Title: Professional Standards and Business Conduct --
Use of University Technological and Information Resources

Code: 1-100-025

Date: 9-1-95

Approved: JDM

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 central educational mission of Boston College, 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 to adhere to high moral, legal, and professional standards, and are expected to support the mission, and act in the best interests, of Boston College. (For additional information regarding the ethical business standards of Boston College, please see policy 1-100-010, Professional Standards and Business Conduct -- General Policy.)

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 Boston College community. While the University encourages the exploration of educational and scholarly interests through the use of its technological resources, respect for the rights and privacy of others must be observed. 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.

Boston College 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 are to comply with the following policies, procedures, and security controls.

Access

Many of the technological and information resources of Boston College 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 are to determine and authorize the appropriate degree of access for each member of their units, and are to provide unit members with adequate orientation and training regarding the ethical use of all technological and information resources.

Users are to take precautions to prevent the unauthorized use of their access codes. Access codes are not to be shared with others and their confidentiality is to be strictly maintained. In choosing access codes, users are to 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. Users will be held accountable for all actions performed under their access codes, including those performed by other individuals as a result of user negligence in protecting the codes. Users are responsible for monitoring access on their accounts and for changing access codes on a regular basis. If access codes become compromised, users are to change them immediately.

Users are not to attempt to access, search, or copy technological and information resources without the proper authorization. No one is to use another individual's account, either with or without permission, and active sessions are not to be left unattended. The provision of false or misleading information in order to gain access to technological and information resources is prohibited. Users are not to test or attempt to compromise internal controls, even for purposes of systems improvement. Such actions require the advance, written approval of the authorized organizational unit head, or must be included among the security evaluation responsibilities of one's position. Suspected violations are to be reported to the Data Security Administrator in the Office of Information Technology.

Protecting Confidentiality

No user is to disclose confidential information unless disclosure is a normal requirement of that user's position and has been so authorized. All users with access to confidential data are to safeguard the accuracy, integrity, and confidentiality of that data by taking the precautions, and performing the office 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. (For information regarding the confidentiality of student educational records, please see policy 4-730-005, Student Education Records.)

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. Boston College recognizes that individuals have a substantial interest in and reasonable expectation of privacy. Accordingly, Boston College respects the privacy rights of all members of the University community.

The University will not monitor users' 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 centralized locations. In such instances, user deletion of an electronic file, such as an e-mail message, may not delete a previously archived copy of that file.

It is a violation of Boston College policy for any member of the University community to engage in electronic "snooping," or, the use of technological resources for the purpose of satisfying idle curiosity about the affairs of others, with no substantial business purpose for obtaining access to such files.

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: (1) maintaining system integrity (e.g., tracking viruses); (2) protecting system security; (3) investigating indications of impropriety; (4) protecting the University's property rights; and (5) meeting legal obligations (e.g., subpoenas).

Copyright Issues

Copyright is a form of protection the law provides to the authors of "original works of authorship" for their 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. Boston College respects the ownership of intellectual material governed by copyright laws. All members of the University community are to comply with the copyright laws and the provisions of the 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 are to be reviewed for specific stipulations.

All technological 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, please see the Boston College Research Policies published by the Office for Sponsored Programs.)

Integrity and Protection of Technological and Information Resources

- Viruses
  It is the responsibility of the user to ensure that any imported or exported executable code or data are free of any destructive code, such as a virus. To this end every precaution is to be taken by the user, and the Office of Information Technology is to be consulted for related information and software.

- Backups
  It is the responsibility of the organizational unit head or network administrator to ensure that appropriate procedures and resources are in place to backup data on a regular basis. Backups are to be stored in a location that is physically secure and that protects the confidentiality of the data. It is the responsibility of the individual user to perform any actions necessary to comply with these procedures.

- Physical Security
  All users are responsible for the physical security of their technological and information resources. Organizational unit heads are to help ensure physical security by instituting procedures for the use of locked doors and/or for the use of the security devices made available by the University for the protection of equipment. To avoid loss by fire or theft, backups of important data are not to be stored in the same location as the originals. Adequate power regulators and surge suppressers are to be employed.

- University Property
  Technological and information resources that are the property of the University are not to be copied, altered, manipulated, transferred, retained, or removed from campus. (The ownership of technological resources purchased with grant funding is determined by the individual granting agency. For additional information, please contact the Office of Research Compliance and Intellectual Property Management.) The location of each physical resource is to be entered in the University Capital Equipment Inventory System and/or the Information Technology Inventory System and updated as necessary.

Personal Use of University Technological Resources

Authorization for the personal use of University technological resources by employees is to be determined on an individual basis by, and at the discretion of, the responsible unit head. The use of University technological resources, including the network, for a revenue generating activity that benefits an individual employee is strictly prohibited without the express written approval of the cognizant vice president and the Executive Vice President. Personal telephones and data connections in student residence halls are considered to be part of the private residence. Student use of these and other University technological resources that intrudes on general University use or that utilizes significant resources is prohibited.

Misuse of Technological and Information Resources

The use of University technological and information resources, and the resources themselves, are not to be abused in any way. Unauthorized users are not to modify, destroy, or in any other way render resources unsuitable for their intended purpose. Users are not to attempt to alter the restrictions associated with their accounts or to attempt to breach internal or external security systems. Moreover, users are not to impersonate other individuals or to misrepresent themselves in any way when using University technological resources.

The network is not to be used for criminal purposes or, for example, to post another individual's credit card numbers or personal access codes. External networks (e.g., FAXON, WESTLAW, NEXUS, the Internet, bulletin boards) are to be used in an ethical, responsible, and courteous manner, and all users are to adhere to the policies of these services.

University technological and information resources are not to be used in a manner that is invasive or that diminishes their efficiency. One example of such usage involves the broadcast function. Although current technology enables users to broadcast voice, e-mail, or video messages to all members of the University community simultaneously, the use of this technology is restricted. Specific guidelines regarding network and video broadcasting are available from the Office of Information Technology or the Audiovisual Department.

Handling Potentially Offensive Material with Discretion

Material is accessible on network resources which some individuals may consider objectionable or offensive. Boston College does not encourage or endorse the access of such material except for legitimate academic purposes. Users are to exercise caution and good judgment if there is a reasonable expectation that accessed material may be considered objectionable by some. Such material is to be accessed in a private environment and in a manner that will not negatively affect those who may deem it objectionable or offensive. Public workstations (i.e., those in open offices, laboratories, the libraries, and other public places) are not to be used to access such material, hard copies are not to be directed to public printers, and potentially offensive material is not to be forwarded to others without their consent. The use of potentially offensive language in the text of network messages or to identify technological resources is prohibited. The use of University technological resources for creating or sending nuisance, harassing, or obscene materials or messages is also prohibited. Moreover, users of network resources are prohibited from engaging in any activity that is proscribed by federal and/or state law.

Communications from members of the University community are to reflect mutual respect, civility, and other moral standards. The use of obscene or intolerant language, and the use of similarly offensive graphic or video images, clearly violate these standards and are considered inappropriate for electronic and all other forms of University discourse. The determination of what is obscene, offensive, or intolerant is within the sole discretion of the University. Users should note that University technological and information resources may be accessed by minor children outside the Boston College community.

Reporting Suspected Violations

Suspected violations of this policy are to be reported to the appropriate organizational units or unit heads. Depending on the nature of the violation, the appropriate units or unit heads may include the University Harassment Counselor, the Office of the Dean for Student Development, the Office of

University Housing, the responsible Vice President's office, the Data Security Administrator in the Office of Information Technology, or the Internal Audit Department. If a suspected violation is reported instead to a supervisor, chairperson, director, dean, or other responsible person, that person is to report the instance to the appropriate units or unit heads.

Suspected violations are to be reviewed in accordance with current resolution processes. Depending on the nature of the violation, such processes may include the Discriminatory Harassment Complaint Resolution Process, the Student Judicial Procedure, or faculty and staff grievance procedures. Suspected violations of a less serious nature may be subject to review and educational follow-up by the Data Security Administrator in the Office of Information Technology.

The University will consider the intent, effect, and seriousness of the incident in levying sanctions for violations of this policy. Any person who engages in any kind of computer or systems misuse as described above may be subject to disciplinary action, including the loss of computer privileges and/or dismissal from the University, and to criminal prosecution under the applicable state and/or federal laws. Whenever the University deems it appropriate, restitution may be sought for any financial losses sustained by Boston College, or by others, as a direct result of the misuse.

Posted: October 16, 1995
WWW: April 24, 1997
Update: June 9, 2003; March 30, 2004
