunctions of computer systems, by malicious actions of hackers, and by deliberate publication by individuals with legitimate access to the information. Users are urged to use caution in the storage of any sensitive information.

Access

Some portions of the virtual campus, such as public web pages, are open to everyone. Other portions are restricted in access to specific groups of people. No one is permitted to enter restricted areas without authorization or to allow others to access areas for which they are not authorized. The ability to access a restricted area does not, by itself, constitute authorization to do so.

Individual accounts are for the use of the individual only; no one may share individual accounts with anyone else, including members of the account holder’s family. Joint access to resources when needed, should be provided from separate accounts.

Security

All members of the University community must assist in maintaining the security of information technology resources. This includes physical security, protecting information and preventing and detecting security breaches. Passwords are the keys to the virtual campus and all users are responsible for the security of their passwords. Users must report all attempts to breach the security of computer systems or networks to an appropriate official.

Plagiarism and Copyright

Intellectual honesty is of vital importance in an academic community. You must not represent the work of others as your own. You must respect the intellectual rights of others and not violate their copyright or trademark rights. It is especially important that you obey the restrictions on using software or library resources for which the University has obtained restricted licenses to make them available to members of the University community.

Enforcement:

Anyone who becomes aware of a possible violation of this policy or the more specific regulations of the systems that comprise the virtual campus should notify the relevant department head or system administrator. The administrator will investigate the incident and determine
whether further action is warranted. The administrator may resolve minor issues by obtaining the agreement that the inappropriate action will not be repeated. In those cases that warrant disciplinary action, the system administrator will refer the matter to the appropriate authorities. These include Public Safety for violations of criminal law, the Office of Student Affairs for violations by students, the appropriate Provost for violations by faculty, and the Office of Human Resources for violations by staff members. System administrators can act to block access and disable accounts when necessary to protect the data system or prevent prohibited activities, but such actions cannot be used as punishments. Users must be notified promptly of the action and the restrictions must be removed unless the case is referred for disciplinary action.

Approved by the UC President’s Cabinet, September 2000

Audience:

This policy applies to all members of the University community, including guests who have been given accounts on the University’s information technology systems for specific purposes. It also applies whether access is from the physical campus or from remote locations. In addition, there may be specific policies issued for individual systems, departments, colleges and the like. While these policies must be consistent with this general policy, they provide more detailed guidance about what is allowed and what is prohibited on each system. All members of the University community are responsible for familiarizing themselves with any applicable policy prior to use.

Definitions:

Procedure:

Information Technology Management Procedure Document

Related links:

Applicable Laws and Regulations - All members of the University community must obey:

- all relevant federal, state, and local laws. These include laws of general application such as libel, copyright, trademark, privacy, obscenity and child pornography laws as well as laws that are specific to computers and communication systems, such as the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act.
- all relevant University rules and regulations. These include the Rules of the University, the Student Code of Conduct, the various collective bargaining agreements between the University and its employees, and all other University policies including the policy against sexual and racial harassment.
- all contracts and licenses applicable to the resources made available to users of information technology.
- this policy as well as other policies issued for specific systems.
Contact Information:

IT@UC Office of Information Security  513-558-ISEC (4732)
Email: infosec@uc.edu
UC Office of the CIO  513-556-2228

History:

Issued: 09/01/2000
Revised: 06/20/2014