Western Kentucky University Computing Ethics Policy

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

1. "Hardware" – physical equipment used for processing or data 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 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 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 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. 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.

3. Attempting to damage or disrupt operation of computing equipment, data communications equipment, or data communications lines.

4. Using University computing resources for purposes other than those intended by the University body granting access to these resources, include but is not limited to:

    a. Allowing access to them by unauthorized persons, even if they are members of the University community.

    b. The using of University computing 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.

5. Sharing copyrighted music, movies, software, and games without the consent of the copyright holder is against federal law and is expressly prohibited under this policy. With the number of web sites now available to purchase and share music, movies, software, and games, there is no excuse for sharing copyrighted files. If the university receives a complaint from the Recording Industry Association of America (RIAA), Motion Picture Association of America (MPAA), or any other organization responsible for client media, the following punitive actions will be taken:

   a. For the 1st offense the person will be removed from network access until the offending file is removed, and until he/she has gone to MMTH, 3rd floor, to read the policy, watch the RIAA video, and sign a document stating the policy has been read and understood.

   b. For the 2nd offense, the person will be removed from network access for 1 month, the file will be removed from their computer, they will meet with the Associate Vice President for Student Affairs and Development (Dean of Students) to make sure they understand the importance of this violation, and go through the University’s disciplinary process which will include a $50.00 reconnect fee.

   c. For the 3rd offense, the person will be removed from network access for 3 months, the file will be removed from their computer, and they will incur a $100 reconnect fee. This violation will also be reported to the Associate Vice President for Student Affairs and Development (Dean of Students).

6. Removing desktop hardware from University premises without prior written approval is a violation of University policy and the WKU Code of Student Conduct. To obtain approval, the requesting employee must provide a valid business purpose and must certify that a personal insurance policy will cover the equipment. The University’s insurance policy only covers desktops that are located on campus. Laptops are insured by the University provided that they remain in the United States.

The University seeks to protect the civil, personal, and property rights of those actually using its computing 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 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 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 university systems for the purpose of altering data.

Some of the University's computer systems require that each user have a unique identity, protected by a password, to gain access to the system. The computer identity is used to represent a user in various system activities, to provide access to certain software and data based o his/her credibility and purpose for requiring such access, and to associate his/her software use and data access with that identity. As such, this computer identity is another instrument of identification and its misuse constitutes forgery or misrepresentation. Conduct which involves misuse of computer identities includes but is not limited to:

1. Allowing an unauthorized individual to use the owner's identity.

2. Using another individual's computer identity without that person's express permission, even if the individual has neglected to safeguard his/her computer identity.

University computing 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 misuses of computing 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. Any intentional activity that degrades the quality of the network.

5. Other activities that will cause congestion, disruption of networks or systems including, but not limited to Internet games or online gaming.

The university provides students access to e-mail and considers that privilege (not a right) 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 peer-to-peer communications between participants, they also have 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 connotation 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 or harassing 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, images, games, or other software) in violation of copyright laws.

The management of University computing 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 resources will be referred to the appropriate university authority for consideration under the University's disciplinary processes. Student referrals will be made to the Associate Vice President for Student Affairs and Development. This referral may be accompanied by a temporary suspension of computing privileges awaiting outcome of the disciplinary process. In addition, Kentucky law contains specific statues with respect to improper use of computers in state agencies. Therefore, improper use of University computing resources may be subject to criminal or civil legal action in addition to University disciplinary action.

Revised per the President's Administrative Council, June 25, 2007.