Cleveland State University

Cleveland State University

General Policy for University Information and Technology Resources

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 Univer

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

- Violations of the rights of any person or company protected by copyright, trade secret, patent

- University Administrative Data Policy