**Policy Statement:**

The publishing of an Acceptable Use Policy is not to impose restrictions contrary to Western Kentucky University’s (WKU’s) established culture of openness, trust, and integrity. Information Technology is committed to protecting WKU faculty, staff, students, and partners from illegal or damaging actions by individuals, either knowingly or unknowingly. 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.

All students, faculty and staff are responsible for conducting themselves in a manner that helps to embrace an environment of learning in which the rights, dignity, worth, and freedom of each member of the academic community are respected.

**Reason for Policy/Purpose**

This policy is required for the effective communication of the acceptable use of university computer equipment at WKU. These rules are in place to protect faculty, staff, students, and Western Kentucky University. Inappropriate use exposes WKU to risks including virus attacks, compromise of network systems and services, and legal issues.

While WKU's network administration desires to provide a reasonable level of integrity, users should be aware that the data/email they create/receive on university systems remain the property of WKU and that no privacy can be expected while using these systems. Because of the need to protect the university's network, management cannot guarantee the confidentiality of information stored on any network device belonging to WKU.

Faculty and staff are responsible for exercising good judgment regarding the reasonableness of personal use. Information Technology recommends that any information which users consider sensitive or vulnerable be password protected.

For security and network maintenance purposes, authorized individuals within the

WKU Information Technology Department (IT) may at any time analyze network utilization, traffic patterns and volumes related to WKU systems/equipment and network.

WKU’s Information Technology Department (IT) reserves the right to audit networks and systems periodically to ensure compliance with this policy.

WKU students, faculty and staff are expected to comply with University policies concerning the use and/or access to University Information Technology systems, which are posted at <http://www.wku.edu/it/policies/>.

Web publications using University computers or utilizing the University Internet connection or address may only be used for instruction, research, or public service. With the exception of consulting which qualifies as University public service, use of University computing resources to promote for-profit enterprise or activity is not acceptable. For instance, while faculty members who provide private consulting services related to their disciplines might briefly describe these on their personal or professional pages and provide information for direct personal contact, enterprises that fail to meet this definition should not be promoted through the University network. In no case would public description of specific service offerings and prices be appropriate on a University subsidized Web service.

Individuals and organizations are reminded that their pages may be viewed by any person with network access, on- or off-campus, and should always be in good taste. Any statement, act, or offer which could lead to criminal or civil action if made in public, over a telephone, or through the mail should be viewed as equally subject to legal action if made over the Internet.

### ****Support of Web Pages****

The support of World Wide Web pages consumes disk space, communications capacity, and personnel time. University resources are subject to limitations and competing demands, and the priority order of reasonable support for web pages is departmental, professional, and personal. Thus, the Information Technology Division’s Network Department may determine the need to set rules for maximum size of pages residing on the University's multi-user systems and/or restrictions on access hours (wherever the page resides). Such rules may vary between classes, and the committee may create exception within a class, e.g., personal pages created by students as an instructional requirement might be given a higher priority than other pages of that type. Complaints or questions about Web policies or about the form and/or content of any particular page should be directed to the IT Webmaster at webmaster@wku.edu This e-mail address is being protected from spambots. You need JavaScript enabled to view it .

### Acceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances are faculty, staff, and students of WKU authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing WKU-owned resources.

The list below is by no means exhaustive, but an attempt to provide a framework for activities which fall into the category of unacceptable use:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation of “pirated” or other software products that are not appropriately licensed for use by WKU.
2. Collection, storage or distribution of pornography or material considered to be obscene in violation of this policy.
3. Unauthorized copying of copyrighted materials including but not limited to, digitization and distribution of photographs for magazines, books or other copyrighted sources, copyrighted music, copyrighted movies and the installation of any copyrighted software for which WKU or the end user does not have an active license is strictly prohibited.
	1. 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.
	2. b. For the 2nd offense, the person will be removed from network access for 1 month, the file will be removed from their computer, and a $50 reconnect fee will be incurred. This violation will be reported to The Office of Judicial Affairs.
	3. 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. They will meet with the Director of Judicial Affairs to make sure they understand the importance of this violation, and go through the University’s disciplinary process.
4. Prohibiting theft or vandalism applies to software and data as well as to physical equipment.
	1. Removing software or desktop hardware from University premises without prior written approval is a violation of University policy and the WKU Student Code of 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.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
6. 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 on 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.
	1. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
	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.
7. Using a WKU computing asset to actively engage in procuring or transmitting material in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any WKU account.
9. Effecting security breaches or disruptions of network communication.
	1. Security breaches include, but are not limited to, the following: Accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.
10. Port scanning or security scanning is expressly prohibited unless prior notification is given to Information Security and /or these processes are within the scope of regular duties.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duties.
12. Circumventing user authentication or security of any host, network, or account.
13. Operating an unauthorized server connected to the campus network.
14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, by any means, locally or via the Internet/Intranet/Extranet.
16. 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.
17. Not following computer lab, system, or University policies, procedures, or protocol.
18. Violating local, state or federal laws.

The university provides students access to e-mail and considers that privilege (not a right) to be an important form of communication. Use of University e-mail resources is a privilege that may be revoked at any time for inappropriate conduct. Any person found in violation of this policy will be notified immediately to cease and desist. The user will be given a time frame to comply or be disconnected from the WKU network until they can prove the issue has been addressed.

**Email and Communications**–The following activities are strictly prohibited, without exception:

1. Sending email messages, including "junk mail/SPAM" or other advertising material, to individuals who did not specifically request such material (email spam).
2. Providing information about (or lists of) WKU faculty, staff, or student protected/non-directory information to parties outside the university without the express written permission of the university administration.
3. Users must respect the right of others and communication should be free from harassment or intimidation to the same extent that this right is recognized in the use of other communications media. Consequently, although each user has the right to freedom of speech, unlawful material may not be sent or displayed to others. Any uses of computing resources to threaten; harass or bully others, or transmitting obscene or fraudulent messages is prohibited.
4. Unauthorized use, or forging, of email header information in an attempt by an individual to misrepresent or hide his or her identity.
5. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
6. Creating or forwarding chain letters or other pyramid schemes of any type.
7. Use of unsolicited email originating from within WKU's networks to advertise for service, or make profit not authorized by WKU.
8. Posting the same or similar non-business-related messages to large numbers of Usenet news groups (newsgroup spam).

## Threats, Coercion, Harassment, Intimidation, or Hostile Communication

The University embraces and strives to uphold the freedoms of expression and speech guaranteed by the First Amendment of the U. S. Constitution and the [state] Constitution. The University has the right, when reported, under the above circumstances to regulate the time, place, and manner of exercising the judicial process when a student or constitutionally protected rights are violated.

In determining whether student conduct violates the local, state and federal laws or rights of others, all relevant facts and circumstances shall be considered. Careful examination of the Student Code of Conduct will be exercised prior to any action in order to preserve freedoms of speech, and expression, as articulated in current legal standards.

**Reporting Violations**

All suspected violations must be reported immediately to the proper authorities.

For alleged student violations, contact the Office of Judicial Affairs.

For faculty and staff, contact your immediate supervisor. For all others, contact the IT Division.

**ENFORCEMENT**

Faculty, Staff, and Students:

Any faculty, staff, or student found to have violated this policy may be subject to disciplinary action, up to and including suspension, expulsion and/or termination of employment in accordance with procedures defined by USM administrative policies stated in the handbook governing that individual.

External Entities:

Any external entity, contractor, consultant, or temporary worker found to have violated this policy may be held in breach of contract, and as such, may be subject to grievances or penalties allowed by such contract

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 Office of Judicial Affairs. 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.

## University Computing Resources

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.

## Computing & Copyright Facts

Downloading copyrighted music, movies, software, and games 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.

* Students are responsible for all network activity originating from their port and their computer.
* It is the student’s responsibility to properly maintain the security of his or her computer.
* The network is a shared resource.
* Software enables us to accomplish many different tasks with computers.
* Unauthorized copying of software is illegal. Copyright Laws protect software authors and publishers.
* Unauthorized copying of software by individuals can harm the entire academic community. If unauthorized software is available on a campus, the institution may incur a legal liability.
* Unauthorized copying of software deprives developers of a fair return on their work, increases prices, reduces the level of future support and inhibits the development of new software.
* Copyright protection lasts through the life of the author, plus 70 years.
* Copyright protects: books, articles, photographs, paintings sculptures, software, websites, music, sound recordings, and even graffiti.

## Recent Statistics

* There are billions of unauthorized music downloads per month.
* Last year, record sales in the United States were down 10 percent.
* The Motion Picture Association of America estimates that it loses more than $3 billion annually on the sale of illegally copied videotapes and DVDs.
* More than 350,000 movies are illegally downloaded every day.
* Pirating works online is the same as shoplifting a videotape, DVD, book or record from a store.

## Illegal File Sharing

**XDCC—Direct Client Connection**

Your computer may be UPLOADING OTHER FILES WITHOUT YOUR KNOWLEDGE OR PARTICIPATION! In addition to the concern about the KaZaA, Morpheus and similar clients, there have been directed attacks against any number of student, faculty, and staff computers. It is probable the excessive Uploading is due to a file-sharing exploit, referred to as DCC (Direct Client Connection), having been surreptitiously loaded onto your computer. In this scenario, copyrighted movies, games, TV programs, music or pornographic files are loaded (or stored) on the computer along with the DCC client. This can result in excessive (and illegal) uploading, or outbound traffic, from the affected computer (traffic moving away from Western Kentucky University), necessitation bandwidth management of the network connection. This can happen completely without your knowledge or participation. The article at the following link is just one of many on the DCC client: [*http://www.securiteam.com/securitynews/5ZP021575W.html*](http://www.securiteam.com/securitynews/5ZP021575W.html)

The file-sharing exploit needs to be immediately eliminated. Once done, the network connection speed will return to normal within twenty-four (24) to forty-eight (48) hours. If you require technical assistance with removing the file-sharing client, it is STRONGLY RECOMMENDED that you contact Western Kentucky University Info Tech Help Desk at (270)745-7000.

##

## Information Technology Resource Page at Western Kentucky University

<http://www.wku.edu/it/>

### IT Security:

Although antivirus software cannot completely protect your computer from malicious files, it is by far your best protection. Always run antivirus software on your computer. The University provides Symantec Antivirus software to students that live on campus.

Visit: <http://www.wku.edu/it/sms/>

**Safe Computing:**

[*http://www.wku.edu/it/security/sc-general.php*](http://www.wku.edu/it/security/sc-general.php)

**File Sharing:**

[*http://www.wku.edu/it/security/file-sharing.php*](http://www.wku.edu/it/security/file-sharing.php)

**Security Alerts:**

[*http://www.wku.edu/it/security/471*](http://www.wku.edu/it/security/471)

**Software Updates:**

[*http://www.wku.edu/it/security/software-updates.php*](http://www.wku.edu/it/security/software-updates.php)

**Desktop Support:**

[*http://www.wku.edu/it/helpdesk/*](http://www.wku.edu/it/helpdesk/)

**Computing Ethics Policy**

**Internet and Electronic Mail Acceptable Use Policy**

**Account Retention & Termination Guidelines:**

[*http://www.wku.edu/it/policies/*](http://www.wku.edu/it/policies/)

**Copyright Information**

**Recording Industry Association of America:**

[*http://www.riaa.com/physicalpiracy.php?content\_selector=piracy\_details\_online*](http://www.riaa.com/physicalpiracy.php?content_selector=piracy_details_online)

**Motion Pictures Association of America:**

[*http://www.mpaa.org/contentprotection/copyright-info*](http://www.mpaa.org/contentprotection/copyright-info)