John Carroll UNIVERSITY

Communication/Electronic Media Policy

Definition

Technological and information resources are defined to include: data; records; software; facilities; equipment; storage media; networks and network services; and electronic voice, video and multimedia communications.

Policy

University technological and information resources are provided to allow faculty, staff and students to pursue the mission of John Carroll University, and are to be used to the extent that they promote that mission either directly in teaching and research or indirectly in supporting the offices and agencies that maintain university operations. Technological and information resources are to be accessed and utilized in an ethical manner. All users of technological and information resources are expected to observe high moral, legal and professional standards, and are expected to support the mission, and act in the best interests of John Carroll University.

All users of technological and information resources are responsible for the protection of university assets and for the accuracy, integrity and confidentiality of the information to which they have access. Resources are not to be abused or employed in such a way as to interfere with, or cause harm or damage to, another person, institution or company within or outside the John Carroll University community. While the university encourages the exploration of educational and scholarly opportunities through the use of its technological resources, respect for the rights and privacy of others must be observed. University community members and their guests may not access the files or communications of others without authorization. Those who are authorized to access confidential files must respect the privacy rights of others and use data only for legitimate academic or administrative purposes.

John Carroll University supports accessibility to technological resources and strives to provide state-of-the-art, environmentally sound facilities for all members of the university community. The university acknowledges its responsibility to all faculty, staff and students to provide a safe and healthful technical environment for work and study.

All members of the university community must comply with the following policies, procedures and security controls.

Access

Many of the technological and information resources of John Carroll University may be accessed by all members of the university community, and by the public as well. However, access to some resources is restricted to specific positions or organizational units as determined by the appropriate unit head. Organizational unit heads should determine and authorize the appropriate degree of access for each member of their units, and should provide unit members with adequate orientation and training regarding the ethical use of technological and information resources.

Individuals should take precautions to prevent unauthorized use of their access codes (passwords). Active sessions should not be left unattended. Access codes may not be shared with others, and their confidentiality is to be strictly maintained. In choosing access codes, individuals should avoid the use of common words, proper names, readily associated nicknames or initials, and any other letter and/or number sequences that might easily be guessed. Individuals will be held accountable for all actions performed under their access codes, including those performed by other individuals as a result of negligence in protecting the codes. Individuals are responsible for monitoring access on their accounts and for changing access codes on a regular basis. If an individual’s access code(s) become compromised, it (they) must be changed immediately.

The following activities are strictly prohibited:

a. Attempts to access, search, or copy technological and information resources without proper authorization;
b. Use of accounts other than one’s own individual or group account(s);
c. Providing false or misleading information in order to gain access to technological and information resources;
d. Attempting to compromise internal controls, even for purposes of systems improvement; (such actions for the purpose of improvement require the advance, written approval of the authorized organizational unit head, or must be included among the security evaluation responsibilities of one’s position function).

Suspected activities such as those listed above should be promptly reported to the director of computing systems and services at the Department of Information Services so that timely preventative measures can be taken to safeguard the integrity of data or facilities.

Protecting Confidentiality

Disclosure of confidential information is prohibited, unless disclosure is a normal and authorized requirement of one’s position function. Individuals with access to confidential data must safeguard the accuracy, integrity, and confidentiality of that data by taking appropriate precautions and following appropriate procedures necessary to ensure that no unauthorized disclosure of confidential data occurs. Such precautions and procedures include the secure storage of data backups and the protection of sensitive data with access codes (passwords).

Privacy

For purposes of this policy, privacy is defined as the right of an individual or an organization to create, maintain, send and receive electronic data, software and communications files that are safe from examination and disclosure by others. John Carroll University recognizes that individuals have a substantial interest in, and reasonable expectation of, privacy. Accordingly, John Carroll University respects the privacy rights of all members of the university community.

The university will not monitor an individual’s private electronic data, software, and communications files as a routine matter. Users should note that some electronic files are copied to backups and stored for indefinite periods in specific locations. In such instances, deletion of an electronic file, such as an e-mail message, will not necessarily delete a previously archived copy of that file.

It is a violation of university policy for any member of the university community to engage in electronic “snooping,” or to employ technological resources for the purpose of “prying into” the affairs of others (i.e., to access or attempt to access electronic files without proper authorization to do so for genuine business purposes of the university).

The university reserves the right to access and to disclose the contents of an individual’s electronic data, software, and communications files, but will do so after obtaining the proper approvals, only when a legitimate need exists and the urgency of the need is sufficiently strong to offset the university’s commitment to honor the individual’s privacy. Such grounds might include: maintaining system integrity (i.e., tracking viruses and other potentially destructive software agents); protecting system security; investigating indications of impropriety; protecting the university’s property rights; and meeting legal obligations (i.e., subpoenas).

Copyright Issues

Copyright is a form of protection provided by law to authors of “original works of authorship” for intellectual works that are “fixed in any tangible medium of expression,” both published and unpublished (Title 17, United States Code). It is illegal to violate any of the rights provided by the law to the owner of a copyright. John Carroll University respects the ownership of intellectual material governed by copyright laws. All members of the university community must comply with the copyright laws and the provisions of licensing agreements that apply to:

software; printed and electronic materials, including documentation; graphics; photographs; multimedia, including musical works, video productions, sound recordings, and dramatic works; and all other technological resources licensed and/or purchased by the university or accessible over network resources provided by the university. Individual author, publisher, patent holder and manufacturer agreements should be reviewed for specific stipulations.

All technological and information resources developed by university employees, students and contractors for use by the university, or as part of their normal employment activities, are considered “works for hire.” As such, the university is considered the “author” and owner of these resources. (For information regarding the ownership of technological resources developed with grant funding, contact the Associate Academic Vice President.)

Revised Date: 03/10/2006