

3342-9-01 University policy on responsible use of information technology

- (A) Purpose. Access to modern information technology is essential to Kent state university's mission of providing the students, faculty and staff with educational services of the highest quality. The pursuit of the missions of teaching, research and public service is greatly enhanced by the use of computing systems and software, access to the world wide web, and other technology resources that are available to the entire campus community. The preservation of those resources for the community requires that each faculty member, staff member, student or other authorized user comply with institutional policies, applicable federal and state laws and responsible use of technical resources.
- (B) Operational procedure.
- (1) Authorized users of campus computing and network resources shall be faculty, staff, student and other affiliated individuals or organizations authorized by the vice president for information services.
 - (2) Notwithstanding the geographical location of the user, authorized use of campus-owned or operated computing and network resources shall be consistent with the teaching, research and public service mission of Kent state university and consistent with this policy.
 - (3) Information technology provides important means for both public and private communication. Users and systems administrators shall respect the privacy of person-to-person communications in all forms including telephone, electronic mail and file transfers, graphics and television to the fullest extent possible under applicable law and policy. The principle of academic freedom shall apply to public communication in all these forms of communication, as well as in the transmission of information in both the physical and virtual classrooms, subject to the limitations set forth hereinafter.
 - (4) Subject to requirements of network administration, Kent state university shall not monitor or restrict the content of material

posted on university-owned computers, or transported across its networks. However, Kent state university reserves the right to:

- (a) Limit access to its networks; and
 - (b) Remove or limit access to content or to material residing on or transmitted on university-owned computers or networks when exigent circumstances arise (i.e., evidence of a reported violation of applicable university policies, contractual).
- (5) Determination of violations shall be made in accordance with established applicable due process procedures (i.e., student code of conduct, collective bargaining agreement, academic and administrative grievances and appeals policies, as appropriate).
 - (6) In the normal course of system maintenance, both preventative and troubleshooting, staff members operating the computer systems may be required to view files. Staff shall be required to maintain the confidentiality and privacy of information in such files unless otherwise required by law or university policy.
 - (7) Kent state university reserves the right, upon reasonable cause for suspicion, to access all aspects of its computing systems and networks, including individual login sessions to determine if a user is violating this policy or state or federal laws.
 - (8) This policy may be supplemented with additional guidelines or regulations developed by units and companies that operate their own computers or networks, provided they are consistent with this policy.
 - (9) A university member who stores or distributes copyrighted material must be the copyright holder or have the permission of the copyright holder as required under law. This includes duplication of audiotapes, videotapes, photographs, illustrations, computer software, and all other information for educational use or any other purpose.

- (10) No user may, under any circumstances, use Kent state university computing equipment, software or networks to harass or defame any other person.
- (C) Security and privacy of e-mail.
- (1) Access. The university recognizes the private nature of electronic mail communications. The university may access such files in the course of its normal supervision of the network or system (i.e., backing up of electronic messaging material), or when exigent circumstances arise (i.e., evidence of reported violations of policies or laws). Accordingly, the private nature of electronic mail communications sent or received by users on any computer system owned or operated by the university shall be maintained, subject to the technology limitations of the university's electronic systems and in a manner consistent with university polices, state and federal laws.
 - (2) Public records request. From time to time the university may receive requests pursuant to section 149.43 of the Revised Code (the Ohio Public Records Act). When such requests are for access to a user's e-mail files, the university will make a good faith effort to notify the affected user. A good faith effort may include, though not be limited to, an e-mail message sent to the affected user's university e-mail address or telephone notice, including a message left on the university-based voice mail system.
 - (3) Security. Kent state university employs various measures to protect the security of its computing resources and its users' accounts. Users should be aware, however, that the university cannot guarantee the absolute security and privacy of data stored on university computing facilities. Users should therefore engage in safe computing practices including but not limited to establishing appropriate access restrictions for their accounts, guarding their passwords, changing them regularly, and by backing up critical files when appropriate.

Effective: June 1, 2007

Prior Effective Dates: March 14, 2002; September 19, 2005