Information Services Ethics Policy

CWRU Information Services Ethics Policy

June 1996

General Principles

Access

Access to computers, network facilities, information services and resources owned and operated by Case Western Reserve University imposes certain responsibilities and obligations and is granted subject to University policies, and local, state, and federal statutes. Access to the University's computers, network facilities, information services and resources is granted solely to Case Western Reserve University faculty, staff, registered students, and individuals outside the University who are authorized to use services that have been made available through Case Western Reserve University. The University reserves the right to limit, restrict, or extend access privileges to its computers, network facilities, information services and resources.

Acceptable Use

The University's computers, network facilities, information services can provide access to resources both on and off campus. Such open access is a privilege and requires that individual users act in a responsible and acceptable manner. Acceptable use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. Acceptable use demonstrates respect for intellectual property, truth in communication, ownership of data, system security mechanisms, and individuals' right to privacy and freedom from intimidation, harassment, and unwanted annoyance. The University considers any violation of acceptable use principles or guidelines to be a serious offense and reserves the right to test and monitor security, and copy and examine any files or information resident on University systems allegedly related to unacceptable use.

Disciplinary Action

Those who do not abide by the policies and guidelines listed below should expect at least suspension of CWRUnet network privileges and possible disciplinary action in accordance with University rules for misconduct and existing judicial, disciplinary, or personnel processes. Offenders may also be subject to criminal prosecution under federal or state laws, and should expect the University to pursue such action.

Notification of Possible Misconduct

CWRUnet Services should be notified about violations of Information Services Ethics Policy, laws, as well as potential loopholes in the security of the University's computers, network facilities, information services and resources. The user community is expected to cooperate with CWRUnet Services in its operation of the University's computers, network facilities, information services and resources as well as in the investigation of misuse or abuse.

Guidelines

Standards of Conduct

The general standards of conduct expected of members of the Case Western Reserve University community also apply to the use of the University computers, network facilities, information services and resources. These facilities and resources include:

- wiring or infrastructure used for communications;
- electronics, digital switches and communication equipment used for processing or communications;
- programs, programming languages, instructions, or routines which are used to perform work on a computer;
- digital information such as records, images, sounds, video or textual material stored on or accessible through a computer;
- computers used for automation or the administration of information services;
- information such as CWRUnet IDs, authorization codes, account numbers, usage and billing records, or textual material stored on or accessible through the network or other communication lines.

Property Rights

University computers, network facilities, information services and resources are made available to individuals to assist in the pursuit of educational goals. In order to promote the most effective use of these, it is expected that users will cooperate with each other and respect the privacy of information even though it may be in electronic form rather than printed form. Individuals and organizations will be held no less accountable for their actions in situations involving University computers, network facilities, information services and resources than they would be in dealing with other media.

Though some of them are intangible, these University computers, network facilities, information services and resources are the property of the University. Rules prohibiting theft or vandalism apply to authorization codes, long distance

telephone services, television signals and service information as well as to physical equipment.

Conduct which violates the University's property rights with respect to University computers, network facilities, information services and resources is subject to University disciplinary action. This conduct includes:

- using University computers, network facilities, information services and resources for purposes other than those intended by the University body granting access to those resources (especially using them for personal financial gain or allowing access to them by unauthorized persons even if they are members of the University community);
- using any portion of University computers, network facilities, information services and resources for the purpose of:
  - copying University-owned or licensed information to another computer system for personal or external use without prior written approval;
  - attempting to modify University-owned or licensed information (including software and data) without prior approval;
  - attempting to damage or disrupt the operation of computer equipment, communications equipment, or communications lines;
- knowingly accepting or using University owned or licensed information (including software and data) which has been obtained by illegal means;
- from a single CWRUnet faceplate, receiving more than one set of television signals or distributing these signals to multiple receivers;
- knowingly accepting or using television signals which has been obtained by illegal means.

Confidentiality

The University seeks to protect the civil, personal, and property rights of those actually using its computers, network facilities, information services and resources and seeks to protect the confidentiality of University records stored on its computer systems. The University also seeks similarly to protect those computers, network facilities, information services and resources of other institutions to whom University personnel have access via the University computers, network facilities, information services and resources. Conduct which involves the use of University computers, network facilities, information services and resources to violate another's rights is subject to University disciplinary action. This conduct includes:

- invading the privacy of an individual by using electronic means to ascertain confidential information, even if an individual or department inadvertently allows access to information;

- copying another user's information without the permission of the owner, even if it is readily accessible by electronic means;
- knowingly accepting or using information which has been obtained by illegal means;
- abusing or harassing another user using the University computers, network facilities, information services and resources.

Accessibility/Use

Some of the University computers, network facilities, information services and resources require that each user have a unique identity (i.e. CWRUnet ID, telephone long distance authorization code). The identity is used to represent a user in various University computers, network facilities, information services and resources activities; to provide access to certain University computers, network facilities, information services and resources based on his/her credibility and purpose for requiring such access; and to associate his/her own service use and information with his/her identity. As such, this identity is another instrument of identification and its misuse constitutes forgery or misrepresentation.

Conduct which involves inappropriate access or misuse of University computers, network facilities, information services or resources and service identities is subject to University disciplinary action. This conduct includes:

- allowing another individual to use ones unique identity;
- using another individual's identity, even if the individual has neglected to safeguard it.
- using the University computers, network facilities, information services or resources in the commission of a crime;
- gaining access to non-public computers, network facilities, information services and resources.

Case Western Reserve University's computers, network facilities, information services and resources are networked on the CWRU campus and to other locations. Information on the University's networks and communication lines is considered to be private. Tapping the University's network or communication lines for the purpose of examining or using information other than that destined for the intended user is considered unacceptable conduct and is subject to disciplinary action.

State and National Laws

Conduct in violation of the principles set forth above, with respect to the use of University information services and facilities may be subject to criminal or civil legal action in addition to University disciplinary action.

http://cnswww.cns.cwru.edu/phone/phonebook/IS-Ethics96.html