University IT Policies

Acceptable Use

Computer Usage: The purpose of University policies regarding computer and network usage is to protect all individuals affiliated with William Woods University. Inappropriate use exposes the University to risks, including virus attacks, compromise of network systems and services, and possible legal liability.

Access to the information technology environment at William Woods University is a privilege and must be treated as such by all users. Students are expected to be positive members of the University community, which extends to cyberspace, by following the Community Code and all University policies.

Users who violate any acceptable use policy will be subject to disciplinary action, up to and including loss of privileges and/or expulsion, and may be at risk for civil or criminal prosecution. All violations will be handled in accordance with William Woods University policies and procedures.

Following is a brief summary of relevant University policies regarding computer and network usage. All policies in their entirety can be found on the University's website or requested from the University Information Technology (UIT) Office.

Acceptable Use Policy: William Woods University information technology resources, including electronic communications on and off the WWU campus and the computers attached to this network, are for the use of persons currently affiliated with William Woods University, including faculty, staff and students. Information technology resources are provided by the University to further the mission of lifelong education. Use of these resources should be consistent with this mission and this policy.

Central to appropriate and responsible use is the stipulation that computing resources shall be used in a manner consistent with the instructional, public service, research, and administrative objectives of the University. Use should also be consistent with the specific objectives of the project or task for which such use was authorized. All uses inconsistent with these objectives are considered to be inappropriate use and may jeopardize further access to services.

Unacceptable uses include, but are not limited to, the following:

- Using the resources for any purpose that violates federal or state laws.
- Using the resources for commercial purposes, sales and/or advertising.

- Using excessive data storage or network bandwidth in such activities as propagating of “chain letters” or “broadcasting” inappropriate messages to lists or individuals or generally transferring unusually large or numerous files or messages.
- Sending or storing for retrieval patently harassing, intimidating, or abusive material.
- Misrepresenting your identity or affiliation in the use of information technology resources.
- Using someone else’s identity and password for access to information technology resources or using the network to make unauthorized entry to other computational, information or communications devices or resources.
- Attempting to evade, disable or “crack” password or other security provisions of systems on the network.
- Reproducing and/or distributing copyrighted materials without appropriate authorization.
- Copying or modifying files belonging to others or to the University without authorization including altering data, introducing or propagating viruses or worms, or simply damaging files.
- Interfering with or disrupting another information technology user’s work as well as the proper function of information processing and network services or equipment.
- Intercepting or altering network packets.

Gramm, Leach, Bliley and Compliance

In order to protect critical information and data, and to comply with Federal Law, specifically the Gramm, Leach, Bliley Act, William Woods proposes certain practices in WWU information environment and institutional information security procedures. The goal of this document is to define the WWU's Information Security Program, to provide an outline to assure ongoing compliance with federal regulations related to the.

Guidelines:

II. Gramm Leach Bliley (GLB) Requirements

GLB mandates that WWU appoint an Information Security Plan Coordinator, conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust the Information Security Program periodically. The Vice President of Financial Services has been appointed the Information Security Plan Coordinator. He as appointed the Director of Human Resources and Benefit Services and the Web Administrator to implement the GLB requirements.

III. Information Security Plan Coordinator

The Coordinator and his designees will assist WWU's relevant offices identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; evaluate the effectiveness of the current safeguards for controlling these risks; design and implement a safeguards program, and regularly monitor and test the program.

IV. Risk Assessment and Safeguards

The Coordinator and his designees must work with all relevant areas of the university to regularly assess and identify potential and actual risks to security and privacy of information. Each Division or Department head, or her designee, will conduct an annual data security review, with guidance from the Coordinator. Vice Presidents will be asked to identify any employees in their respective areas that work with covered data and information. University Information Technologies will conduct an annual security audit and develop electronic information security best practices and an incident response policy.

While the university has discontinued usage of social security numbers as student identifiers, one of the largest security risks may be the possible non-standard practices concerning social security numbers, e.g. continued reliance by some university employees on the use of social

security numbers. Social security numbers are considered protected information under both GLB and the Family Educational Rights and Privacy Act (FERPA). By necessity, student social security numbers still remain in the University student information system.

The university will conduct an assessment to determine who has access to social security numbers, in what systems the numbers are still used, and in what instances students are inappropriately being asked to provide a social security number. This assessment will cover university employees as well as subcontractors such as security and food services, and consortiums such as MOBIUS.

University Information Technologies will develop written plans and procedures to detect any actual or attempted attacks on covered systems and will develop incident response procedures for actual or attempted unauthorized access to covered data or information.

V. Employee Training and Education

While directors and supervisors are ultimately responsible for ensuring compliance with information security practices, the Director of Human Resources and Benefit Services and the Web Administrator will develop training and education programs for all employees who have access to covered data.

VI. Oversight of Service Providers and Contracts

GLB requires the university to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. Business Services, in cooperation with the Office of General Counsel, will develop and send form letters to all covered contractors requesting assurances of GLB compliance. While contracts entered into prior to June 24, 2002 are grandfathered until May 2004, the Vice President of Financial Services will take steps to ensure that all relevant future contracts include a privacy clause and that all existing contracts are in compliance with GLB.

VII. Evaluation and Revision of the Information Security Plan

GLB mandates that this Information Security Plan be subject to periodic review and adjustment. The most frequent of these reviews will occur within University Information Technologies where constantly changing technology and constantly evolving risks indicate the wisdom of quarterly reviews. The plan itself should be reevaluated annually in order to assure ongoing compliance with existing and future laws and regulations.

VIII. Definitions

Covered data and information for the purpose of this policy includes student financial information required to be protected under the Gramm Leach Bliley Act (GLB). WWU chooses as a matter of policy to also define covered data and information to include any credit card information received in the course of business by the university, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records.

Student financial information is that information the university has obtained from a student in the process of offering a financial product or service, or such information provided to the university by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and social security numbers, in both paper and electronic format.

Network Printing

Purpose of Policy: The purpose of this policy is to define and enforce procedures that apply to printing at the University. This policy also allows UIT to keep printing costs down and enables us to provide more and better services.

- Approved: This policy was reviewed and approved by the President.
- Person(s) with Primary Responsibility: PAS Administrator

Principles of Printing Policy

The purposes of printing policies are twofold; to reduce the amount of resources required to sustain maximum operations while reducing overall costs.

- Charge Method—A charge will be made for any print request sent to a University printer.
- Account Balance provided—University Information Technologies will provide each student the amount equal to 100 printed pages free at the beginning of the fall semester.
- Adding to Account Balance—Additional pages may only be purchased at the cashier's windows during regular business hours for a fee at a rate of $0.05 per b/w page.
- Account Balance Carry Over—a remaining balance will carry over from the fall semester to the spring semester, but will NOT be carried over from the spring semester for the full academic year.
- Refunds—a refund will only be given by and when the Print Account Server Administrator deems a miscalculation by the PAS system has occurred.

User Account Information

Each student's printing account information will be included with their William Woods network account.

- Checking Account Balance—Users may check their current PAS account balance by logging on to a University computer and double clicking the PAS coin icon located in the system tray.

- Detail Account Reporting—for a detailed account report, in the Internet browser type: http://ntps:2914 and press Enter. Enter your William Woods username beginning with: williamwoods\username and password. This will give your current balance. Click 'statement' to view a record of print jobs within the past 30 days.

RESPONSIBILITY

University Information Technologies maintains and defines responsibilities or both UIT and the individual end user.

- Using Persons Accounts—University Information Technologies accepts no responsibility for prints occurring by other users under any account. You MAY NOT use another person's PAS account balance. You MAY NOT transfer balances between accounts.

- End User Responsibility—It is the individual's responsibility to completely log off the system there by keeping others from using their account information.

- Violations of Policy—using another person's account information is considered stealing and a violation of this policy. Any violation should be reported to UIT and will be prosecuted according to University policy.

- Reservations—University Information Technologies reserves the right to make changes to printing rates charged at their discretion and as needed. This policy is subject to amendment at any time. For a copy of the most recent policy, see the William Woods University web site at: http://www.williamwoods.edu/.

Revision History

March 10, 2004

March 11, 2004

Network Use Policy

Summary

To establish guidelines governing the use and connection of networking devices on the University's Data Communications Network. This policy applies to all university networked devices, ranging from multi-user systems to single user personal computers. This includes networked printers, mini-hubs, routers, switches, and any other network communication devices, which are connected to the university's network. The individual with primary responsibility is the Network Administrator and the back-up designee.

The university provides network access and capabilities through the Network Services Division of the University Information Technologies Department. The guidelines listed below are required in order to provide the university a reliable and stable networking platform.

Guidelines

All networking equipment connected to the university network must first be registered and approved by Network Services Division of the University Information Technologies Department. The responsible parties with problem network devices and/or services will be notified and expected to correct the problem in a timely manner. Any networked devices or services that degrade the quality for service on the network, will result in termination of network service to that device until the correction occurs. Activities, which interfere with the operation of the network, are prohibited. These include but are not limited to the propagation of computer worms, network sweeps, network probing, viruses, or Trojan horses.

Violations of this policy will be handled in accordance with William Woods University policies and procedures.

Personal Wireless Point Access Installation

Unauthorized Wireless Access Points (APs not installed, maintained and managed by the UIT Division) are prohibited at WWU. Please do not use personal networking or home networking devices. This policy was implemented in order to manage the limited airwave space at WWU and to facilitate a common campus wide standard for wireless networking that will be available to all legitimate WWUusers. If unauthorized APs are identified (usually by their interference with other services), the owners of the offending APs will be asked to remove them from the network and the devices will be blocked from the network. Repeat offenders will be referred to the Dean of Student Life for appropriate judicial action.

Revised July 14, 2008

Password Policy

Summary

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of changeThe individual with primary responsibility is the Network Administrator and the back-up designee.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of William Woods University's entire network. Thus, all William Woods University employees (including contractors and vendors with access to William Woods University systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The scope of this policy includes faculty, staff and students who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any William Woods University facility, has access to the William Woods University network, or stores any non-public William Woods University information.

All system-level passwords (e.g., root, enable, 2000 admin, application administration accounts, etc.) must be changed on at least a quarterly basis. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months. Passwords should never be inserted into email messages or other forms of electronic communication. All user-level and system-level passwords must conform to the guidelines described below.

Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at William Woods University. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local switch logins. Since very few systems have support for one-time tokens, (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as: dog, desk, apple, etc.
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "William Woods University", "Fulton", "owls" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics that are required for all WWU users:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, <>?,./">!@#$%^&*()_+|~-=\`{}[]:";'<
- Are at least eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for William Woods University accounts as for other non-William Woods University access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various William Woods University access needs. For

example, select one password for the Jenzabar and a separate password for email and network. These should be different from your home ISP or electronic banking password.

William Woods University passwords should not be shared with anyone, including faculty, staff or students. All passwords are to be treated as sensitive, confidential William Woods University information.

Here is a list of “don'ts”:

- Don't reveal a password over the phone to ANYONE, EVER.
- Don't reveal a password in an email message.
- Don't reveal a password to the boss.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on vacation.
- Don’t reveal a password in chat.

If someone demands a password, refer them to this document or have him/her call the Network Administrator.

The "Remember Password" feature of applications (e.g., Eudora, Outlook, Entourage, and Outlook Web Access) should not be used.

Passwords should not be written down and stored them anywhere in your office. Passwords in a file on ANY computer system (including Palm Pilots or similar devices) should not be stored without encryption.

Change passwords at least once every six months. The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to the Helpdesk and change all passwords.

University Information Technologies or its delegates may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

D. Use of Passwords and Pass phrases for Remote Access Users

Access to the William Woods University Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Pass phrases

Pass phrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Pass phrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good pass phrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase: "The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

Enforcement

Violation of this policy will be handled in accordance with William Woods University policies and procedures.

Mailbox Management Policy

Summary

To establish guidelines for automatic removal of older mail items in the Inbox, Sent Items, Calendar, and Deleted Items folders. Automatic purging will maintain the client databases, limit disk space usage, and reduce possible corruption. Reasonable mailbox sizes are necessary to efficiently manage the universities email system. Users exceeding limitations for more than 14 days will be notified by University Information Technologies. The individual with primary responsibility is the Network Administrator and the back-up designee.

Guidelines

The email system is set up so that the following purges are automatically implemented as follows:

- Inbox - 180 days: The Inbox is the primary folder for all incoming mail items. Items that are older than 180 days will automatically be deleted. These items will be placed in the Deleted Items folder for up to seven days.
- Calendar - 365 days: Appointments, Tasks, and Notes that are older than 365 days will automatically be deleted. These items will be placed in the Deleted Items folder for up to seven days as indicated below. Reoccurring appointments will only be removed from the calendar if they meet the 365-day criteria.
- Deleted Items - 7 days: The items that are marked for deletion are placed in the Deleted Items folder for seven days. Afterward, the items will be automatically removed. These items cannot be restored easily; therefore, it is critical to mark only the items that need deleting.

*In order to maintain mail past the date limitations, users may establish automatic archiving to a specific directory on your personal computer or within another folder in your mailbox before the dates indicated above. Please reference HELP in the particular email client for assistance.

Email Policy

Summary

This policy covers appropriate use of any email sent from William Woods University email address and applied to all employees, vendors, and agents operating on behalf of William Woods University.

Guidelines

The William Woods University email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, religion, or national origin. Employees who receive any emails with this content from any William Woods University employee should report the matter to their supervisor immediately.

All email sent or received from a William Woods University server must comply with the Acceptable Use Policy.

While it is our intent to maintain a creative and educational environment, please be aware that all equipment and functions related to the operations of the computer systems at William Woods are university owned. Please also be aware that no expectation of privacy should exist for any material stored on the computer network or computer equipment. Because university personnel are responsible for the maintenance and support of the computer systems, the university reserves the right to access equipment and material stored on any computer equipment or software programs at any time.

Violations of this policy will be handled in accordance with William Woods University policies and procedures.

File Sharing Policy

Summary

The purpose of this policy is to define William Woods University's position on the sharing, distributing, or using illegal or unauthorized copies of software, music, video, and all other forms of piracy; digital or non-digital. The individual with primary responsibility is the Network Administrator and the back-up designee.

Guidelines

Providing or obtaining unauthorized copies of audio and visual works in either digital or non-digital format is not appropriate and may be illegal.

Any number of file-sharing applications, Kazaa or Morpheus for example, enables you to locate and download music, movies and video in digital format. Use of this type of software raises important issues regarding copyright law, network traffic and security.

Copyright Law

Copyright laws were enacted to protect the original expression of an idea, whether it is expressed in the form of music, art or written material. A number of rights are given copyright owners by Federal law. These rights include the right to control the reproduction, distribution and adaptation of their work, as well as the public performance or display of their work. Many states have laws that support the federal laws and often go further to address piracy.

William Woods University takes a strong stand against unlawful distribution of copyrighted music, movies and software. If a student is found to be distributing copyrighted material using any university computing resources, that person's network connection will be terminated and the student will be referred to the Office of Community Life. If the user* provides or obtains copyrighted files (music, videos, text, etc.) without permission from the copyright owner or their representative, the user* is in violation of federal and state copyright laws and the William Woods University Acceptable Use Policy.

By using programs such as Limewire, Kazaa or Morpheus file serving networks, or direct-connects that allow you to copy music or film to his/her computer, he/she may also be permitting the computer to become a "server" from which others can download the same file.

Running a server from a university building is a violation of the William Woods University Network Use Policy.

Network Service

Transferring large movie or music files may overload the network and degrade services. Transferring large files can slow the network making it less responsive or even unavailable to users*. Excessive network traffic can be generated, adversely affecting performance for other users*. William Woods University routinely monitors network usage patterns. Interfering with the ability of others to use the network services violates University policy and may result in termination of access to the university network services, and other disciplinary action.

***User is defined as all faculty, staff and students.**

Digital Millennium Copyright Act

The Digital Millennium Copyright Act (DMCA) of 1998 is a federal law that is designed to protect copyright holders from online theft — that is, from the unlawful reproduction or distribution of their works. The DMCA covers music, movies, text and anything that is copyrighted.

DMCA Violations

You could violate federal copyright law if:

- Somebody e-mails copyrighted material to you and, in turn, you forward it to one or more friends.
- You make an MP3 copy of a song from a CD that you bought (purchasers are expressly permitted to do so) but subsequently make the MP3 file(s) available on the Internet using a file-sharing network.
- You join a file-sharing network and download unauthorized copies of copyrighted material you want from the computers of other network members.
- To gain access to copyrighted material on the computers of other network members, you pay a fee to join a file-sharing network that is not authorized to distribute or make copies of the copyrighted material. You then download unauthorized material.
- You transfer copyrighted material using an instant messaging service.
- You have a computer with a CD burner that you use to burn copies of music you have downloaded onto writable CDs which you then distribute to your friends.

A simple rule of thumb to help you identify which materials are protected by copyright and which are not: If you would typically pay for it, then it is probably protected.

DMCA at WWU

If you are using WWU's computer network, the University is your registered Internet Service Provider (ISP). The DMCA requires ISPs to take down or block access to copyrighted materials in a timely fashion when notified that their customers are sharing copyrighted files.

Complaints typically arrive directly from software, music and motion picture associations, copyright holders and law firms. The University Information Technology Department disables

network access for the listed device and attempts to identify the owner to inform him or her about the complaint. If the owner believes the complaint to be inaccurate, they are given the opportunity to contest the finding.

If your network connection has been disabled, call the Help Desk at (573)592-4224. If you are informed that your connection has been disabled due to illegal file sharing or downloading, the steps below must be followed in order to have network access restored:

1. Sharing of all copyrighted materials as defined by the UIT Acceptable Use Policy and federal law must be stopped.
2. The UIT "Safe and Legal Computing on the Internet" course must be completed. After completing the course an agreement to cease sharing copyrighted materials is signed. Upon signing the agreement it is expected that any files currently being shared across the network will be removed.
3. The device will remain off of the WWU network for a minimum of two weeks.

Any future violations by the same person are forwarded to the Dean of Student Life for possible punitive action. Additionally, network access for students with multiple violations may be suspended for one semester on the second violation and forfeited permanently (on the third violation).

Any attempts to circumvent the disabling of network access are treated as a flagrant violation of policy and are forwarded to Dean of Student Life for punitive action.

For faculty and staff violations, departmental supervisors are notified. Repeat employee offenses may be referred to deans, department heads and/or department chairs.

Legal Repercussions for DMCA Violation

In addition to University penalties, DMCA violations may carry heavy civil and criminal penalties. For example, civil penalties include damages and legal fees. The minimum fine is $750 per downloaded file. Criminal penalties, even for first-time offenders, can be stiff: up to $250,000 in fines and five years in prison. Unless served with a subpoena as required under the DMCA, the University does not release the names of (or any personal information about) subscribers in the process of servicing a DMCA notice.

File-Sharing Programs: A Frequent Culprit in DMCA Violations

In many of the cases that UIT handles, violators claim to be unaware that they were distributing copyrighted works across the WWU network. This is due to the design of file-sharing programs such as Kazaa, BitTorrent and others. These programs can automatically make your computer

act like a server, causing copyrighted materials to be made available from your computer without your knowledge. In an effort to reduce the number of DMCA violations at WWU, access to all peer-to-peer sharing applications will be blocked campus wide.

If you have copyrighted material on your computer and need assistance removing it, call the UIT Help Desk at (573)592-4224.

For additional information regarding the DMCA, visit the Music United Web site.

Revised July 14, 2008

Drop off Form

Drop-In computing user agreement

UIT will work with students to get computers connected to the campus network. We use a web based system, TrustWave to protect our network from viruses and worms. TrustWave will not let you on the campus network if you do not have an updated antivirus product or Java installed.

These two steps will normally allow your computer to pass onto the campus network. If it does not, it generally means that one or more of the following are causing the problem:

1. Spyware infestation

2. Third-party software like AOL, Kazaa, Limewire etc.

3. Corrupt or illegal Windows installation

4. Hardware problem

If you bring your computer to the helpdesk, UIT will attempt to address some of these problems, but we cannot solve all of them. If you bring your computer to the helpdesk for us to work on, we may do any of the following:

1. Uninstall personal virus/security software – Norton, McAfee etc.

2. Uninstall personal Internet software – AOL, Netzero, Skype etc.

3. Uninstall other software that may cause spyware problems like file-sharing programs, torrent software etc.

4. Install spyware scanning software

5. Install virus detection software

6. Remove objectionable or problematic themes, wallpapers and screensavers.

In some cases, attempts to address these problems may cause corruption of the Windows operating system. If that is the case, the student will be responsible for addressing it. UIT is not

responsible for any software or hardware corruption these steps may cause. Often, the only solution in serious spyware infestations is to format and reinstall all software. UIT will NOT perform this task for any student. We recommend that any important files and software be backed up before bringing the computer to the helpdesk.

I understand and agree to all of the above.

Name (Printed)

_____

Date Signature

_____

Copyright in the Classroom

WWU follows the Fair Use provisions in US copyright law as determined by the WWU copyright policy. UIT offers several training sessions a year to WWU faculty, staff and students. If you would like someone to speak to your class or group on the topic, please contact us.

Copyright & the Online Class

The Technology, Education, and Copyright Harmonization (TEACH) Act, took effect in November 2002. Its purpose was to provide educators a framework for providing transmitted copyrighted works to their students at a distance.

The TEACH act requires that WWU disseminate accurate information regarding copyright. TEACH requires specific actions be taken by the administration, faculty, and information technology personnel for the university.

Administration is responsible for created and disseminating copyright policies to the appropriate faculty and staff. IT personnel are responsible for limiting storage and retrieval of copyrighted works. Faculty is responsible for ensuring the copyright compliance of the works they use in their classroom.

This site assists WWU with disseminating copyright policies, University Information Technologies provides a streaming server to meet the guidelines for limited storage and retrieval of information. Please contact Instructional Technology Coordinator for more information on the streaming server.

WWU provides the following information for faculty:

- What material is covered by the TEACH Act?
- What material is excluded from the TEACH Act?
- Instructor oversight responsibility.
- How to convert analog to digital.

The following works are specifically covered by the TEACH Act.

- Performances of nondramatic literary works;
- Performances of nondramatic musical works;
- Performances of any other work, including dramatic works and audiovisual works, but only in "reasonable and limited portions"; and

- Displays of any work "in an amount comparable to that which is typically displayed in the course of a live classroom session."

Fair Use guidelines apply to the works listed above.

The following are specifically excluded from the act:

- Works that are marketed "primarily for performance or display as part of mediated instructional activities transmitted via digital networks"; and
- Performances or displays given by means of copies "not lawfully made and acquired" under the U.S. Copyright Act, if the educational institution "knew or had reason to believe" that they were not lawfully made and acquired. The above section is specifically to preserve the market for educational media.

Instructor's Responsibility

The Act requires that faculty be an integral part of the distance education experience. It requires them to be responsible for the transmission of digital works that are an "integral part" of their class. The works must meet the following criteria:

- The performance or display "is made by, at the direction of, or under the actual supervision of an instructor";
- The materials are transmitted "as an integral part of a class session offered as a regular part of the systematic, mediated instructional activities" of the educational institution; and
- The copyrighted materials are "directly related and of material assistance to the teaching content of the transmission."

Converting analog to digital

Another issue covered by the TEACH act is when an instructor can digitize the content for online delivery. Digitized media must meet Fair Use criteria and be unavailable in digital format before an instructor can digitize a print or analog version.

The above information was compiled using the following resources. Many of them provide detailed analysis of the implications of the TEACH Act in the classroom as well as useful checklists if you have any questions about a resource.

Fair Use

The Fair Use section of US Copyright Law allows the use of copyrighted materials for non-profit use if you consider the following conditions. The full statute is here.

1. The purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
2. The nature of the copyrighted work;
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
4. The effect of the use upon the potential market for or value of the copyrighted work.

The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors.

WWU Copyright Policy

The Digital Millennium Copyright Act (DMCA) of 1998 is a federal law that is designed to protect copyright holders from online theft — that is, from the unlawful reproduction or distribution of their works. The DMCA covers music, movies, text and anything that is copyrighted. More importantly, the law involves you, because there is a good chance you might be breaking the law, even if you are not aware that you are. DMCA violations may carry heavy civil and criminal penalties. For example, civil penalties include damages and legal fees. The minimum fine is $750 per downloaded file. Criminal penalties, even for first-time offenders, can be stiff: up to $250,000 in fines and five years in prison.

Many of the cases that UIT handles, violators claim to be unaware that they were distributing copyrighted works across the WWU network. This is due to the design of file-sharing programs such as Kazaa, Limewire, BitTorrent and others. These programs can automatically make your computer act like a server, causing copyrighted materials to be made available from your computer without your knowledge.

If you have copyrighted material on your computer and need assistance removing it, call the UIT Help Desk at (573)592-4224. For additional information regarding the DMCA, visit the Music United Web site.