


HAWK, JAN W
CONTROLLER
0553

ADMINISTRATIVE MEMORANDUM NO. 125

TO: All Administrative Unit Heads
FROM: Frederick H. Siff 
RE: General Policy on the Use of Information Technology

Attached is the final version of the University's General Policy on the use of Information Technology, which will take effect on September 5, 2000. During the month of September, UC data services clients will be required to read and acknowledge this policy.

An appointed University Task Force, managing a public comment period and dealing with community comments and concerns, designed this policy. The President and his Cabinet have approved the final version.

Attachment

The University of Cincinnati General Policy on the Use of Information Technology

Final Version, May 2000

Introduction

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.

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.

Guiding Principles

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.

Specific Areas

1) 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.

2) 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.

3) 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 (forthcoming).

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.

4) 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.

5) 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.

6) 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.

7) 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 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.

Additional Explanations

General Policy on the Use of Information Technology

These explanations are intended to help people, particularly students, understand the General Policy. They describe in a general way what is covered by the legal terms, and are certainly not intended to be adequate guides to the law.

Copyright

Scholarly, literary, artistic, musical, dramatic and other types of intellectual property embodied in a tangible medium are protected by law from unauthorized use, publication, sale or reproduction. Work is protected even if it is not marked with a copyright notice. There are complex rules about what and how much can be copied.

Federal and State Laws

Federal and state laws make it illegal to hack into computer systems, disrupt or intercept communications, distribute computer viruses, commit fraud using a computer, or to use a computer to abuse, threaten, or harass another person. The two major federal laws are the Electronic Communications Privacy Act (ECPA), 18 USC §2510 et seq. and the Computer Fraud and Abuse Act, 18 USC §1030. Major Ohio state laws are ORC §2913.04 ("Unauthorized use of computer or telecommunication property") and ORC §2917.21 ("Telecommunication harassment").

Joint Access

An examples of a situation requiring joint (or shared) access is a departmental or program email addresses for inquires or applications from prospective students. More than one person may need to read and respond to these email messages. Most current systems allow accounts to be set up so that multiple people can access the email messages from their own accounts rather than by logging in to the common account. Unless this is impossible, users should not access common accounts directly.

Libel

Publication of false information that is injurious to the reputation of another is called libel and can be the basis of a lawsuit for damages. Internet communications (web pages and postings to newsgroups or mailing lists) are considered publications.

Obscenity, Pornography, and Child Pornography

Pornographic materials are those which appeal to prurient interests. When they go beyond the community standards, they may be classified as "obscene" and become illegal. The community standards that would be applied are not those of the University of Cincinnati or the Internet, but rather those of Hamilton County and perhaps other communities as well. There are separate laws covering pornography that portrays minors. The potential penalties are more severe and mere possession of child pornography is illegal.

Ohio Public Records Act

The Ohio Revised Code, §149.03, provides that public records are to be made available to the public upon request. Most general University records are considered to be public records. Student Education records are a major exception.

Privacy

The major privacy law affecting educational institutions is the Family Educational Rights and Privacy Act (FERPA). This law prohibits the University from disclosing more than directory information about students.

Student Code of Conduct

The Student Code of Conduct defines behavior expected of all University of Cincinnati students and the disciplinary procedures used in cases of misconduct. It can be found on the Web at <http://www.uc.edu/conduct.html>.

Trademarks

Trademarks and logos may not be used without the permission of the owner. This includes the use of the UC logos. For questions or information about the use of UC logos, contact the Licensing Program in the Office of General Counsel, telephone 513-556-3483.

The Virtual Campus

The term "virtual" refers to the metaphorical spaces created by computer networks. The University of Cincinnati now has a virtual campus that parallels the physical campuses in many ways. Students take courses that meet on the virtual campus instead of in regular classrooms. They study in the virtual library with electronic resources instead of reading books and journals printed on paper. There are also social and recreational activities on the virtual campus like those provided in student centers and athletic facilities. Most of the University offices now have counterparts on the virtual campus.

Acceptable use policies for computer systems are often intended to protect equipment. This policy uses the virtual campus metaphor deliberately to emphasize that the goal is not only to protect equipment, but also to insure that we treat each other according to established rules and customs governing behavior in our electronically mediated encounters. It is vitally important that the virtual campus be a safe and friendly place that facilitates the achievement of all members of the University community.
