

## **Western Kentucky University Computing Ethics Policy**

The general standards of conduct expected of a member of an education institution also apply to the use of University computing and communications resources. These resources include:

1. "Hardware" - physical equipment used for processing or communications.
2. "Software" - programs, programming languages, instructions, or routines which are used to perform work on a computer.
3. "Data" - information such as records or textual material stored on or accessible through a computer.

University computing and communications resources are made available to individuals to assist in the pursuit of educational goals. It is expected that users will cooperate with each other so as to promote the most effective use of computing and communications resources and will respect each other's ownership of work even though it is in electronic rather than printed form. Individuals and organizations will be held no less accountable for their actions involving computers than they would be in other situations.

Rules prohibiting theft or vandalism apply to software and data as well as to physical equipment. Conduct which violates the University's property rights with respect to computing and communications resources includes but is not limited to:

1. Copying University-owned or licensed software or data to another computer system for personal or external use without prior written approval.
2. Sharing copyrighted music or video files on FTP, e-mail, or using any peer-to-peer software.
3. Attempting to modify University-owned or licensed software or data files without prior written approval by the administrator or faculty member responsible for its maintenance.
4. Attempting to damage or disrupt the operation of computing or communications equipment or services.
5. Using University computing or communications resources for purposes other than those intended by the University body granting access to these resources, includes but is not limited to:
  - a. Allowing access to resources by unauthorized persons, even if they are members of the University community.
  - b. The use of University computing or communications resources in external consulting, except for "occasional or incidental" professional activities, unless approved in accordance with University procedures. ("Occasional and incidental" use is defined in the Faculty Handbook under "Professional Responsibilities, subsection "Extra-University Consulting and Other Professional Activities.") When approved, such use is limited to the specific resources allocated for the purpose, and fees may be charged for such use.

- c. Downloading or sharing copyrighted files outside of the “fair use” guidelines or without the author’s permission.

The University seeks to protect the civil, personal and property rights of those actually using its computing and communications resources and seeks to protect the confidentiality of University records stored on its computer systems from unauthorized access. Conduct which involves use of University computing or communications resources to violate another's rights includes but is not limited to:

1. Invading the privacy of an individual by using electronic means to ascertain confidential information.
2. Copying or altering another user's software or data that have been obtained by illegal means.
3. Knowingly accepting or using software or data that have been obtained by illegal means.
4. Abusing or harassing another user through electronic means.
5. Using the University's computing or communications facilities in the commission of a crime.
6. Accessing data residing on university systems not related to the user’s job.
7. Intruding (hacking) into or attempting to intrude into any computer, network or communications system without authorization.

Some of the University's computer and communications systems require that each user have a unique identity, protected by a password, to gain access to the system. These authorization credentials are used to represent a user in various system activities and to provide access to certain software and data based on his/her level of authorization. As such, this computer identity is a primary instrument of identification and its misuse constitutes forgery or misrepresentation. Conduct which involves misuse of computer identities includes but is not limited to:

1. The sharing of authorization credentials with an unauthorized party.
2. Obtaining or using another individual's authorization credentials without their express permission, even if the individual has neglected to safeguard his/her computer identity.

University computing and communications resources are appropriately designed to handle expected data access and file transfer activity on the network both internally on the backbone and externally to/from the Internet. Any conduct which jeopardizes this network activity is considered misuse of computing and communications resources and includes but is not limited to:

1. Operating an unauthorized server connected to the campus network.
2. Conducting or attempting to conduct denial-of-service attacks in any form.
3. Sending harmful computer viruses.

4. Sending large audio or video files.
5. Any intentional activity that degrades the quality of the network.
6. Other activities that will cause congestion, disruption of networks or systems including, but not limited to file sharing or online gaming, downloading music or video files.

The university provides students access to e-mail and considers that privilege to be an important form of communication. We are moving towards an era where all official communications with students will be via e-mail. Since the Internet constitutes an uncensored worldwide network of networks, and e-mail provides for communications between participants, there is a great potential for misuse. Use of University e-mail resources is a privilege that may be revoked at any time for inappropriate conduct. Examples of inappropriate conduct include, but are not limited to:

1. Using the Internet and e-mail for personal gain or personal business activities in a commercial endeavor such as buying or selling of commodities or services with a profit motive.
2. Engaging in illegal activities or using the Internet for any illegal purposes, including initiating or receiving communications that violate any federal or state laws and regulations.
3. Transmitting statements, language, images or other materials that are reasonably likely to be perceived as offensive or disparaging of others based on race, national origin, sex, sexual orientation, age, disability, religious or political beliefs.
4. Using abusive, harassing, or objectionable language in either public or private messages.
5. Knowingly visiting pornographic or illegal sites, disseminating, soliciting or storing sexually oriented messages or images that are not required as part of educational requirements.
6. Misrepresenting, obscuring, suppressing, or replacing a user's identity on e-mail. This includes the use of false or misleading subject headers and presentation of information in the distribution of e-mail.
7. Sending or forwarding chain letters.
8. Distributing or forwarding unsolicited commercial e-mail.
9. Soliciting money for religious or political causes, or advocating religious or political opinions.
10. Copying, disseminating or printing copyrighted materials (including articles, music, video, images, games, or other software) in violation of copyright laws.

The management of University computing and communications resources is distributed among many University bodies. Rules and regulations governing specific resources are available through the individual governing bodies such as the open student computer labs and the departmental computer labs. Abuses of University computing or communications resources will be referred to the appropriate university authority for consideration under the University's disciplinary processes. Student referrals will be made to the Dean of Students. This referral may be accompanied by a temporary suspension of computing or communications privileges pending the outcome of the disciplinary process. In addition, Kentucky law contains specific statutes with respect to improper use of computers in state agencies. Therefore, improper use of University computing or communications resources may be subject to criminal or civil legal action in addition to University disciplinary action.

Last Modified: May 24, 2004