Cleveland State University

General Policy for University Information and Technology Resources

08/13/2007

Introduction

As an institution of higher learning, Cleveland State University both uses information and technology resources and provides these resources to the members of the university community. This policy sets forth the general rights and responsibilities common to all uses of information and technology resources, from the simple stand-alone PC to the University's complex systems.

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.

Guiding Principles

The primary guiding principle is that the rules are the same for the use of information and technology resources as for other university resources. The rights and responsibilities which govern the behavior of members of the University community are the same for both and the same disciplinary procedures will be followed when such rules are violated.

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

1) Applicable Laws and Regulations

All members of the University community must obey:

- all federal, state, and local laws. Laws of general application include but are not limited to those laws which govern copyright, trademark, libel, privacy, discrimination, obscenity and child pornography as well as laws that are specific include but are not limited to the Family Education Rights and Privacy Act (FERPA), the Health Insurance Portability Protection Act (HIPPA), the Computer Fraud and Abuse Act, the Digital Millennium Copyright Act (DMCA) and the Electronic Communications Privacy Act.
- all relevant University rules, regulations, policies and procedures. These include but are not limited to all University policies, the Student Code of Conduct, and the various collective bargaining agreements between the University and its employees.
- all contracts and licenses applicable to the resources made available to users of information technology. (Please refer to the University Computer Hardware Policy)
- this policy as well as other policies and procedures issued for specific systems.

2) Resource Limits

The University's information technology resources are limited. 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

The University does not routinely monitor or inspect individual computers, accounts, files, or communications. There are situations, however, in which the University needs to do so:

- when required to comply with the law;
- when ordered to do so by a court;
- when ordered to do so pursuant to a subpoena or other legally enforceable order;
- when the email or computer file is a "public record" as described defined in ORC §149.43 to which the public has access under ORC §149.43, and a member of the public has sought to inspect or to get a copy of the particular message or file to be accessed and a proper request is made;
- when the University has reasonable cause to believe that a “litigation hold ” is necessary based upon knowledge by University Legal Counsel of the presentment of a claim or of a potential cause of action which has an impact on the University;
- when in the normal operation and maintenance of the University's computer facilities, staff of the Information Services and Technology department (or their staff analogues in other units of the University) inadvertently open or otherwise briefly access an electronic mail message or computer file;
- when emergency entry is necessary to preserve the integrity of the University’s computer and network facilities or to preserve public health and safety;
- when co-workers and/or supervisors need to access accounts used for university business when an employee becomes unavailable; or
- when the University has reasonable cause to believe there has been a violation of the law.

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 or discovery rules 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. Users are urged to keep their personally identifiable information secure.

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. Members of the University community shall not attempt to access the private files of others. 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. If joint access to resources is required then it should be provided through separate accounts. (Please refer to the University Password Policy)

5) Security

All members of the University community must assist in maintaining the security of information and 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. They must never be shared with supervisors, co-workers or family members. Users must report all attempts to breach the security of computer systems or networks to the University's Security Administrator or the University's Action Line (888-837-1824). (Please refer to the University Administrative Data Policy and University Password Policy.)

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 property rights of others and not violate copyright or trademark. You must 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 rules and regulations of the systems that comprise the virtual campus should notify the University Security Administrator or the University's Action Line (888-837-1824). The Security Administrator will investigate the incident and determine whether further action is warranted. The Security 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 Security Administrator will refer the matter to the appropriate authorities. These include but are not limited the Cleveland State University Police Department for violations of criminal law, the Office of Judicial Affairs for violations by students, the Provost for violations by faculty, and the Office of Human Resources for violations by staff members. Any disciplinary procedures will be carried out pursuant to applicable University rules, regulations, policies and procedures and the various collective bargaining agreements between the University and its employees.

System administrators can act immediately to block access and disable accounts when necessary to protect the system or prevent prohibited activities. Users will be notified promptly of any such action and the restrictions must be removed once the prohibited activity is stopped unless the case is referred for disciplinary actions.

8) Unacceptable Use

The following activities are, in general, prohibited. Students, faculty or staff may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of Cleveland State University authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing University-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Cleveland State University or the end user.
- Unauthorized copying and downloading of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music and films, and the installation of any copyrighted software for which Cleveland State University or the end user does not have an active license is strictly prohibited.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your administrative system account(s) by others. This includes family, other household members, friends, co-workers or supervisors.
- Using a University computing asset to procure, solicit, or transmit material that is in violation of sexual harassment or hostile workplace laws.
- Making fraudulent offers of products, items, or services originating from any Cleveland State University account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these activities are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless it is done by the network or computer manager of a department, college or the University.
- Executing any form of network monitoring which will intercept email or file data not intended for the monitor's computer.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Sending "junk mail" or advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information, or packet information.
- Broadcasting of unsolicited mail or messages. Examples of such broadcasts include chain letters, mail bombs, virus hoaxes, spam mail, and other email schemes that may cause excessive network traffic or computing load. Those who anticipate sending large numbers of electronic mail messages for official University or academic purposes are responsible for following the University’s procedures for the electronic distribution of information.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

9) Related Policies

In addition to this general policy, the University has other policies which address specific topics. These policies include but may not be limited to:

- University Administrative Data Policy
- University Password Policy
- University Policy for Network and Application Access
- University Policy on Software and Hardware
- University Telephone Policy

While these policies must be consistent with this general policy, they provide more detailed guidance about what is allowed and what is prohibited. All members of the University community are responsible for familiarizing themselves with any applicable policy prior to use.

10) Updates to this Policy

As changes to the way CSU operates require changes to this policy, additions, deletions and modifications to this policy will be reviewed and approved by Senior Staff before the changes become permanent.