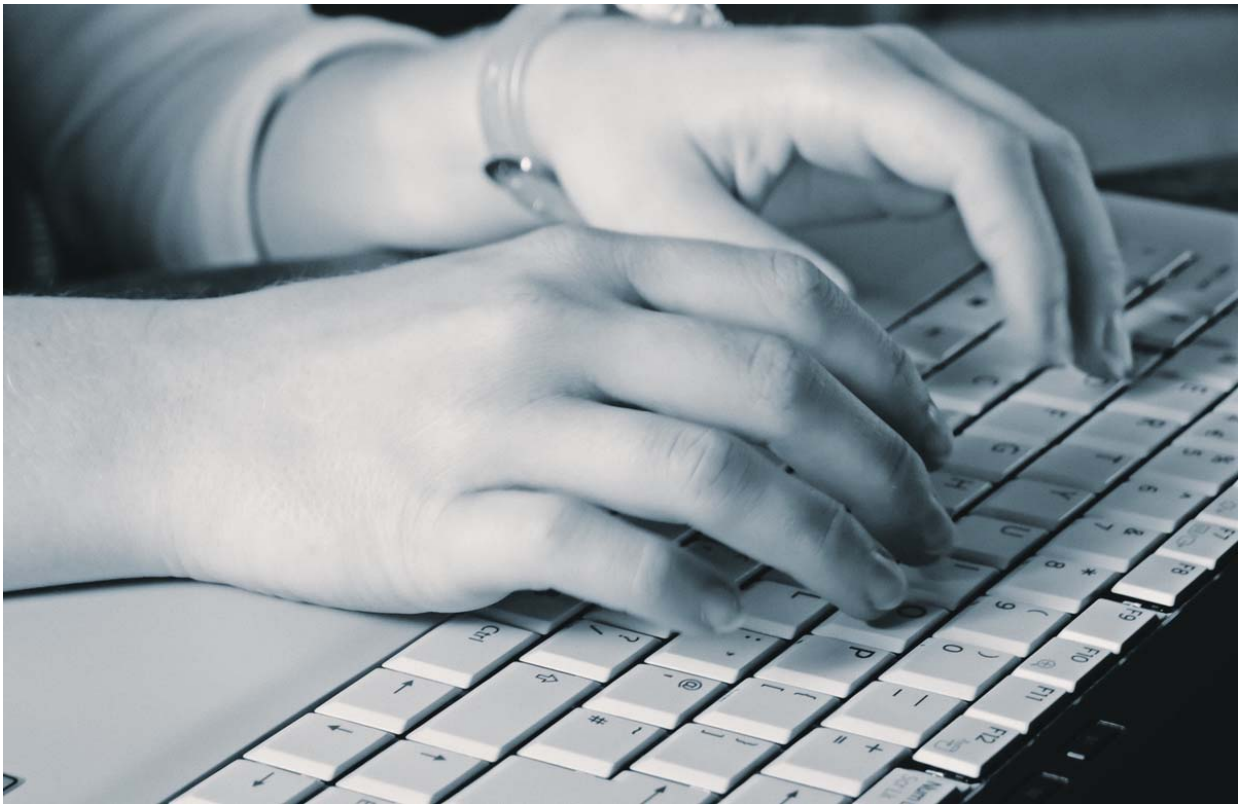

COMPUTER POLICIES

University Services

Concordia University Texas

2008

Rev. 0308

DEPARTMENT MISSION STATEMENTS

UNIVERSITY SERVICES

The mission of University Services is to provide and effectively maintain the physical plant, electronic infrastructure and campus security so that Concordia University Texas can accomplish its mission of developing Christian leaders.

UNIVERSITY SERVICES DEPARTMENTS –

A. INFORMATION & TECHNOLOGY SERVICES (ITS)

The mission of Information & Technology Services is to maintain appropriate and reliable computing and telecommunication systems and services for the conduct of education and business at Concordia University, including access to current software, hardware, computing resources, telephones, voicemail, and cable television along with appropriate training and maintenance.

B. FACILITIES MANAGEMENT

The mission of Facilities Management at Concordia University is to efficiently and effectively provide services that maintain the campus physical infrastructure in order to support the faculty, staff, and students in the process of developing Christian leaders and the pursuit of academic excellence.

C. CAMPUS POLICE

The mission of the Concordia University Police Department is to enhance the educational mission of the university by providing a safe and security campus environment through professional law enforcement services, safety programs and emergency management.

Table of Contents Page

COMPUTER POLICIES

University Services

Concordia University Texas

2008

1. BIBLICAL FOUNDATION

In His role as Creator, God the Father has blessed His people through a variety of spiritual and physical gifts. The crowning gift is salvation through the life, death and resurrection of His Son, Jesus Christ.

> **John 3.16** – *For God so loved the world that He gave His one and only Son, that whoever believes in Him shall not perish but have eternal life*.

In response to His undeserved grace, Christians strive to show their thankfulness and love by living lives that bring glory to God.

> **Matthew 5.16** – *Let your light shine before men, that they may see your good deeds and praise your Father in heaven.*

To facilitate Christian living, the Lord equips His people for active witness through a variety of resources.

> **Psalm 119.105 –** *Your word is a lamp to my feet and a light for my path.*
> **1 Peter 2.9** – *You are a chosen people, a royal priesthood, a holy nation, a people belonging to God, that you may declare the praises of Him who called you out of darkness into His wonderful light.* (*see also:* **Romans 12.6-10**)

Concordia University Texas is a Christian community dedicated to serving the Lord and preparing students to be Christian leaders in a complex, changing world. To help succeed in its mission, the University maintains an extensive electronic infrastructure to support both the academic and administrative functions of the school. Embracing its Christian heritage, Concordia Texas manages its computer networks and telecommunication systems to glorify God. To this end, the following policies and guidelines reflect the spiritual, ethical and moral foundation of the university. All users of the electronic infrastructure are expected to conduct themselves within the parameters outlined below, *driven by a desire to glorify the Lord*.

Access to electronic resources owned and operated by Concordia University Texas is a privilege. Concordia reserves the right to limit, restrict or extend access privileges to its computers, networks, and telecommunication systems, as it deems appropriate to fulfill its mission and remain faithful to its Christian principles. Those who knowingly infringe the policies outlined in this document may face loss of access and possible disciplinary action. In some cases, violation of policy may result in criminal prosecution under federal or Texas laws.

2. DEFINITIONS

Responsibility for managing and maintaining the electronic infrastructure at Concordia University Texas is delegated to **University Services**, which is divided into three departments:

- ✓ ***Information & Technology Services (ITS)***
- ✓ ***Campus Police***
- ✓ ***Facilities Management***

The following definitions apply to the policies and guidelines governing the electronic infrastructure of Concordia University Texas.

2.1 Electronic infrastructure – includes approved computers, networks, servers, telephones, and other similar devices that comprise the electronic infrastructure of Concordia University Texas. Networks shall mean and include video, voice, and data and all the ancillary hardware and software used to operate these systems such as routers, switches, firewalls, storage devices, and cabling. Telephones shall include the phone switch, voice mail, cabling, and all the ancillary hardware and software used to operate the telecommunication system.

2.2 Information Technology Asset – An approved system or systems comprised of computer hardware, software, networking equipment, and any data on these systems. Such assets include but are not necessarily limited to desktop computers, servers, printers, telephones, network lines, E-mail and web based services.

2.3 Electronic communication – includes the use of electronic infrastructure for communicating or posting information or material by way of video, voice or data such as electronic mail (email), instant messaging, weblogs (blogs), bulletin boards, listservs, chats, Internet access, phone calls, voice mail, and multimedia applications.

2.4 Authorized users – includes the following categories:

A. Current employees of Concordia University Texas(full and part time faculty and staff),
B. Current registered full and part time students of Concordia University Texas,
C. Any patron of the Library accessing the public resources of the Library Online Service (LOS), and
D. Others authorized by University Services to support the mission of Concordia University.

Authorized users, except for library patrons accessing LOS public resources, are required to have a user ID and password officially issued by Information & Technology Services.

2.5 User ID – includes the alphanumeric designation provided to an authorized user by Information & Technology Services for access to specific university computer and/or telecommunication systems. The user ID and initial password remains the exclusive property of Concordia University Texas and should NOT be shared with anyone, except designated personnel of ITS. Divulging user IDs and passwords violates *Texas Penal Code 33* (see *Section 4.3*) and could result in disciplinary action, removal, dismissal or criminal prosecution.

2.6 Access – Means the right to communicate with any Concordia University Texas electronic information resource including, but not limited to computers, computer networks, computer programs, computer and telecommunication systems, audio and/or video recordings, email, and other messaging systems for the purpose of conducting academic endeavors or official University business.

2.7 Malware – Means any set of computer instructions (commonly known as viruses, worms, Trojan horses, spyware, dishonest adware, etc.) that are designed to modify, damage, destroy, record, and/or transmit information within a computer system or network without the permission of the owner . The programs are malicious in nature in that they are designed to infect other computer programs or computer data; consume resources; deny or severely limit network traffic; modify, destroy, record or transmit data; or disrupt normal operation of a computer system or network.

2.8 Data – a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or process, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer printouts, magnetic storage media and optical storage media or may be stored internally in the memory of a computer or server.

2.9 Obscene material – is defined by U.S. Supreme Court guidelines as material that:

A. An average person, applying contemporary community standards, would find taken as a whole predominately appeals to the prurient interest or a shameful or morbid interest in nudity, sex, or excretion;
B. Depicts or describes in a patently offensive way sexual conduct specifically set out under the Texas Penal Code; and
C. Taken as a whole, lacks serious literary, artistic, political or scientific value.

NOTE: ***It is a federal crime to handle or possess child pornography in any manner.***

3. CONNECTIVITY

Concordia University Texas provides a variety of networks and electronic resources for use by employees and students to accomplish the mission of developing Christian leaders. Some of these networks and resources include –

- ✓ **CTXNet (Concordia University Texas Network) –** describes web-based resources designed for employee only access.
- ✓ **Banner** – the administrative computer system managed by the Austin Banner Council (ABC)
- ✓ **LOS** (Library Online Services) – an electronic public network accessible on and off campus providing educational material and resources based in the library
- ✓ **Computer labs** – computer labs are maintained in the various locations on campus
- ✓ **Email** – Email accounts are provided to all full-time employees and all full and part-time faculty
- ✓ **Internet access** – available through ports and wireless access points located throughout the campus and in all dormitory bedrooms
- ✓ **Intranet access** – the private internal network maintained for employees and students

- ✓ **WebCT** – a password protected course management system used as an online resource to enhance instruction and learning
- ✓ **University website** – located at: http://www.concordia.edu
- ✓ **Student centered website** – located at http://www.ctx.edu
- ✓ **MyInfo Online Self-Service –** located at http://myinfo.concordia.edu
- ✓ **PBX** – the main telephone switch for Concordia University Texas interconnecting all campus buildings to the phone system
- ✓ **Voicemail** – a computer system that records and manages voicemail for campus telephone users

4. APPROPRIATE USE OF ELECTRONIC RESOURCES

The following section outlines what is deemed appropriate and inappropriate use of the electronic infrastructure at Concordia. University Services maintains campus electronic systems to facilitate the mission and ministry of the school. These tools are meant to encourage exploration of God's creation, facilitate global communication and maintain the business functions of the University – with everything done to the glory of God. The following Bible passages illustrate the biblical foundation upon which Concordia operates its electronic infrastructure. Appropriate and inappropriate use of all campus electronic systems is guided by these theological precepts.

> **Philippians 4.8** – *Finally, brothers, whatever is true, whatever is noble, whatever is right, whatever is pure, whatever is lovely, whatever is admirable – if anything is excellent or praiseworthy – think about such things.*
>
> **Ephesians 5.1-4** – *Be imitators of God, therefore, as dearly loved children and live a life of love, just as Christ loved us and gave Himself up for us as a fragrant offering and sacrifice to God. But among you there must not be even a hint of sexual immorality, or of any kind of impurity, or of greed, because these are improper for God's holy people. Nor should there be obscenity, foolish talk or coarse joking, which are out of place, but rather thanksgiving.*
>
> **2 Corinthians 5.17** – *Therefore, if anyone is in Christ, he is a new creation; the old has gone, the new has come!*
>
> **John 8.31-32** – *If you hold to My teaching, you are really My disciples. Then you will know the truth, and the truth will set you free.*
>
> **Matthew 7.12** – *So in everything, do to others what you would have them do to you, for this sums up the Law and the Prophets.*

While it would be impossible to identify all the appropriate and inappropriate uses of the electronic infrastructure, the following lists some examples in both categories to guide users. University Services reserves the right to monitor electronic systems in order to maintain the integrity and security of all computer and telecommunication networks and assess observance of policies and guidelines.

4.1 Examples of appropriate use –

A. Using the electronic infrastructure in an effective, ethical, Christian and lawful manner to conduct official and authorized business activities of the University.

B. Using the electronic infrastructure to meet educational objectives and facilitate academic research and employee development.

C. Taking the necessary steps to protect and maintain the integrity and security of Concordia University computer equipment, networks, data, software, passwords and electronic facilities.

D. Maintaining the privacy of others – this includes, but is not limited to, abstaining from unauthorized access to email, computer programs and operating systems, data files, personnel information and student records

E. Adhering to U.S. copyright laws regarding software, data, intellectual property, and Internet resources. This applies to the work of authors and publishers of all media and encompasses respect for the right to acknowledgement, right to privacy and right to determine the form, manner and terms of publication and distribution.

F. Providing proper and honest identification in all electronic communication with Concordia University, maintaining valid, traceable identification if required by applications or servers within the University or in establishing remote access to the electronic infrastructure.

G. Faculty and staff can utilize the electronic infrastructure (telecommunications, email and Internet access) for limited personal usage, as long as the activity does not include any item prohibited in *section 4.2.1*.

H. Residential students can use the electronic infrastructure (telecommunications, email and Internet access) for personal communication, as long as the activity does not include any item prohibited in *section 4.2.1*.

4.2 Inappropriate use of the electronic infrastructure – Inappropriate use of the electronic infrastructure impedes the mission and ministry of Concordia University and can comprise the integrity and security of electronic systems. Unacceptable use of the electronic infrastructure falls into three general categories:

1. MISUSE OF SERVICE – *any action that interferes with or renders facilities or systems unusable to those who rely on them.* Examples: failure to observe posted or approved instructions and guidelines, unauthorized excessive use of resources and bandwidth, damage to software or hardware, posting inappropriate material on a web server, or sending inappropriate or unwanted email.

2. BREACH OF SECURITY – *any attempt to circumvent the protection that the University has in place to prevent unauthorized access to electronic equipment, systems or data; or any action which reduces the security of Concordia's electronic infrastructure.* Examples: attempts to misappropriate passwords, attempts to gain unauthorized access to networks and equipment or sharing passwords with others.

3. ILLEGAL USE – *any use of computer or network resources in the commission of an illegal act or crime.* Examples: violation of software licensing agreements, attempts to break into a computer, sending harassing or threatening email, possession of obscenity or child pornography and violation of the U.S. Copyright Act. Federal and state laws govern certain aspects of computer and telecommunications use. (See *Section 4.3*)

4.2.1 Examples of inappropriate use –

A. Attempting to modify or remove computers, software, telecommunication or peripheral equipment belonging to Concordia University without proper authorization.

B. Accessing computers, software, information or networks belonging to Concordia University without proper authorization from University Services. This includes taking actions that interfere with the proper operation of any electronic information or telecommunication network operated by Concordia University – including circumventing or disabling logon or other security measures employed by Information & Technology Services and Telecommunication Services.

C. Providing access to computers, software, information or networks belonging to Concordia University without proper authorization from University Services. This includes allowing friends, acquaintances, family member, or other unauthorized users access to hardware, software, or networks without proper authorization from ITS.

D. Transmitting (internal or external) unsolicited information containing obscene, indecent, lewd or lascivious material, or other material explicitly referring to sexual conduct.

E. Transmitting unsolicited information containing profane language, hatred, harassment, sexism or others forms of discrimination.

F. Communicating information concerning any password or user ID, identification code, personal identification number (PIN) or other confidential information, without the permission of its owner or University Services.

G. Creating, modifying, executing or retransmitting any computer program or instructions intended to obscure the true identity of the sender of email or electronic messages, including, but not limited to: forgery of messages or alteration of system or user data used to identify the sender of messages.

H. Violating any software license or copyright, including unauthorized copying or redistributing copyrighted software, without the written authorization of the software owner or producer.

I. Using electronic communication to harass or threaten users (on or off campus) in such a way as to create an atmosphere that unreasonably interferes with the education or the employment environment at Concordia University.

J. Using electronic communication to disclose proprietary information, without the explicit permission of the owner or producer.

K. Academic dishonesty or plagiarism.

L. Forging, fraudulently altering or falsifying, or otherwise misusing University or non-University records – including records, permits, identification cards, or other documents or property.

M. Using electronic communication to fabricate research data (academic and professional dishonesty).

N. Launching malware or distributing “spam” email or other nuisance electronic communication.

O. Downloading or posting illegal, proprietary or damaging material to a University computer or server.

P. Violating state or federal law in connection with gambling.

Q. Violating state or federal law in teaching or demonstrating the use or making of any illegal firearm, dangerous weapon, explosive or incendiary device capable of causing injury or death of another person.

R. Communicating any credit card number or other financial information or transactions, without the permission of its owner.

S. Using the electronic infrastructure to conduct political campaigning for candidates outside Concordia University Texas.

T. The following types of information or software cannot be placed on any University-owned computer system or on any system connected directly to the University electronic infrastructure:

U. That which infringes the rights of another person.

V. That which is abusive, profane or sexually offensive to the average person.

W. That which consists of information which may injure someone else and/or lead to a lawsuit or criminal charges. Examples include: libelous statements, pirated software, malware, pornographic material, or illegally used copyrighted images and information.

X. That which consists of any advertisements for commercial enterprises. Computer facilities at Concordia University cannot be used for personal or financial gain unrelated to a valid University function.

4.3 Legal considerations – In addition to the appropriate and inappropriate uses listed above, state and federal laws also apply to use of the electronic infrastructure at Concordia University Texas, especially through Internet access and email. In some cases, University Services may be required by law enforcement agencies or court order to provide information or assistance with investigations of illegal activity or behavior. It is the policy of the department to comply with state and federal regulations and law enforcement agencies.

4.3.1 Federal law *– It is a violation of federal law to intentionally:*

A. Access a computer without authorization to obtain classified information.

B. Access a computer without authorization to obtain financial records of a financial institution.

C. Access any U.S. Government computer without authorization if such conduct affects the use or operation of the government's computer.

D. Access a Federal computer without authorization with the intent to defraud.

E. Access a financial institution or U.S. Government computer without authorization and thereby alter, damage or destroy information which causes losses to others of a value exceeding $1,000 or more during any one year or which modifies or impairs medical diagnosis, treatment or care.

F. Traffic, with the intent to defraud, passwords or similar information which a computer may be accessed if the trafficking affects interstate commerce or the computer is used by the U.S. Government. The penalty can be a fine or as much as 20 years in a federal penitentiary for certain violations **(18 USCA Sec. 1030).**

G. Access, possess or distribute child pornography.

H. Breaking U.S. copyright laws.

4.3.2 Texas law – *It is a violation of Texas law to intentionally:*

A. Use a computer without the consent of its owner or to access data stored in a computer system without the consent of its owner or licensee if you know there is a security system intended to prevent your doing either of these things.

B. Give passwords, or similar confidential information about a computer security system to another person without the consent of the person employing the security system to restrict access to a computer or its data.

C. Cause a computer to malfunction or to interrupt operation of a computer system without the consent of its owner.

D. To alter, damage or destroy data or a computer program in a computer without the consent of the owner or licensee of the data or computer program. Convictions under the Computer Crimes section of the Texas Penal Code can result in a fine up to $5,000 and a jail sentence up to ten years **(7 Texas Penal Code, sec. 33).**

4.4 Sanctions – All individuals utilizing the electronic infrastructure owned and operated by Concordia University Texas are expected to comply with computer policies outlined in this document. While University Services desires that all users strive to honor the Lord through their words and actions, it is also the reality of sinful human beings that individuals will occasionally succumb to temptation and knowingly violate the policies governing the electronic infrastructure. In such cases, department policy is to follow the three-step approach articulated by Jesus in the following verses of Matthew 18.

> **Matthew 18.15-17 –** *If your brother sins against you, go and show him his fault, just between the two of you. If he listens to you, you have won your brother over. But if he will not listen, take one or two others along, so that every matter may be established by the testimony of two or three witnesses. If he refuses to listen to them, tell it to the church; and if he refuses to listen even to the church, treat him as you would a pagan or a tax collector.*

In the course of monitoring electronic systems, should University Services personnel discover inappropriate activity or behavior on any system owned and operated by the school the following three-step approach will be utilized.

- ✓ **Step 1** – The individual(s) will be notified by University Services of the inappropriate activity or behavior and be asked to comply with school policy.
- ✓ **Step 2** – If the activity or behavior continues, University Services will share the information with the appropriate supervisor or vice president to whom the individual(s) is responsible. The supervisor or vice president will be responsible for discipline at this stage.

- ✓ **Step 3** – Should the activity or behavior persist, University Services will share the information with the University president for disciplinary action. Continued violation of usage standards outlined in this document may result in the loss of network access or telecommunication privileges, disciplinary action, fine or loss of pay, suspension or dismissal from the University, civil liability and/or criminal prosecution.

NOTE: *An exception to this process may be made should the activity or behavior be life-threatening, endanger or threaten the life of another person or violate state or federal law. In such cases, University Services may take the situation directly to the University president or the appropriate law enforcement agency.*

5. DATA MANAGEMENT

5.1 Data management and maintenance – In the course of maintaining the electronic networks of Concordia University Texas, authorized personnel from University Services are required to access files or data stored on servers and computers. These activities include testing systems to ensure data integrity, network security, and proper performance of equipment along with regular system backups. Department personnel are prohibited from exceeding their access privileges or making use of individual user files or data for any purpose other than repair or maintenance services. Any staff member violating this policy will be immediately dismissed.

DISCLAIMER: *Users need to understand that no electronic resource (especially email) is completely private. Email, for example, is comparable to sending a postcard through the U.S. Postal Service – anyone can read the information along the delivery path. Messages sent via email transverse other public and private networks over which the University has no authority or control. Such messages may be broadcast or duplicated by a recipient without the permission of the sender. Just as with printed documents, the University owns and backs-up for disaster recovery purposes digital communication, data and information residing on University owned systems through its departments and organizations. Concordia University Texas considers static digital files and dynamic digital streams to be private and does not disclose their contents, except as required by contractual obligation, state or federal law or when it violates the policies outlined in this document.*

5.2 File and data monitoring – The president of Concordia University Texas or the vice president of University Services may authorize department personnel to monitor the activities of a specified account or computer system and to search electronic data stored in a user account or database if:

A. The University has reasons to believe that a user account or system security has been breached and is being illegally used by someone other than the authorized user,

B. The University has received a legitimate complaint with sufficient evidence that an account or electronic system is being used to gain unauthorized access or to attempt to gain unauthorized access to a network or electronic resource, or

C. The University has legitimate reason to believe that an account or electronic system is being used in violation of school policy, federal or state law.

The authority for this type of monitoring or search must be requested on an account-by-account basis. Any monitoring will be restricted to the specified account or system involved. If this search provides evidence of violation of University policy or federal or state laws, the department will follow the disciplinary steps outlined in *Section 4.4*.

5.3 Electronic Communication Storage and Retention – Information and Technology Services (ITS), on behalf of Concordia University Texas, does not actively archive incoming and outgoing email, Instant Messaging (IM) conversations, or any other forms of electronic communication. Due to the evolving nature of electronic communication beyond basic email and text into imaging, voice, video, and web-based conferencing, it is unreasonable (both physically and fiscally) to provide a wide array of archiving services for the University. As a result, the longevity of these and similar communication records cannot be guaranteed by the Concordia University Texas.

Electronic correspondence may be considered official University records and as such the property of Concordia University Texas. Official University correspondence should be maintained in accordance with applicable document retention policies. It is the responsibility of the user to preserve and retain these unaltered records in an appropriate manner.

Email users have the ability to archive email through Microsoft Outlook. Those who wish to keep electronic communication records for an extended period of time must archive their own data. However, users should be cautioned in relying upon the long-term access to archival data as electronic standards and formats change over time.

Information and Technology Services performs routine backups of all mission critical systems which includes email and may include other types of electronic communication stored on University servers. However, backups are performed only to assure system integrity, reliability, and for disaster recovery. Backups are not performed for future document retrieval. The ability to provide future retrieval from system backups is purely coincidental.

In some circumstances, users may be required by civil action to retain and store currently available electronic data and communication in compliance with E-Discovery, the process by which Electronically Stored Information (ESI) is exchanged during the early stages of litigation. Users must comply with requests for ESI and comply with the processes and procedures to secure the data as specified by Concordia University Texas.

6. PRIVACY, OWNERSHIP RIGHTS & FREEDOM OF EXPRESSION

University Services strives to preserve and protect the privacy of all users of the electronic infrastructure owned and operated by Concordia University Texas. When systems function properly, users can expect the files and data they generate to be private information, unless the creator of the file or data takes action to reveal it to others. However, users should be advised that no electronic information or telecommunication system is completely secure. Individuals both within and outside the University may find ways to illegally access files. Users are advised to utilize any University system at their own risk.

6.1 Freedom of expression – All existing guarantees of freedom of speech and expression under the Constitution of the State of Texas and the First Amendment to the U.S. Constitution are extended to those who use the electronic infrastructure of Concordia University Texas. However, the school recognizes that there are legal limitations that can be imposed on these freedoms, such as, but not limited to:

- ✓ Reasonable time, place, and manner restrictions
- ✓ Invasion of privacy
- ✓ Obscenity
- ✓ Inciting or producing imminent lawless action
- ✓ Threats of violence or terrorism
- ✓ Disruption of the academic environment
- ✓ Fighting words
- ✓ Vulgar, rude and offensive speech
- ✓ Sexual and racial harassment

While University Services strives to protect the freedom of speech and expression of all electronic infrastructure users, it is important to realize that there are services available through the Internet that may be considered offensive to some. Users take responsibility for their own navigation of off-campus electronic resources. Should it become necessary to limit or restrict access to certain electronic sites or resources, University Services will do so within the parameters of the First Amendment and the U.S. Constitution.

6.2 Intellectual property rights – Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in electronic environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, are grounds for sanctions against any user of the electronic infrastructure owned and operated by Concordia University Texas. All users are responsible for recognizing (attributing) and honoring the intellectual property rights of others. *See also the Concordia University Texas Employee Handbook.*

6.3 Harassment – No user may, under any circumstance, use any electronic information or telecommunication system, equipment, or network owned and operated by Concordia University Texas to libel, slander, or harass any other person or entity. The following shall constitute electronic harassment:

A. Intentionally using electronic equipment to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other material or threats of physical harm to the recipient or the recipient's immediate family;

B. Intentionally using electronic equipment to repeatedly contact another person with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;

C. Intentionally using electronic equipment to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he/she desires such communication to cease (such as debt collection);

D. Intentionally using electronic equipment to disrupt or damage the academic, research, administrative, or related pursuits of another person; and

E. Intentionally using electronic equipment to invade or threaten to invade the privacy of another person or entity (e.g. personal records, data files, voice mail, etc.).

Anyone using the electronic infrastructure of Concordia University to harass another person or entity will face appropriate disciplinary actions as outlined in *Section 4.4.* Note: *harassment may lead to the involvement of law enforcement agencies and civil or criminal prosecution.*

7. GAMES & ENTERTAINMENT

Playing electronic games and accessing entertainment electronically is discouraged for employees of Concordia University Texas. The electronic infrastructure owned and operated by the University is solely intended for conducting University business.

Residential students housed in University dormitories are permitted to play electronic games and access appropriate entertainment through the Internet within the constraints of available network bandwidth and in conformity to the computer policies articulated in this document. Information & Technology Services monitors the effects these activities have on network performance and periodically blocks or manages sites that substantially slow network performance.

Playing electronic games, using computers to access entertainment over the Internet, and participating in online chats (e.g. instant messaging or Internet chat rooms) is prohibited on workstations in University public computing facilities – the library (Building F) and all computer labs. Equipment in these areas is restricted to academic and University business use only. Individuals violating this policy can have their user access revoked.

8. SOFTWARE

Software enables people to accomplish a variety of tasks with computers and other electronic equipment. Concordia University allocates a portion of its annual budget to purchase software for use on campus computers and the electronic infrastructure. Information & Technology Services maintains licensing agreements with a variety of vendors to provide multiple copies of computer programs at reduced rates. Unfortunately there are individuals who make and use unauthorized software copies. This is known as “pirating” and is NOT condoned in any way by Concordia University Texas.

Unauthorized copying of software –

- **Is illegal!** *Copyright law protects software authors, producers, and publishers – just as patent law protects inventors (Title 17 of the U.S. Code). Violating copyright law is a federal crime and can lead to fines and imprisonment.*

- **Jeopardizes the University!** *The institution may incur legal liability for proliferation of pirated software on campus.*
- **Is stealing!** Making illegal copies of software deprives publishers and developers of a fair return for their work, increases prices, reduces the level of future support and enhancements and can inhibit the development of new software products. Theologically it breaks the Seventh Commandment – *Thou shall not steal (Exodus 20.15 & Deuteronomy 5.19).*

As an academic community, Concordia University Texas values the free exchange of information and ideas. Such an exchange is the essence of education. But just as the University does NOT tolerate plagiarism, Concordia University Texas does NOT condone any illegal copying or distribution of software – including programs, applications, databases, computer code or manuals.

8.1 Software classification – In terms of copyright, there are four broad software classifications:

- Commercial
- Shareware
- Freeware
- Public domain

The restrictions and limitations regarding each classification are different as noted in the following descriptions.

8.1.1 Commercial software – represents the majority of software purchased from publishers, commercial computer stores, etc. When software is legally purchased, the buyer acquires a license to USE it – NOT own it. The license is granted from the company that owns the copyright. The conditions and restrictions of the license agreement vary from program to program and should be read carefully. In general, *commercial software* licenses stipulate that:

A. U.S. copyright laws cover the software.

B. Although one archival copy of the software can legally be made, the backup copy cannot be used, except when the original program is damaged or destroyed.

C. Modifications to the software are not permitted.

D. Decompiling (reverse engineering) of the program code is not allowed without the permission of the copyright holder. Computer code is protected under U.S. Copyright laws.

E. Development of new works built upon the program (derivative works) is not allowed without the permission of the copyright holder.

8.1.2 Shareware – this is also software covered by copyright law. When software is acquired under a "shareware" arrangement, an individual is actually acquiring a license to use it – NOT own it. The license is acquired from the individual or company who owns the copyright. The conditions and restrictions of the license agreement vary from program to program and should be read carefully. The copyright holder for shareware allows purchasers to make and distribute copies of the software, but expects payment after the user tests the software and decides to keep it. In general, *shareware* software licenses stipulate that –

A. U.S. copyright laws cover the software.

B. Although one archival copy of the software can be made, the backup copy cannot be used, except when the original program is damaged or destroyed.

C. Modifications to the software are not allowed.

D. Decompiling (reverse engineering) of the program code is not allowed without the permission of the copyright holder.

E. Development of new works built upon the program (derivative works) is not allowed without the permission of the copyright holder.

Selling software as *shareware* is a marketing decision – it does not change the legal requirements with respect to copyright. That means an individual can make a single archival copy, but is obligated to pay for all copies adopted for use.

8.1C Freeware – is also covered by copyright law and subject to the conditions defined by the copyright holder. The conditions for freeware are in direct opposition to normal copyright restrictions. In general, freeware software licenses stipulate that:

A. U.S. copyright laws cover the software.

B. Copies of the software can be made for both archival and distribution purposes – but distribution CANNOT be for profit.

C. Modifications to the software are allowed and encouraged.

D. Decompiling (reverse engineering) of the program code is allowed without the permission of the copyright holder.

E. Development of new works built upon the program (derivative works) are allowed and encouraged with the condition that derivative works must also be designated as freeware.

This means that an individual user can take *freeware*, modify or extend it, but CANNOT sell it as commercial or shareware software.

8.1D Public domain – software to which the original copyright holder explicitly relinquishes all rights. Since under current U.S. copyright law, all intellectual works (including software) are protected as soon as they are committed to a tangible medium, for something to be *public domain* it must be CLEARLY MARKED as such. Before March 1, 1989, it was assumed that intellectual works were NOT covered by copyright unless the copyright symbol appeared on the work. With the U.S. signing the Berne Convention, this presumption has been reversed. **Now all works assume copyright protection unless the public domain notification is stated**. This means that for *public domain* software:

A. Copyright protection has been relinquished.

B. Copies can be made for both archival and distribution purposes with no restrictions.

C. Modifications to the software are allowed.

D. Decompiling (reverse engineering) of the program code is allowed.

E. Development of new works built upon the program (derivative works) is allowed without the permission of the copyright holder and without conditions on the distribution or use of the derivative work.

8.2 Possession and return of software – Software purchased by Concordia University Texas, either individually or under a licensing agreement, is limited for use on computers and equipment owned or leased by the University. Software inventories are maintained by Information & Technology Services. When an individual leaves Concordia University Texas by graduation, retirement, resignation or dismissal, any software owned by the University must either be returned to ITS or destroyed. In addition, any University equipment must also be returned – such as computers, laptops, monitors, printers, telephones, etc. Any software or equipment not returned will be treated as theft from the institution and the individual will be subject to prosecution under Texas law.

9. ACCESS & SECURITY GUIDELINES

Concordia University Texas provides access to its electronic infrastructure for users in the following categories:

A. Current employees of Concordia University Texas (full and part time faculty and staff),

B. Current registered full and part time students of Concordia University Texas,

C. Any patron of the Concordia University Library accessing the public resources of the Library Online Service (LOS), and

D. Others authorized by University Services to support the mission of Concordia University Texas.

Authorized users, except for library patrons accessing LOS public resources, are required to have a user ID and password officially issued by Information & Technology Services.

9.1 Unauthorized access – Authorized users of electronic information and telecommunication systems at Concordia University Texas are required to work within specific parameters. Employees are granted access to different parts of the administrative computer system, depending on job descriptions and officially assigned tasks. Students are prohibited from accessing administrative systems or databases, except as authorized by Concordia University Texas.

Unauthorized access includes:

- ✓ Damage to computer systems or equipment
- ✓ Obtaining access to unauthorized programs, databases or equipment
- ✓ Depriving an authorized user from access to authorized resources or equipment

By using knowledge of:

- A special password
- Loopholes or “backdoors” in computer security systems.
- Another user’s password.
- Access abilities gained during a previous position at the University.

All users are not permitted to circumvent or subvert any system security measures put in place by University Services to manage and protect the campus electronic infrastructure. All users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information. Deliberate attempts to degrade the integrity and performance of any portion of the electronic infrastructure or to deprive authorized personnel access to any system or network is prohibited and will result in appropriate disciplinary action or criminal prosecution under the policies in *Section 4.4.*

9.2 Termination of access – A user will automatically lose access privileges to University networks and electronic systems when they cease being a member of the campus community.

A. **For students –** through transfer to another school, withdrawal, suspension or graduation.

   Note: This does not affect access to public resources available through the library, unless authorized library personnel have denied the student access.

B. **For employees** – termination or accepting a position outside the institution.

   Note: This does not affect access to public resources available through the library, unless authorized library personnel have denied the employee access.

   Loss of access to University networks and systems for an employee is a complex issue and may warrant special action on a case-by-case basis. Depending on security concerns and work responsibilities, ***network access may be terminated immediately upon dismissal or release of an employee***. In such a case, Information & Technology Services will immediately suspend access to all university networks for that individual, erase the user ID and password, and impound all email and personal files on servers and individual computers associated with that individual. The immediate supervisor or respective vice president will be responsible for permitting any further access to personal files. If such access is permitted, the respective supervisor or vice president along with a representative of Information & Technology Services must supervise it. This is meant to protect network and data integrity. In some situations, termination of employment may result in removal of the hard drive from an individual computer to prevent future sabotage or disruption of University business. If a former employee makes any attempt to break into any portion of the electronic infrastructure operated by the University, criminal charges may be filed with appropriate law enforcement authorities. Hacking into or unauthorized tampering or interference with the operation of any computer or computer system is a crime under *Texas Penal Code (Section 33).*

   Employees who retire from Concordia University Texas can maintain their network access (email account and personal website). They are required to observe all computer policies. In most cases, University equipment will need to be returned to ITS upon retirement.

9.3 Contact by law enforcement representatives –
Any user contacted by a representative from a law enforcement agency (e.g. FBI, Austin Police Department, District Attorney's Office, etc.) or publishing company conducting an investigation of any alleged violation involving Concordia University Texas computer, network or telecommunication systems, must inform the vice president of University Services and the Campus Police Chief immediately.

9.4 Storage of Personally Identifiable Information

No university employee is allowed to store, either temporarily or permanently, ***Personally Identifiable Information*** (PII) regarding university employees or students in electronic format on University supplied desktop or laptop computers, CD-ROMs, flash drives or other removable media formats. All such information should be stored within the individual user or department ***network storage folder*** (also known as the H-drive). Banner users should daily purge browsers of files in temporary storage. Unknown to the user, data extracts from Banner may be stored in the browser cache.

Personally Identifiable Information is considered any data capable of specifically identifying a student or employee (and their associated personal records and confidential information) that has not been declared by the University as "directory information" with regards to FERPA (**Family Educational Rights and Privacy Act)**. Examples of this would include Social Security numbers, bank account information, driver license information, credit card information, etc.

This policy also applies to any other electronic information which would be considered confidential and critical to Concordia University Texas.

In the rare case where an employee has a legitimate, temporary need to store such information on removable media or a desktop or laptop computer, the employee is responsible for gaining supervisor approval to do so, and must have ITS set up a ***properly encrypted folder*** in the temporary location for data storage.

9.5 Securing Personal Identifying Information

The following Policy verbiage is taken from State Bill 122 – Sec. 48.102 (BUSINESS DUTY TO PROTECT AND SAFEGUARD SENSITIVE PERSONAL INFORMATION) and modified for Concordia University Texas application.

Concordia University Texas departments and personnel shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by Concordia University in the regular course of business.

Concordia University Texas staff and faculty shall destroy or arrange for the destruction of student and constituent records containing sensitive personal information within the University's custody or control that are not to be retained by Concordia University by:

A. Shredding;
B. Erasing; and/or
C. Modifying the sensitive personal information in the records to make the information unreadable or undecipherable through any means.

In this section, "breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person. Good faith acquisition of sensitive personal information by an employee or agent of Concordia University Texas for the purposes of the person is not a breach of system security unless the sensitive personal information is used or disclosed by the person in an unauthorized manner.

Concordia University Texas conducts business in the State of Texas and owns or licenses computerized data that includes sensitive personal information, and thereby shall disclose any breach of system security, after discovering or receiving notification of the breach, to any person whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made as quickly as possible, except as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

It is the responsibility of the staff and faculty of Concordia University Texas to notify Information and Technology Services immediately of any suspected data breach as outlined in section 8.6.

If Concordia University Texas maintains computerized data that includes sensitive personal information that the University does not own shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Concordia University Texas may delay providing notice as required at the request of a law enforcement agency that determines the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines it will not compromise any investigation. Concordia University Texas may give notice as required by providing:

A. Written notice, and/or
B. Electronic notice, if the notice is provided in accordance with Federal Law (15 U.S.C. Section 7001)

If Concordia University Texas demonstrates the cost of providing notice would exceed $250,000, or the number of affected persons exceeds 500,000 or the university does not have sufficient contact information, the notice may be given by:

A. Electronic mail, if the person has an electronic mail address for the affected persons;
B. Conspicuous posting of the notice on the Concordia University Texas website; or
C. *Notice published in or broadcast through major statewide media.*

If Concordia University Texas is required to notify at one time more than 10,000 persons of a breach of system security, the University shall also notify, without unreasonable delay, all consumer reporting agencies maintain files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.

9.6 Security Response –

Due to privacy issues and the possibility of identity theft, it is imperative that a formal reporting and response policy be followed when responding to security incidents. The following policies and procedures are to be used by Concordia University Texas faculty, staff and students to report any potential security incidents. The policy also outlines the appropriate response by Information and Technology Services staff.

A SECURITY INCIDENT IS DEFINED AS –

A. An occurrence that potentially violates Federal law, Texas law, or Concordia University Texas policy;

B. intentional or unintentional breach or attempted breach of any Concordia University Texas technology asset, whether emanating from inside or outside the Concordia network;

C. Malware; or

D. Any conduct using a Concordia University Texas technology asset which could be construed as dangerous, threatening, harassing or in violation of Concordia University Texas policy.

REPORTING A SECURITY INCIDENT

Information and Technology Services staff must be notified immediately of any security incident involving a Concordia University Texas technology asset. All "suspected" security threats must also be reported to Information and Technology Services immediately. If it is unclear a situation is a security threat, Information and Technology Services personnel should be contacted to help assess any potential response.

Any theft or loss of a technology asset from or by Information and Technology Services should be considered a security threat if the asset contains a hard drive or other memory device or media that may contain data.

The following action should be taken by staff, faculty and students when a security incident is suspected:

- *All hardware involved in the incident should be immediately removed from the network by disconnecting network cables and disabling wireless devices.*
- *Do NOT shutdown or restart the computer.*
- *The computer or hardware device should remain on with all current programs left running. Do not alter the computer in any way.*
- *Report the security incident.*

Contact Details – Security incidents should be immediately reported to Information and Technology Services staff. ITS staff will determine the appropriate response.

- ✓ Primary contact: **Stan Kruse – 512-313-4002**
- ✓ Secondary contact: **DeWayne Mangan – 512-313-4003**

Document all information while waiting for Information and Technology Services staff to respond. This should include the date, time, and nature of the incident, possible data compromises, and approximate length of exposure or compromise. All information can aid in the response, troubleshooting and investigation of the situation.

RESPONSE

Information and Technology Services staff will first determine the severity of the incident and then plan and implement an appropriate response. In cases where an incident is not deemed severe, the issue will be assigned to the appropriate support area for troubleshooting and correction. For severe breaches of security that compromise data and possibly expose personal identifiable information, the Vice President of University Services will be formally notified, and along with appropriate authorities. A formal response may range from getting a critical system back online, gathering evidence, taking appropriate action against individual(s), and/or notifying appropriate Internet Service Providers (ISPs) or other third parties of inappropriate activity originating from their network.

10. UNIVERSITY WEBSITE & EMAIL COMMUNICATIONS

University Services maintains an official website on the Internet for Concordia University Texas. The official web address is: *http://www.concordia.edu*. A student home page is maintained by Concordia University at: *http://www.ctx.edu*. The dynamic nature of the Internet makes it difficult to anticipate all the different problems and challenges surrounding management of the Concordia website. As a result, the following policies are broad-based and will continue to evolve as circumstances warrant

10.1 Homepage & CTX website – Information & Technology Services employees a full time webmaster to manage the homepage and website for Concordia University Texas. The site is an OFFICIAL document of the University that represents the corporate interests of the entire campus – not the views of any particular individual or group. As a result, the documents that comprise the Concordia website must be formatted to the standards set forth by Information & Technology Services through its webmaster and comply with all federal, state, and local laws and regulations, including laws related to accessibility, copyright, obscenity, libel and privacy. Photographs and documents contained on the official University website are the exclusive property of Concordia University Texas.

10.2 Content – All material posted or linked to the Concordia website must be consistent with the mission of the University and comply with the ethical, theological and moral standards of the institution as well as state and federal laws. The Concordia webmaster will apply these standards to any information or images submitted for posting or linking to the website. Departments with content editors and direct access to specific pages are expected to apply these standards at all times. Information, images or links deemed inappropriate will not be posted. Any employee may become a website content editor with the recommendation of the supervising vice-president. New content editors must be trained by Information and Technology Services personnel before editing access is granted.

10.3 Accuracy of information – Considerable effort goes into preparing and managing the online resources of the University homepage. However, Concordia University Texas and its agents shall not be held liable for any damages, however caused, by errors or omissions that may occur in the preparation and posting of documents on the University website. All parties posting or submitting for inclusion material and information on the Concordia website represent and warrant that the submission, installation, copying, distribution, and use of such material in connection with the website does not violate copyright law or property rights of any individuals. Any claims against the University for copyright infringement are the responsibility of the individual user posting the content.

10.4 Domain names: On the Internet, a domain name provides a direct link to a website registered with the domain name system (DNS). The DNS translates the name to an IP address where the website or similar content is located. In practice domain names consist of levels separated by periods. As an institution of higher education, Concordia University Texas uses the *edu* top-level domain. Concordia owns two second-level domains, *concordia.edu* and *ctx.edu*. Third- and higher-level domains, also known as subdomains, are also used by Concordia for various purposes (*myinfo.concordia.edu, webct.ctx.edu,* etc.).

All websites that conduct the official business of Concordia University Texas must contribute positively to the overall mission of the university. All content must exhibit the highest standards of professionalism and be conveyed in a manner worthy of an institution of higher learning. All websites must prominently identify the connection to Concordia University Texas and be registered and approved by ITS on behalf of the university.

Subdomains within the ctx.edu and concordia.edu second-level domain names may be requested through ITS. subdomain requests that are approved and registered meet the following criteria:

- The requesting department expects to use the subdomain on a permanent on-going basis. Use for services provided for a limited time will not be approved.
- The name is a word or abbreviation that is widely known within the university community.
- The name is a unique identifier for the entity and would not be confused with another university department or organization or with an outside entity (*med.concordia.edu* would be declined for the Masters of Education because it could be interpreted as *medical*)
- The name does not violate copyright or trademark laws. (m*icrosoft.concordia.edu*)
- The subdomain is useful for promoting and marketing university programs.
- The subdomain is useful for a significant portion of the university, not just a small subset (*skating.concordia.edu*)

In general, all university business on the Internet should be within the *concordia.edu* or *ctx.edu* domains. Using the *concordia.edu* or *ctx.edu* domains provides a consistent web presence and ensures the highest ranking in Internet search queries. Domains outside of the two official domains must be owned and maintained by ITS. In practice, the outside domain names should always redirect to pages within the *edu* domains. In some instances, domain names outside the Concordia namespace (concordia.edu and ctx.edu) may be appropriate. Reasons include:

- For use in collaboration with an outside entity. Using an independent namespace may be appropriate to show the nature of the collaboration.
-

10.5 Email – Email accounts are provided to all employees using Microsoft Exchange Server. All email messages are considered official communications of Concordia University Texas. As such, users should use discretion in sending messages that may be deemed personal. Users are expected to monitor and respond appropriately to all email communication in a timely manner. Users should also maintain appropriate email etiquette. While electronic text communication has digressed into a combination of actual words and chatspeak (lol, bcuz, 2nite, u r, etc.), employees and students associated with Concordia University Texas are expected to maintain the highest quality of spelling and grammar in all forms of communication.

Retention and archiving of email is the responsibility of the user and should follow department document retention guidelines (See Section 5.3).

Information & Technology Services will create email lists to segments of the faculty and/or staff with the approval of the supervising vice-president. Once created, the management of the email list will be the responsibility of the appointed moderator. The moderator must follow Information and

Technology Services email list guidelines. Only one moderator will be allowed per list. Mass emailing to large groups must be done through approved distribution lists. Users who violate this policy will be given one written warning from the director of Information and Technology Services. A second violation will result in the user being restricted to no more than three addresses per email message.

The use of email lists is restricted to messages directly related to official University business. The message must be pertinent to all users contained in the email list. News, event announcements, invitations, etc. should be sent via scheduled newsletters.

The *All Faculty*, *All Students* and *All Staff* lists are moderated by the President's Office and the Administrative Council or their appointed moderators. Each member of the Administrative Council may appoint one moderator with the approval of the whole Administrative Council. Appointed moderators work in the stead of the Administrative Council member, not in addition to.

11. PASSWORD MANAGEMENT

Information handled by electronic systems must be adequately protected against unauthorized modification, disclosure or destruction. Effective controls for access to electronic data minimize inadvertent employee error and negligence, and reduce opportunities for computer crime. Most users of the electronic infrastructure at Concordia University Texas are assigned a unique personal user identification. The user ID is authenticated before the system or network grants access to the user.

11.1 Password Selection

Passwords are used to authenticate a user's identity and to establish accountability. A password that is easily guessed is a bad password that compromises security and accountability. Computer hackers are extremely sophisticated. Instead of typing each password by hand, hackers use personal computers and automated programs to dial into networks trying different passwords. If the system disconnects them, the program dials back in and tries another password – automatically. Instead of trying every combination of letters, starting with AAAAAA (or whatever), hackers use hit lists of common passwords such as *WIZARD* or *DEMO* or *DEFAULT*. Even a modest home computer with a good password-guessing program can try thousands of passwords in less than 24 hours. Some hit lists used by hackers contain several hundred thousand words. Therefore, a password that might be easily guessed is a bad choice.

11.2 Guidelines for choosing a password –

- ✓ Use both uppercase and lowercase letters if the computer system considers an uppercase letter to be different from a lowercase letter when the password is entered.
- ✓ Include digits and punctuation characters as well as letters.
- ✓ The Concordia University Texas network logon follows a "three-out-of-four" policy for passwords. The password must contain *at least three (3) of the following types of characters*:

uppercase letter, lowercase letter, number, special character (punctuation, bracket, parenthesis, etc.). [September 2008 implementation]

- ✓ Choose something easily remembered so it does NOT have to be written down.
- ✓ Network passwords must be at least eight (8) characters. Password security is improved slightly by having longer passwords.
- ✓ It should be easy to type quickly so someone cannot follow what was typed by watching the keyboard.
- ✓ Use two short words and combine them with a special character or number and intersperse uppercase letters, like *RoboT4Me* or *Eye-coN*.
- ✓ Put together an acronym that has special meaning to you, like N0tfsW (None Of This Fancy Stuff Works) or Avp3gcaN (All VAX Programmers Eat Green Cheese At Night). Also notice the use of numbers in place of letters. Zero for an "O", three for an "E" or one for an "I" are some examples.
- ✓ Network passwords expire after three (3) months. Users will be notified two (2) weeks in advance of a pending expiration. Users may change passwords at any time. Once the password expires, users will be required to change it to access the network or email.
- ✓ Never use a date, especially birthdays, anniversaries, etc., as a password or PIN.

11.3 Handling passwords

Never write down a password! Users must not write passwords on desk calendars, Post-It notes attached to a computer or on the pullout drawer of a desk. Memorize passwords! It is more secure because there is less opportunity for another person to discover the password and memorize it. A password that must be written down in order to be remembered is likely a password that is not going to be guessed easily.

If a user must write down a password, follow a few precautions:

- ✓ Do not identify the password as being a password.
- ✓ Do not include the name of the account or user ID on the same piece of paper upon which the password is written.
- ✓ Do not attach the password to any part of a computer.
- ✓ Mix in some "noise" characters or scramble the written version of the password in a way that you remember – making the written version different from the real password.
- ✓ Never record a password online and never send a password to another person through email.
- ✓ Change passwords monthly!

Users must only use their appointed user accounts. The sharing of accounts or passwords is strictly prohibited and is considered a severe breach of security. Violators will be subject to disciplinary action.

Users who suspect that an account has been compromised or logon information may be known by others must immediately change their password and contact Information and Technology Services. ITS will determine an appropriate response as outlined in Section 9.6.

12. APPENDIX A – Copyright & Intellectual Property

Concordia University strives to protect copyright and intellectual property rights of individuals. To that end, the following information is provided as a guideline for copyright management on campus. The section was written by Dr. Michael Albright, director of instructional technology at California State University, Monterey Bay, CA – and ***used by permission****.*

Copyright law places college faculty members in an unusual conflict of interest situation. All of you have prepared lecture notes, conference presentations, or other unpublished papers that represent your intellectual property and to which you are entitled copyright protection. Many of you have published materials, for which you have either retained the copyrights or assigned them to the publishers. You may even receive royalties or other forms of revenue from these publications. Thus, you are in a unique position to appreciate the copyright law, because it preserves your rights and attempts to protect your income stream from these materials.

However, as teachers and facilitators of student learning, you have a somewhat different perspective on copyright. In this role, you want the broadest possible access to copyrighted materials. You wish to duplicate journal articles, book chapters and other printed materials of value and distribute them to students. During lectures, you want to display audiovisual materials and other works created by others. You would like to provide students maximum access to Internet resources. Each of these examples involves the intellectual property of others and they are equally entitled to copyright protection.

12.1 Brief Overview of Copyright

Copyright is one of four major categories of intellectual property protection, along with *patents*, *trademarks*, and *trade secrets*. Copyright is sometimes confused with patent law. Copyright covers works of authorship representing the tangible expression of ideas, requiring originality and some degree of creativity. Patents are issued for inventions that demonstrate novel, non-obvious, and useful products, or methods. While works of authorship may be registered with the U.S. Copyright Office, protection begins immediately after a work is fixed in a tangible form. Patent protection begins only after approval by the U.S. Patent and Trademark Office.

The first form of copyright protection in Europe followed not long after invention of the printing press. Congress enacted the first U.S. copyright legislation in 1790, a bill modeled after the Statute of Anne, passed by Parliament in 1714. The law (Title 17 of the U.S. Code) has undergone several major revisions, the last in 1976 (Public Law 94-553). According to Section 102 of the current law, copyright protection subsists:

> ***in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.***

Fixed in a tangible medium of expression is a critical condition for copyright eligibility. The law thus covers any file you have created on your computer and either saved to disk or printed. It includes a work of art, a videotape or sound recording, a dramatic work, architectural drawings, your lecture notes, and even your vacation slides -- in other words, *nearly any original expression that exists in a fixed form and can be perceived, reproduced, or communicated*.

Copyright protection **does not extend** to ideas themselves (only the expression of ideas), procedures, facts, principles, discoveries, titles, names, devices, machines, plans, slogans, familiar symbols, standard forms (such as blank checks, address books, and scorecards), and works consisting of common property

(such as height and weight charts, common lists, and schedules), although some items in these categories may qualify for patent or trademark protection.

12.2 Copyright Registration

A work does not have to be published before receiving copyright protection. Almost anything you create (see the exceptions above) automatically receives copyright protection as soon as it is fixed in a tangible form. Nor does the work have to be registered with the U.S. Copyright Office. The catch is that if the work is not registered and an infringement occurs, you are only eligible to recover actual damages. If the work is registered at the time of an infringement, you may be awarded statutory damages instead and recover all attorney fees, which can be substantial. Statutory damages can be a much greater amount.

Works of any significance that may be compelling to others probably should be registered. The registration fee is quite reasonable ($30 as of the date of this publication), and all the necessary forms and instructions may be downloaded from the Copyright Office website.

12.3 Ownership

Copyright ownership normally resides with the author(s) of the work. For example, your students may be entitled to copyright protection for assignments, papers, and other works turned in to you, depending on the nature of the material (e.g., a term paper on colonial architecture would qualify, solutions to calculus problems would not). Copyright ownership may be assigned to someone else, as is often the case with manuscripts submitted for publication.

An exception is made for "**works for hire**," defined by Section 101 of the copyright law as a work prepared by an employee within the scope of employment, or a work specifically ordered or commissioned under certain circumstances, in which case copyright is reserved for the employer or commissioner of the work. Does a college faculty member who must publish or perform other forms of scholarship as a condition for earning promotion and tenure thus retain the copyright to those works, or are they "works for hire," with the copyright retained by the institution? Most colleges and universities have intellectual property policies that address these issues, and in most cases professors are allowed to keep the copyrights. Work that is supported by grants from external funding agencies may provide a tricky variation on this theme. Contracts must be written so that the ownership of intellectual property resulting from such projects is clearly designated and understood by all concerned parties.

12.4 Duration of Copyright

How can you tell if a work is covered by copyright or has passed into the public domain? The answer varies, depending upon when the work was created, whether ownership resides with an individual or an employer or legal entity ("work for hire"), and whether the work was published. Publication occurs when a work has been duplicated and distributed (e.g., handouts in a class or conference session), or when copyright ownership has been transferred for the purpose of publication. The public performance or display of a work with no copies made does not constitute publication.

The earliest that a work created since January 1, 1978 (published or unpublished) could possibly fall into public domain is the year 2028. Published works dating from 1964-77 will not fall into public domain until at least 2039. The point is that unless a work is quite old, its copyright protection probably still exists, and any use of these materials beyond those specifically authorized by the copyright law or covered by applicable guidelines likely will require permission. The fact that a book is out of print and the copyright holder cannot be located does not waive its copyright protection.

WHEN WORKS PASS INTO PUBLIC DOMAIN		
DATE OF WORK	**POINT PROTECTION BEGINS**	**PROTECTION LENGTH**
Created January 1, 1978 or after. *THIS IS THE CURRENT COPYRIGHT LAW.*	When work is fixed in tangible medium of expression	**Life + 70 years** (or if work is of corporate authorship, the shorter of 95 years from publication, or 120 years from creation
Published before 1923	**In public domain**	**None**
Published between 1923 and 1963	When published with the copyright notice	28 years + could be renewed for 47 years, now extended 20 years for a total renewal of 67 years. If not renewed, new in public domain
Published between 1964 and 1977	When published with the copyright notice	28 years for first term; now automatic extension of 67 years for second term
Created before January 1, 1978, but not published	January 1, 1978, the effective date of the 1976 Act which eliminated common law copyright	Life + 70 years or December 31, 2002, whichever is greater
Created before January 1, 1978, but published between then and December 31, 2002	January 1, 1978, the effective date of the 1976 Act which eliminated common law copyright	Life + 70 years or December 31, 2047, whichever is greater

12.5 Public Domain

Public domain works may be freely used in teaching, research, and any other form of scholarship. Works can enter the public domain several ways. This is not an all-inclusive list.

(1) Expiration of copyright. *Works become public domain when their terms of copyright protection expire.*

(2) Federal Government authorship. *With the exception of some reference data published by the U.S. Department of Commerce, materials published by the U.S. Federal Government are specifically excluded from copyright protection and are in the public domain from the date of creation. However, works produced by an independent contractor with Federal funding do qualify for copyright protection. Hence, a videotape about AIDS research produced by a private contractor for the Department of Health and Human Services is copyrighted and receives the same protection as any other audiovisual work. Note also that restrictions on the Federal Government do not apply to individual states. The works of a state government may be copyrighted, with decisions on whether a work should be copyrighted or entered into the public domain left to the individual states (Carroll, 1994).*

(3) Abandonment of copyright. *Although this rarely happens, an owner may relinquish the copyright to a work and dedicate it to the public domain. The abandonment of copyright requires an explicit and overt statement from the copyright holder (Carroll, 1994). This question has arisen numerous times regarding materials posted on the Internet, such as listserv or Usenet messages or webpages. Unique issues related to the Internet will be discussed below.*

12.6 International Copyright Protection

The Berne Convention for the Protection of Literary and Artistic Works was convened in 1886 to provide mutual recognition of copyright among nations and establish international standards for copyright protection. The treaty has been revised several times, the last in 1971. The U.S. became a signatory of the Berne Convention in 1988, and most countries in the world now adhere to Berne provisions. The effect of the Berne treaty is that the copyright laws of any signatory country apply within that country to the copyrighted works of an author from any other signatory country. In other words, within Japan, Japanese copyright law applies to a publication of an American author registered in the U.S.

12.7 Copyright Notice

As one result of U.S. adoption of the Berne Convention, works published after March 1, 1989 are no longer required to include the familiar copyright notice in order to qualify for copyright protection. However, in a copyright infringement suit, the presence of a copyright notice prevents the defendant from pleading "innocent infringement," or lack of awareness that commission of the infringing act was wrong (Carroll, 1994). Thus, leaving the copyright notice off a published work serves no particular advantage.

The standard format for a copyright notice is © [name of copyright owner] [year]. The term "Copyright" may be used in the U.S. instead of the symbol ©. O'Mahoney (1995) points out that the term "Copyright" is preferable for Internet documents because some browsers do not properly display the C-in-circle symbol. He recommends that both term and symbol be used on webpages.

Prior to adoption of the Berne treaty, the U.S. was signatory to the Buenos Aires Convention of 1911, which required placement of "All Rights Reserved" on copyrighted documents to ensure protection in all signatory countries. All countries that signed the Buenos Aires treaty are now signatory to the Berne Convention, and this notice no longer serves any legal purpose.

12.8 Exclusive Rights of Copyright Owners

According to Section 106 of Title 17, copyright owners are granted the exclusive rights to do, or to authorize others to do, any of the following:

- ✓ *Reproduce the copyrighted work*
- ✓ *Prepare derivative works based on the copyrighted original*
- ✓ *Distribute copies of the copyrighted work*
- ✓ *Perform the copyrighted work publicly*
- ✓ *Display the copyrighted work publicly*

These exclusive rights have significant implications for college faculty members, because effective teaching is difficult in many disciplines without displaying or providing copies of or performing the intellectual property of others, most often in the contexts of classroom activities or out-of-class assignments for students.

Fortunately, the authors of the 1976 revision recognized that under certain circumstances, the use of protected materials could be acceptable without permission from the copyright holder. In fact, the sections describing limitations on exclusive rights consume about 80 percent of Chapter 1 of Title 17. Two are of particular importance to college instructors. Section 107 addresses reproduction and distribution under the concept of "fair use." Section 110 establishes a "face-to-face teaching exemption" that allows classroom displays and performances.

12.9 Fair Use

The terminology of the law is quite explicit. Congress stipulated that *"the fair use of a copyrighted work . . . for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright"* (Section 107). The law does not say, "the use of a copyrighted work . . . is not an infringement . . . " It specifies, "the fair use of a copyrighted work" This is an important distinction, because ***the myth seems to persist in academe that if a use is for educational purposes, it is legal under fair use, but that is not the case.*** Only a fair use is legal, and fair use cannot be applied until four essential factors have been considered.

Unfortunately, the four criteria are excruciatingly ambiguous and complex. This was intentional on the part of the law's authors, because a virtually infinite number of possible fair use scenarios exist, and Congress wished to provide a flexible structure for assessment that could be applied to all cases without the need for constant revisions to the law. Thus, each fair use situation must be individually judged on its own merits against the four factors. Remember that the four factors help you judge only whether a copyrighted work can be used without permission. Even if the factors weigh against fair use, you still may be able to use the materials if the owner grants approval.

The FOUR ESSENTIAL FACTORS that must be addressed when considering fair use:

1. Purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes.

Educational or nonprofit uses of protected materials tend to weigh in favor of fair use. Reproduction for the purposes of criticism, commentary, and news reporting, even if for commercial purposes, also are more likely to be considered fair use. "Transformative" works that use the old material in new ways is more likely to be favored than cases of simple duplication of an original.

2. Nature of the copyrighted work.

Works of nonfiction presenting factual material are more likely to be considered fair use than fictional and artistic works based on creative expression. Published materials are generally favored more than unpublished works. Audiovisual materials are more questionable than printed works, and reproduction of materials designed to be consumable, such as workbooks and preprinted answer sheets, is rarely considered fair use.

3. Amount and substantiality of the portion used in relation to the copyrighted work as a whole.

This factor has both quantitative and qualitative aspects. In many cases, a reproduction involves a journal article, photograph, illustration, cartoon, or other short publication in which the entire work is desired. The fact that the work may appear with other materials and constitute a small percentage of the total content of the publication is irrelevant. Courts are more likely to favor a use that took no more of the published original than was necessary to meet the user's purposes. Care must also be taken to ensure that the portion taken, even if a small amount of the entire work, does not contain the essence or heart of the original.

4. Effect of the use upon the potential market for or value of the copyrighted work.

While this factor is often considered the most important of the four, it may also be the most misunderstood. A professor may feel that a reproduction is justifiable because as an isolated event the financial harm to the copyright owner is minimal. However, the courts consider effect in the context of the potential impact if the professor's act were a widespread practice. Potential harm to derivative works may also be taken into consideration. Reproductions from scholarly publications are particularly questionable, because in many cases higher education is the primary market for those products, and financial loss is easier to demonstrate.

12.10 Face-to-Face Teaching Exemption

Fair use involves reproduction of protected materials. Public performance and display of copyrighted works is a different matter entirely, and classrooms are considered public. Section 110 permits the performance or display of a work during the face-to-face teaching activities of a nonprofit educational institution, in a classroom or similar place devoted to instruction, with a lawfully-made copy (if applicable). This section covers activities such as the reading aloud of literature, performance of dramatic works by class members (but not by actors not associated with the class), performance of compositions in music classes, and display of videotapes and other audiovisual materials. As with the duplication of materials, *permission should be sought in cases of performance or display that do not appear to comply with these conditions.*

The House of Representatives Report (94-1476) accompanying the 1976 law noted specifically that the face-to-face teaching exemption does not extend to the transmission of audiovisual materials into the classroom from a location outside the building. This is problematic for libraries and media centers that transmit videotapes from centralized collections into classrooms via campus networks. The distribution of materials in this manner requires specific licensing agreements with the copyright holders.

Section 110 cannot be applied to training events that take place in for-profit settings, for example in proprietary institutions and industry. Classroom display of materials such as videotapes in for-profit locations should be covered by licensing agreements when the materials are purchased.

12.11 Guidelines

Congress recognized early on that the non-profit educational community could be assisted by guidelines that help define acceptable practices under fair use. The House Report contained two sets of guidelines that had been carefully negotiated by educator and publisher groups during the development of the law, *one for classroom copying* and *one for educational uses of music.* In 1979, a third set of guidelines was negotiated and approved covering *off-air recording of broadcast programming for educational purposes.*

As the digital age progressed, the shortcomings of the 1976 law and existing guidelines became more and more evident. In 1994, the Clinton Administration convened the Conference on Fair Use (CONFU) to address contemporary fair use issues in the digital environment. For two-and-a-half years, representatives of nearly 100 proprietary, educational, and governmental organizations met collectively and in smaller working groups to develop guidelines for distance learning, image collections, multimedia, electronic reserves, and interlibrary loan.

The outcome was disappointing. Negotiators had considerable difficulty finding common ground, with educators and librarians resisting guidelines they felt were overly restrictive and copyright owners concerned about giving up too much. The sides in the interlibrary loan discussions were so far apart that no workable draft ever appeared from that workgroup. Drafts were developed by the distance learning, image collections, and electronic reserves workgroups but failed to achieve much support. Only the multimedia guidelines workgroup, which had already been functional for a year before the establishment of CONFU, developed a document achieving consensus support, but even these guidelines drew strong opposition from higher education and library organizations.

In May 1997, CONFU elected neither to endorse nor reject any of the drafts. Its participants agreed that the opportunity to meet and negotiate had been healthy, and that discussions should continue. Thus, we have guidelines, at least in draft form, for many of the technology applications college faculty might encounter today. Remember that the guidelines are just that - guidelines. They do not identify absolute limits that cannot be exceeded. They may represent “safe harbor” standards, because the endorsing organizations have agreed not to pursue litigation as long as the guidelines are followed.

A prominent copyright attorney has pointed out that no one has ever been successfully litigated for following the guidelines. ***Intellectual property specialists in higher education emphasize that the guidelines represent the minimal level of acceptable behavior, and the actual boundaries may well exceed the limits specified. The courts can only determine the true limits, although none of us wants to be the test case.***

COPYRIGHT APPLCATIONS IN THE REAL WORLD OF TEACHING

What are the direct implications of all this for your role as a college teacher? I must begin this section with the standard disclaimer. I am not a lawyer, and this chapter does not constitute legal advice. Readers are urged to contact their campus or system attorneys for authoritative legal opinions.

12.12 Printed Material

When you purchase a book, you buy the cover, binding, and pages. You acquire the right to read the intellectual property the book contains, but your "ownership" is restricted to the physical book itself. Under the "first sale doctrine" described in Section 109, you have the right to resell the book, give it away, or otherwise dispose of it, but beyond that point your rights are rather limited. Further use of the content of books, periodicals, and other printed materials, including reproduction for distribution to students, must be governed by existing guidelines or the criteria for fair use.

12.13 Single copies for teaching or research

The Guidelines for Classroom Copying in Not-For-Profit Educational Institutions specify that single copies of the following may be made for the purposes of scholarly research or use in teaching or preparation to teach a class:

- ✓ *A chapter from a book*
- ✓ *An article from a periodical or newspaper*
- ✓ *A short story, short essay or short poem, whether or not from a collective work*
- ✓ *A chart, graph, diagram, drawing, cartoon or picture from a book, periodical or newspaper*

These guidelines extend to student research related to a course or their own scholarship. Note that in each instance the permissible use is in the singular. *Multiple items from the same source would not be acceptable.* The guidelines are also painfully vague. For example, do they permit professors to routinely make overhead transparencies from Dilbert or Foxtrot cartoons because they appear in different newspaper issues? The guidelines seem to imply permissible use, but this is not one I would care to test in a court case. Academic libraries are permitted to make single copies for patrons, both faculty and students, essentially according to the same restrictions, as long as the copies become the property of the user and are for the purposes of private study, scholarship, or research.

Section 108 exempts libraries and their employees from liability for infringements committed on an unsupervised photocopier, as long as a copyright warning notice is displayed on or near the copier, and places liability for infringement directly on the patron whose reproductions exceed the boundaries of fair use.

12.14 Multiple copies for classroom use

Do you duplicate journal articles on the department copier and pass them out in class? The guidelines permit the reproduction and distribution of copyrighted materials (no more than one copy per student in the course), as long as the tests of brevity and spontaneity and the cumulative effect test are met.

*1. The **brevity test** places limits on the length of materials to be reproduced, such as 2,500 words for a complete article and one illustration per book or periodical issue. See the guidelines for limits on other publication types.*

*2. The **spontaneity test** requires that "the inspiration and decision to use the work and the moment of its use for maximum teaching effectiveness are so close in time that it would be unreasonable to expect a timely reply to a request for permission." With contemporary technologies such as email and faxes available for seeking permission, these two events should be pretty close together. Also, since spontaneity is rarely measured in terms of semesters, this test effectively prohibits use of the same materials in subsequent academic terms without permission.*

*3. The **cumulative effect test** requires that no more than one item may be copied from the same author, nor more than three from the same collective work or periodical volume, in the same academic term. Moreover, the guidelines set the maximum number of multiple copying activities, of any kind, for any single class in any single course term, at nine.*

By now, you may have concluded that the classroom copying guidelines are quite restrictive. **Unless a publication is fresh off the press, you may find it more convenient to go through the permission process and have students pay the licensing fee in the form of a purchase price.** The information age and resulting explosion of knowledge have made it difficult for publishers to keep textbooks current. As a result, many instructors have turned to course packs as a means of providing up-to-date information to students, either supplementing or replacing textbooks. Course packs are compilations of readings that may include journal articles, book chapters, conference papers, and other publications, copyright-cleared and sold by bookstores or copy services. If you compile the list of publications you wish to include in a course pack, a system is likely in place on or near your campus to expedite the clearance process and handle the reproduction and sales for you.

The ***Copyright Clearance Center*** (CCC) has been established as the Reproduction Rights Organization (RRO) for the U.S. for the purpose of licensing the duplication of copyrighted print material and collecting and distributing royalties. The CCC can provide immediate permission for over 1.7 million titles already pre-authorized by copyright holders and will seek permission for publications not yet registered. Bookstores and copy centers serving many campuses already have accounts set up with the CCC to clear and reproduce these materials for you, then sell them to the students. Course packs are licensed through the CCC's Academic Permissions Service (APS).

The CCC operates collective licensing systems that facilitate compliance with the copyright law. Its website provides helpful information about CCC services and copyright in general.

Copyright Clearance Center – ***http://www.copyright.com/***

12.15 Computer Software

Computer software falls into four general categories: *commercial*, *shareware*, *freeware* and *public domain*. Commercial software licenses permit making one archival copy, which may only be used if the original becomes damaged or nonfunctional. Additional copies, for example for a second office or home computer, are legal only if permitted by the specific license for that software. Many higher education institutions have negotiated site licenses that permit multiple copies of some software at reduced rates. Check with your computing center to find out what agreements are in place for your campus.

Shareware and freeware also receive copyright protection. Both are widely available from software archives on the Internet and other sources. Shareware licenses permit you to install the software on your computer and try it out. If you decide to keep it and continue to use it, then you must pay the specified fee to the copyright holder. You may make an archival copy of shareware under the same conditions as

for commercial software. Freeware is just that. It may be installed, used, copied, and even modified without payment of any fee. About the only limitation on freeware is that it cannot be redistributed for profit by anyone except the copyright holder, although derivative versions may be distributed by anyone as freeware.

Public domain software, which must be clearly marked as such, is fair game.

Illegal software on your computer carries a risk, both to you and to your institution. Most colleges and universities have policies that prohibit the installation and use of unlicensed software, and copyright holders are becoming increasingly aggressive in obtaining search warrants to find out if their software has been pirated.

12.16 Classroom Use of Video

Section 110 permits unlimited classroom display of videotapes that have been purchased or rented by your institution and are intended or licensed for educational use. However, the face-to-face teaching exemption does not automatically extend to tapes marked *"For Home Use Only,"* such as entertainment films bought over the counter or rented from Blockbuster or Hollywood Video.

Entertainment films purchased by educational institutions are normally accompanied by licensing agreements permitting classroom use, but a tape you acquired at the local discount store for your personal use probably does not have such a license and should not be used in the classroom. The waters regarding use of tapes rented from video stores are really muddy. Some copyright authorities feel it is legal – some disagree. This practice is risky, at best!

12.16.1 Off-air recording

There are clear-cut guidelines regarding classroom use of television programs. The Guidelines for Off-Air Recording of Broadcast Programming for Educational Purposes, negotiated in 1979, permit the classroom use of television programs taped off-air, under certain conditions.

The guidelines only apply to broadcast programming, in other words the programs of stations that reach your community over-the-air, and not to cable channels. For example, the programming of a local television station received through a cable TV system may be taped, but the Discovery Channel and the Arts & Entertainment Network (A&E) cannot.

A program recorded off-air may be displayed once and repeated once in each class section only within 10 consecutive working days following the date of taping. The tape may be retained for an additional 35 days for your own review and evaluation purposes but cannot be shown to students during this time without permission from the broadcaster.

Following this 45-day period, the guidelines **require that the tape be erased**. Programs must be taped in their entirety, including the copyright notice, but undesired sections may be omitted during classroom playback. Any single program may be taped only once by or for the same faculty member and may not be recorded again if it is re-broadcast.

Classroom use beyond that permitted by the guidelines requires permission. Local broadcasters normally are quite willing to permit extended use of programs produced by their own stations. However, permission may be more difficult to obtain from the major networks and cable programmers. The reason, quite simply, is that many of their programs are offered for sale, either by sales divisions of the networks themselves or by authorized distributors, normally at quite reasonable prices.

Several cable services (e.g., A&E, History Channel, Discovery Channel, Turner Broadcasting) do offer limited educational licenses, but the programs authorized for use are directed at primary and

secondary school students and are likely to be of limited value in higher education. C-SPAN is the one exception, offering all its programming for unlimited educational use.

12.16.2 Locally-produced videotapes

Perhaps the simplest solution to copyright limitations is to use videotapes produced at your own college or university. Unless unusual circumstances exist, your institution holds the copyright to these tapes, and you should be able to use them without restrictions.

12.17 Music

Guidelines for Educational Uses of Music accompanied the 1976 copyright law revision and were directed primarily toward music faculty. The guidelines permitted:

- ✓ *Emergency copying to replace purchased copies not available for an imminent performance.*
- ✓ *For academic purposes other than performance, single or multiple copies of excerpts of works that do not constitute performable units and do not exceed 10 percent of the whole.*
- ✓ *Recordings of student performances for evaluation or rehearsal purposes.*
- ✓ *Single copies of sound recordings owned by the institution or the faculty member for the purpose of constructing aural exercises or examinations.*

Specifically excluded were copying for the purpose of performance and copying as a substitute for purchase, except as permitted above.

Section 110 permits both the playing of legally-acquired audio and video recordings of music in a classroom as well as the in-class performance of copyrighted musical compositions by the students and/or faculty member. The course topic is irrelevant. Such learning activities may be equally valuable in the languages, history, art and aesthetics, and myriad others besides music department courses. The House Report on the law clarified that this provision would include guest lecturers "if their instructional activities remain confined to classroom situations," but not to singers or instrumentalists brought in from off campus for the purpose of presenting a program.

A discussion of public performances is beyond the scope of this article. Check with your campus or school copyright office for current information on licensing requirements and licenses that may already be in place for your institution. It is important to recognize that licensing requirements exist for public performances beyond those mounted by music departments. For example, the use of copyrighted music in theatrical performances and student-produced works, such as slide-tape programs, multimedia, and videotapes, in campus media fairs open to the public may also require licensing agreements.

12.18 Internet Resources

On the surface, it would appear that the Internet presents a whole new "can of worms" related to copyright issues. However, while ease of access and reproduction may lead one to believe that the rules are different, they really are not. Email messages, listserv and Usenet postings, the content of webpages, FTP files, and other materials available through the Internet are fixed in a tangible medium of expression and meet all the legal requirements for copyright protection, just like any other form of intellectual property.

Does the deliberate and purposeful placement of information on such a public forum as the Internet imply that copyright has been abandoned? Very clearly, the answer is no, not without an explicit statement to that effect on the part of the copyright holder – which is often someone other than the poster (Templeton, 1997).

12.18.1 Email messages and listserv/Usenet postings

The author of an email message retains the ownership of that message. Most copyright authorities agree that a person-to-person message can be saved, printed, and forwarded to a limited group of other individuals interested in the same subject without the permission of the originator under the concept of "implied license," but implied license does not extend to reposting that personal message to a listserv or newsgroup.

For example, a professor should not redirect a personal message from a student to the course listserv without the student's consent. Moreover, forwarding a message received via one listserv or newsgroup to another *without permission* may also extend beyond the boundaries of implied license, if the forwarded message is likely to reach an essentially different audience or is sent through a different distribution system (O'Mahoney, 1997). *When in doubt, ask permission before you forward.*

Subscribers to a listserv normally grant to the list owner the right to archive the postings, often on a web site, so that messages can be reviewed if desired. Depending upon the list topic, access to the archive may be password-protected or otherwise restricted. Listserv postings in courses discussing sensitive or controversial topics, such as death and dying or the psychology of bisexuality, will likely be quite subdued if students know the archives are open to the public.

Archives represent the limit to which messages may be compiled. For instance, messages on a specific topic may not be collected and then republished in any form such as a printed anthology without the expressed permission of each message author.

What about the practice of including all or a portion of a received message within a reply, as a point of reference to clarify the response? As long as the portion used is not taken out of context and does not alter the originator's intent, this appears to fall under the "comment" or "criticism" provisions of fair use.

Paraphrasing elements of the original message in one's own terms is not an infringement, because the copyright law applies only to the expression of ideas (the originator's own text) and not to the ideas themselves (O'Mahoney, 1997). The sender of such a message has an ethical obligation to attribute the ideas to the originator and not claim credit for them.

12.18.2 Webpages

When you access a page on somebody's website, you are not viewing the page directly on that site's server. Your browser copies all the files associated with that page (hence the long download time in some cases) into the memory of your own computer and reassembles them there for your reading enjoyment. Thus, the copying of files is an essential prerequisite before a web page can be viewed. This is how the web works. Site webmasters expect that their files will be copied for that purpose. However, this is where the line is drawn. Any additional copying, including printing and saving, must be governed by the criteria for fair use.

12.18.3 Copying individual pages or articles

The simple presence of *Print* and *Save* buttons on your browser tool bar should not imply that all web pages are fair game. The Consortium for Educational Technology for University Systems (CETUS), a joint project of the California State University, State University of New York (SUNY), and City University of New York (CUNY), has published a fair use handbook that addresses this issue, among others. CETUS (1995) suggests that the copying of a short Internet document for personal use, including research, likely falls within fair use but urges faculty to consider all four fair use criteria on a case-by-case basis. The CETUS handbook does not discuss making multiple copies

of Internet publications for distribution to students, such as incorporation in course packs. The guidelines and recommendations for other printed materials (see above) are equally applicable to web documents and other files retrieved from the Internet.

The fair use criteria are particularly important when you consider copying from websites that are password-protected and open only to subscribers or members, or sites that contain documents that are available commercially. For example, a major publisher of computer-related books has for some inexplicable reason put full text of many of its publications on he web, easily downloadable. Since these same books are offered for sale in every shopping mall bookstore, the case for printing these publications off the web as fair use would be extremely difficult to defend.

12.18.4 Copying entire websites

Suppose your classroom does not have an Internet connection, but you do have a computer and a projection system, and you would like to demonstrate some websites to your students. Software is available (e.g., *WebWhacker*) that enables you to download individual pages and entire sites, complete with links and plug-ins, and view them from a disc file rather than the Internet. Copying to this extent may go beyond the implied license permitting you to view the site via a live connection.

This question has received much attention on instructional technology-related listservs, and feelings are strong each way. Proponents claim that you are just replicating what your browser would do if you did have an online connection, and that you are doing nothing that the website administrator does not expect you to do. Demonstrating websites for the purposes of comment or criticism falls under fair use.

Moreover, websites are intended to be viewed by anyone on the Internet, or they would not be there in the first place. Hold on, say the opponents. Many sites are not intended to be viewed by anyone, especially those that have controlled access or are located on intranets. What if the page contains advertising, and in your download you fail to include the link to the ad? The point-counterpoint goes on, but these are the basic arguments.

In general, this type of learning activity can be quite beneficial to your students, and we recommend it. However, you must use some discretion in your downloads. Do not capture any page or site that is not freely available to anyone on the Internet. Avoid sites you feel might cause trouble for you. If the site includes advertising, make sure you download the entire page, including the links to the ads. When in doubt, contact the site webmaster and ask permission.

12.18.5 Photographs and Digital Images

The reproduction of photographs, illustrations, graphic designs, and other still images present an perplexing copyright dilemma because intellectual property may be involved at several levels. For example, you may wish to make a slide from or digitize a textbook photograph.

The book and the photograph may be copyrighted separately, and depending upon the subject matter, the original object may also be protected. Moreover, the chain from the original to the photo in your book may involve intermediate steps, each entitled to copyright protection. Even if the original object is in the public domain, the photograph and book may not be.

Section 110 permits the classroom display of photographic material that has been lawfully acquired. In other words, slide or digital image sets purchased for educational use from someone authorized by the copyright holders are the safest alternative. The “lawfully acquired” condition may apply to slide sets compiled locally from books and magazines using a copystand. The Guidelines for Classroom Copying indicate that one picture per book or periodical issue is permissible.

The CETUS (1995) fair use guidelines suggest that "a small number of images from any one textbook" (p. 26) may fall under fair use, particularly if slides are not available from the publisher. Any slide making or imaging beyond these guides requires a very careful consideration of the four criteria for determining fair use.

Guidelines for the educational use of digital images were drafted by a CONFU working group but were quite restrictive and failed to garner much support in the educational community. The draft does provide some insight into the limits to which some copyright holders perceive fair use. The guidelines include the following selected provisions:

- ✓ *Only lawfully acquired analog images may be digitized.*
- ✓ *Educational institutions may not digitize images that are already available in usable digital form for purchase or license at a fair price.*

Educational institutions may display and provide access to images digitized under these guidelines through a secure electronic network, provided that access is controlled via a password or PIN and restricted to students enrolled in the course.

Use of images digitized from a known source may only be used for one academic term; subsequent use requires permission. If permission is not received, subsequent use is subject to the four-factor fair use analysis.

If the copyright holder is unknown, the image may be used for three years from first use, provided that the institution conducts a reasonable effort to identify the copyright holder and seek permission.

Images digitized under these guidelines may be used in face-to-face teaching, independent study by students, and research and scholarly activities at the institution. The images may not be used in publications without permission.

12.18.6 Multimedia

The display of a multimedia program in a classroom as part of an educational activity is clearly permitted by Section 110. However, incorporation of copyrighted material in the development of a multimedia work presents an extraordinarily complex set of issues.

Some of these concerns were addressed in the Fair Use Guidelines for Educational Multimedia completed in 1996 as part of the CONFU process and the subject of a Non-legislative Report adopted by the U.S. House of Representatives. The multimedia guidelines thus have been accepted by Congress and the U.S. Copyright Office but were not endorsed by CONFU and have been vigorously opposed by some higher education and academic library organizations as too restrictive.

Briefly, the guidelines permit student and faculty use of copyrighted materials in multimedia productions for face-to-face instruction, independent learning settings, presentation at peer conferences, and retention in professional portfolios with the following limitations:

- ✓ *Permission from the copyright holder(s) must be obtained for use following a two-year period beginning with the first instructional use.*
- ✓ *No more than 10 percent or 3 minutes, whichever is less, in the aggregate of a copyrighted motion media work (e.g., video or film) may be used.*
- ✓ *No more than 10 percent or 1,000 words, whichever is less, may be used in the aggregate of a copyrighted work consisting of text material.*
- ✓ *No more than 10 percent or 30 seconds, whichever is less, of the music and lyrics from an individual musical work may be used.*

- ✓ *No more than five photographs or illustrations by a single artist or photographer may be incorporated.*
- ✓ *No more than two copies of the completed production may be made for student or faculty use, with a third copy permitted for the purposes of preservation and reproduction to replace damaged, lost, or stolen copies.*

12.19 Distance Education

Section 110 extends certain provisions of the face-to-face teaching exemption to instruction delivered by transmission to remote locations, including college credit courses. Allowable activities include performances of non-dramatic musical and literary works and the display of photographs, illustrations, maps, and other printed materials, still images from videotapes, and 35mm slides as long as they are not shown in sequence from a copyrighted program. The law specifically excludes the performance of dramatic works and the display of audiovisual materials, defined in the law as works that consist of a series of related images intended to be shown by the use of machines. Thus, according to the law itself, a course that is transmitted cannot include a video or videodisc, or consecutive images from a photographic series without permission.

Obviously, this restriction is problematic for faculty who use video in their conventional classroom teaching. The Educational Fair Use Guidelines for Distance Learning drafted by the CONFU working group attempted to address this concern but were so restrictive the draft failed to gain much support. Among the guidelines' provisions were the following:

- ✓ *Transmission must be over a secure system with limited access.*
- ✓ *Performance of an entire copyrighted work or a large portion thereof may be transmitted only once for a distance learning course; permission must be obtained for subsequent displays or performances.*
- ✓ *Receiving institutions may record the class sessions containing the copyrighted work and make them available to students for up to 15 consecutive working days, as long as the viewing is in a controlled environment that prevents additional reproduction of the portion of the tape that includes the copyrighted material.*

Therefore, use of a video in a course offered on a one-time-only basis would be acceptable, but routine use in a course delivered in ongoing academic terms would require permission. The last provision cited above would prevent course tapes from being sent to, or viewed in, student homes if they included non-cleared copyrighted material.

The CONFU distance learning working group elected not to address online course materials in the guidelines, feeling that this area was in too rapid a state of evolution.

12.20 Liability for Infringement

For the most part, copyright is *civil law – not criminal law*. Unless you make and sell pirate copies of videotapes or computer software or enjoy some other financial gain, you could be sued for copyright infringement but not sent to prison.

The copyright holder has the choice of seeking statutory damages, which can be as much as ***$100,000 per instance*** if the plaintiff can prove in court that the infringement was willful, or actual damages to recover lost revenues. If you have not made a business out of the infringements, the former is more likely.

You are liable for damages even if you did not realize you were committing an infringement. However, Section 504 of the law provides that college employees, including faculty, may not be subject to statutory damages "in any case where the infringer believed and had reasonable grounds for believing that his or her use of the copyrighted work was a fair use under section 107..." Thus, according to this "good faith fair use defense," if you were truly convinced that your use of the protected materials was fair use and have left no evidence to the contrary, you may (emphasize may, at the discretion of the court) escape statutory damages, even if the act in question was not fair use. On the other hand, you will be liable for your own attorney's fees, and the court may direct you to pay for the plaintiff's legal costs as well, and these can be significant.

If your college or university has an established copyright policy, and you violate that policy in the process of committing an infringement, you may find that your institution's legal counsel will not defend you. For example, the University of Texas System's fair use policy states specifically that employees who violate the policy and the terms of any relevant licenses will be personally responsible for their own defense (Harper, 1997). A University of Hawaii system campus has issued a similar warning (Cerny, 1996). I urge you to check your own campus's copyright policies.

12.21 Seeking Permission

Several times in this article I have urged you to seek permission when in doubt. Start by contacting the author or publisher. If no address or phone number is provided, a campus reference librarian might be able to help. The Copyright Clearance Center also has contact information for thousands of authors and publishers.

If at all possible, contact the copyright holder by phone to clarify precisely to whom your request should be addressed. A phone call gives you the opportunity to discuss the specific circumstances of your request and negotiate fees, if applicable. Whether your means of contact is phone, fax, letter, or email, the copyright holder will need the following:

- ✓ *Your personal contact information, including name, position, institution, mailing address, phone and fax numbers.*
- ✓ *Complete identification of the item you wish to use, including title, author, publication title and date, volume and issue, page numbers (if applicable), and amount desired.*
- ✓ *Detailed description of your intended use, including purpose, course name, number of copies, means of distribution, need in multiple academic terms (if applicable), and other relevant information.*
- ✓ *Date by which you need permission. (Provide at least six weeks if possible).*

Permission may be granted over the phone, but get it in writing on the copyright holder's letterhead if at all possible, either by mail or fax. Obtaining permission in a tangible form confirms who provided permission for what, and when. Additional guidance and a sample permission request letter may be found in the CETUS (1995) handbook on fair use.

12.22 References for Appendix A (copyright) –

Association of Research Libraries. (1996). *Timeline: A history of copyright in the U.S.* Washington, DC: Author. (http://arl.cni.org/info/frn/copy/timeline.html)

Carroll, T. (1994). *Copyright FAQ.* (http://www.aimnet.com/~carroll/faq-home.html) [Link no longer active]

Cerny, J. (1996). *The quick and dirty guide to copyright rules.* Honolulu, HI: Honolulu Community College. (http://www.hcc.hawaii.edu/education/hcc/facguide/fg/copyright.html) [Link no longer active]

Consortium for Educational Technology for University Systems. (1995). *Fair use of copyrighted works: A crucial element in educating America.* Seal Beach, CA: California State University Chancellor's Office. (http://www.cetus.org/fairindex.html)

Harper, G. (1997). *Fair use of copyrighted materials.* Austin, TX: University of Texas System, Office of General Counsel. (http://www.utsystem.edu/OGC/IntellectualProperty/copypol2.htm)

Miller, J.K. (1975). *A brief history of copyright.* Audiovisual Instruction.

O'Mahoney, x. B. (1997). *Newsgroups.* (http://www.benedict.com/newsgrp.htm) [Link no longer active]

Templeton, B. (1997). *10 big myths about copyright explained.* (http://www.templetons.com/brad/copymyths.html)

13. APPENDIX B – Fair Use Guidelines for Educational Multimedia

12.1. INTRODUCTION – *Prepared by the Educational Multimedia Fair Use Guidelines Development Committee, July 17, 1996*

12.1.1 Preamble

Fair use is a legal principle that defines the limitations on the exclusive rights** of copyright holders. The purpose of these guidelines is to provide guidance on the application of fair use principles by educators, scholars and students who develop multimedia projects using portions of copyrighted works under fair use rather than by seeking authorization for non-commercial educational uses. These guidelines apply only to fair use in the context of copyright and to no other rights.

There is no simple test to determine what *fair use* is. Section 107 of the Copyright Act*** sets forth the four fair use factors which should be considered in each instance, based on particular facts of a given case, to determine whether a use is a "fair use":

1. ***Purpose and character of use, including whether such use is of a commercial nature or is for nonprofit educational purposes,***
2. ***Nature of the copyrighted work,***
3. ***Amount and substantiality of the portion used in relation to the copyrighted work as a whole, and***
4. ***Effect of the use upon the potential market for or value of the copyrighted work.***

While only the courts can authoritatively determine whether a particular use is fair use, these guidelines represent the participants'**** consensus of conditions under which fair use should generally apply and examples of when permission is required. Uses that exceed these guidelines may nor may not be fair use. The participants also agree that the more one exceeds these guidelines, the greater the risk that fair use does not apply.

The limitations and conditions set forth in these guidelines do not apply to works in the public domain – such as U.S. Government works or works on which copyright has expired for which there are no copyright restrictions--or to works for which the individual or institution has obtained permission for the particular use. Also, license agreements may govern the uses of some works and users should refer to the applicable license terms for guidance.

The participants who developed these guidelines met for an extended period of time and the result represents their collective understanding in this complex area. Because digital technology is in a dynamic phase, there may come a time when it is necessary to review the guidelines. Nothing in these guidelines shall be construed to apply to the fair use privilege in any context outside of educational and scholarly uses of educational multimedia projects.

This Preamble is an integral part of these guidelines and should be included whenever the guidelines are reprinted or adopted by organizations and educational institutions. Users are encouraged to reproduce and distribute these guidelines freely without permission; no copyright protection of these guidelines is claimed by any person or entity.

- ✓ **These Guidelines shall not be read to supersede other preexisting education fair use guidelines that deal with the Copyright Act of 1976.*
- ✓ ***See Section 106 of the Copyright Act.*
- ✓ ****The Copyright Act of 1976, as amended, is codified at 17 U.S.C. Sec.101 et seq.*

- ✓ *****The names of the various organizations participating in this dialog appear at the end of these guidelines and clearly indicate the variety of interest groups involved, both from the standpoint of the users of copyrighted material and also from the standpoint of the copyright owners.*

12.1.2 Background

These guidelines clarify the application of fair use of copyrighted works as teaching methods are adapted to new learning environments. Educators have traditionally brought copyrighted books, videos, slides, sound recordings and other media into the classroom, along with accompanying projection and playback equipment. Multimedia creators integrated these individual instructional resources with their own original works in a meaningful way, providing compact educational tools that allow great flexibility in teaching and learning. Material is stored so that it may be retrieved in a nonlinear fashion, depending on the needs or interests of learners. Educators can use multimedia projects to respond spontaneously to students' questions by referring quickly to relevant portions. In addition, students can use multimedia projects to pursue independent study according to their needs or at a pace appropriate to their capabilities. Educators and students want guidance about the application of fair use principles when creating their own multimedia projects to meet specific instructional objectives.

12.1.3 Applicability of These Guidelines

(Certain basic terms used throughout these guidelines are identified in bold and defined in this section.)

These guidelines apply to the use, without permission, of portions of lawfully acquired copyrighted works in educational multimedia projects which are created by educators or students as part of a systematic learning activity by non-print educational institutions.

12.1.4 Educational multimedia projects created under these guidelines incorporate students' or educators' original material, such as course notes or commentary, together with various copyrighted media formats including but not limited to, motion media, music, text material, graphics, illustrations, photographs and digital software which are combined into an integrated presentation. **Educational institutions** are defined *as nonprofit organizations whose primary focus is supporting research and instructional activities of educators and students for noncommercial purposes.*

For the purposes of the guidelines, **educators** *include faculty, teachers, instructors, and others who engage in scholarly, research and instructional activities for educational institutions.* The copyrighted works used under these guidelines are **lawfully acquired** if obtained by the institution or individual through lawful means such as *purchase, gift or license agreement* but not pirated copies. Educational multimedia projects which incorporate portions of copyrighted works under these guidelines may be used only for **educational purposes** in systematic learning activities including use in connection with non-commercial curriculum-based learning and teaching activities by educators to students enrolled in courses at nonprofit educational institutions or otherwise permitted under *Section 12.3*. While these guidelines refer to the creation and use of educational multimedia projects, readers are advised that in some instances other fair use guidelines such as those for off-air taping may be relevant.

12.2. PREPARATION OF EDUCATIONAL MULTIMEDIA PROJECTS USING PORTIONS OF COPYRIGHTED WORKS

These uses are subject to the Portion Limitations listed in *Section 12.4*. They should include proper attribution and citation as defined in *Sections 12.6.2*.

12.2.1 By students:

Students may incorporate portions of lawfully acquired copyrighted works when producing their own educational multimedia projects for a specific course.

12.2.2 By Educators for Curriculum-Based Instruction:

Educators may incorporate portions of lawfully acquired copyrighted works when producing their own educational multimedia programs for their own teaching tools in support of curriculum-based instructional activities at educational institutions.

12.3. PERMITTED USES OF EDUCATIONAL MULTIMEDIA PROGRAMS CREATED UNDER THESE GUIDELINES

Uses of educational multimedia projects created under these guidelines are subject to the Time, Portion, Copying and Distribution Limitations listed in *Section 12.4.*

12.3.1 Student Use:

Students may perform and display their own educational multimedia projects created under *Section 12.2* of these guidelines for educational uses in the course for which they were created and may use them in their own portfolios as examples of their academic work for later personal uses such as job and graduate school interviews.

12.3.2 Educator Use for Curriculum-Based Instruction:

Educators may perform and display their own educational multimedia projects created under *Section 12.2* for curriculum-based instruction to students in the following situations:

12.3.2.1 For face-to-face instruction,

12.3.2.2 Assigned to students for directed self-study,

12.3.2.3 For remote instruction to students enrolled in curriculum-based courses and located at remote sites, provided over the educational institution's secure electronic network in real-time, or for after class review or directed self-study, provided there are technological limitations on access to the network and educational multimedia project (such as a password or PIN) and provided further that the technology prevents the making of copies of copyrighted material.
If the educational institution's network or technology used to access the educational multimedia project created *under Section 12.2* of these guidelines cannot prevent duplication of copyrighted material, students or educators may use the multimedia educational projects over an otherwise secure network for a period of only 15 days after its initial real-time remote use in the course of instruction or 15 days after its assignment for directed self-study. After that period, one of the two use copies of the educational multimedia project may be placed on reserve in a learning resource center, library or similar facility for on-site use by students enrolled in the course. Students shall be advised that they are not permitted to make their own copies of the multimedia project.

12.3.3 Educator Use for Peer Conferences:
Educators may perform or display their own multimedia projects created under *Section 12.2* of these guidelines in presentations to their peers, for example, at workshops and conferences.

12.3.4 Educator Use for Professional Portfolio
Educators may retain educational multimedia projects created under *Section 12.2* of these guidelines in their personal portfolios for later personal uses such as tenure review or job interviews.

12.4. LIMITATIONS – TIME, PORTION, COPYING & DISTRIBUTION
The preparation of educational multimedia projects incorporating copyrighted works under *Section 12.2,* and the use of such projects under *Section 12.3,* are subject to the limitations noted below.

12.4.1 Time Limitations
Educators may use their educational multimedia projects created for educational purposes under *Section 12.2* of these guidelines for teaching courses, for a period of up to two years after the first instructional use with a class. Use beyond that time period, even for educational purposes, requires permission for each copyrighted portion incorporated in the production. Students may use their educational multimedia projects as noted in *Section 12.3.1*.

12.4.2 Portion Limitations
Portion limitations mean the amount of a copyrighted work that can reasonably be used in educational multimedia projects under these guidelines regardless of the original medium from which the copyrighted works are taken. **In the aggregate** means *the total amount of copyrighted material from a single copyrighted work that is permitted to be used in an educational multimedia project without permission under these guidelines.* These limits apply cumulatively to each educator's or student's multimedia project(s) for the same academic semester, cycle or term. All students should be instructed about the reasons for copyright protection and the need to follow these guidelines. It is understood, however, that students in kindergarten through grade six may not be able to adhere rigidly to the portion limitations in this section in their independent development of educational multimedia projects. In any event, each such project retained under *Sections 12.3.1* and *12.4.3* should comply with the portion limitations in this section.

12.4.2.1 Motion Media
Up to 10% or 3 minutes, whichever is less, in the aggregate of a copyrighted motion media work may be reproduced or otherwise incorporated as part of a multimedia project created under *Section 12.2* of these guidelines.

12.4.2.2 Text Material
Up to 10% or 1000 words, whichever is less, in the aggregate of a copyrighted work consisting of text material may be reproduced or otherwise incorporated as part of a multimedia project created under *Section 12.2* of these guidelines. An entire poem of less than 250 words may be used, but no more than three poems by one poet, or five poems by different poets from any anthology may be used. For poems of greater length, 250 words may be used but no more than three excerpts by a poet, or five excerpts by different poets from a single anthology may be used.

12.4.2.3 Music, Lyrics, and Music Video

Up to 10%, but in no event more than 30 seconds, of the music and lyrics from an individual musical work (or in the aggregate of extracts from an individual work), whether the musical work is embodied in copies, or audio or audiovisual works, may be reproduced or otherwise incorporated as a part of a multimedia project created under *Section 12.2.* Any alterations to a musical work shall not change the basic melody or the fundamental character of the work.

12.4.2.4 Illustrations and Photographs

The reproduction or incorporation of photographs and illustrations is more difficult to define with regard to fair use because fair use usually precludes the use of an entire work. Under these guidelines a photograph or illustration may be used in its entirety but no more than 5 images by an artist or photographer may be reproduced or otherwise incorporated as part of an educational multimedia project created under *Section 12.2*. When using photographs and illustrations from a published collective work, not more than 10% or 15 images, whichever is less, may be reproduced or otherwise incorporated as part of an educational multimedia project created under Section 2.

12.4.2.5 Numerical Data Sets

Up to 10% or 2500 fields or cell entries, whichever is less, from a copyrighted database or data table may be reproduced or otherwise incorporated as part of a educational multimedia project created under Section 2 of these guidelines. A field entry is defined as a specific item of information, such as a name or Social Security number, in a record of a database file. A cell entry is defined as the intersection where a row and a column meet on a spreadsheet.

12.4.3 Copying and Distribution Limitations

Only a limited number of copies, including the original, may be made of an educator's educational multimedia project. For all of the uses permitted by *Section 12.3*, there may be no more than two use copies only one of which may be placed on reserve as described in *Section 12.3.2.3.*

An additional copy may be made for preservation purposes but may only be used or copied to replace a use copy that has been lost, stolen, or damaged. In the case of a jointly created educational multimedia project, each principal creator may retain one copy but only for the purposes described in *Sections 12.3.3* and *12.3.4* for educators and Section *12.3.1* for students.

12.5. EXAMPLES OF WHEN PERMISSION IS REQUIRED

12.5.1 Using Multimedia Projects for Non-Educational or Commercial Purposes

Educators and students must seek individual permissions (licenses) before using copyrighted works in educational multimedia projects for commercial reproduction and distribution.

12.5.2 Duplication of Multimedia Projects beyond Limitations Listed in These Guidelines

Even for educational uses, educators and students must seek individual permissions for all copyrighted works incorporated in their personally created educational multimedia projects before replicating or distributing beyond the limitations listed in *Section 12.4.3*.

12.5.3 Distribution of Multimedia Projects beyond Limitations Listed in These Guidelines

Educators and students may not use their personally created educational multimedia projects over electronic networks, except for uses as described in Section *12.3.2.3*, without obtaining permissions for all copyrighted works incorporated in the program.

12.6. IMPORTANT REMINDERS

12.6.1 Caution in Downloading Material from the Internet

Educators and students are advised to exercise caution in using digital material downloaded from the Internet in producing their own educational multimedia projects, because there is a mix of works protected by copyright and works in the public domain on the network. Access to works on the Internet does not automatically mean that these can be reproduced and reused without permission or royalty payment and, furthermore, some copyrighted works may have been posted to the Internet without authorization of the copyright holder.

12.6.2 Attribution and Acknowledgement

Educators and students are reminded to credit the sources and display the copyright notice © and copyright ownership information if this is shown in the original source, for all works incorporated as part of the educational multimedia projects prepared by educators and students, including those prepared under fair use. Crediting the source must adequately identify the source of the work, giving a full bibliographic description where available (including author, title, publisher, and place and date of publication). The copyright ownership information includes the copyright notice (©, year of first publication and name of the copyright holder).

The credit and copyright notice information may be combined and shown in a separate section of the educational multimedia project (e.g. credit section) except for images incorporated into the project for the uses described in *Section 12.3.2.3*. In such cases, the copyright notice and the name of the creator of the image must be incorporated into the image when, and to the extent, such information is reasonably available; credit and copyright notice information is considered "incorporated" if it is attached to the image file and appears on the screen when the image is viewed. In those cases when displaying source credits and copyright ownership information on the screen with the image would be mutually exclusive with an instructional objective (e.g. during examinations in which the source credits and/or copyright information would be relevant to the examination questions), those images may be displayed without such information being simultaneously displayed on the screen. In such cases, this information should be linked to the image in a manner compatible with such instructional objectives.

12.6.3 Notice of Use Restrictions

Educators and students are advised that they must include on the opening screen of their multimedia program and any accompanying print material a notice that certain materials are included under the fair use exemption of the U.S. Copyright Law and have been prepared according to the multimedia fair use guidelines and are restricted from further use.

12.6.4 Future Uses beyond Fair Use

Educators and students are advised to note that if there is a possibility that their own educational multimedia project incorporating copyrighted works under fair use could later result in broader dissemination, whether or not as commercial product, it is strongly recommended that they take

steps to obtain permissions during the development process for all copyrighted portions rather than waiting until after completion of the project.

12.6.5 Integrity of Copyrighted Works: Alterations
Educators and students may make alterations in the portions of the copyrighted works they incorporate as part of an educational multimedia project only if the alterations support specific instructional objectives. Educators and students are advised to note that alterations have been made.

12.6.6 Reproduction or Decompilation of Copyrighted Computer Programs
Educators and students should be aware that reproduction or decompilation of copyrighted computer programs and portions thereof, for example the transfer of underlying code or control mechanisms, even for educational uses, are outside the scope of these guidelines.

12.6.7 Licenses and Contracts
Educators and students should determine whether specific copyrighted works, or other data or information are subject to a license or contract. Fair use and these guidelines shall not preempt or supersede licenses and contractual obligations.

Appendix

ORGANIZATIONS ENDORSING THESE GUIDELINES:

Agency for Instructional Technology (AIT)
American Association of Community Colleges (AACC)
American Society of Journalists and Authors (ASJA)
American Society of Media Photographers, Inc. (ASMP)
American Society of Composers, Authors and Publishers (ASCAP)
Association for Educational Communications and Technology (AECT)
Association for Information Media and Equipment (AIME)
*Association of American Publishers (AAP)**
Association of American Colleges and Universities (AAC&U)
Association of American University Presses, Inc. (AAUP)
Broadcast Music, Inc. (BMI)
Consortium of College and University Media Centers (CCUMC)
*Creative Incentive Coalition (CIC)***
Iowa Association for Communications Technology (IACT)
Information Industry Association (IIA)
Instructional Telecommunications Council (ITC)
Maricopa Community Colleges/Phoenix
Motion Picture Association of America (MPAA)
Music Publishers' Association of the United States (MPA)
National Association of Regional Media Centers (NARMC)
Recording Industry Association of America (RIAA)
Software Publishers Association (SPA)

U.S. GOVERNMENT AGENCIES SUPPORTING THESE GUIDELINES:

U.S. National Endowment for the Arts (NEA)
U.S. Copyright Office
U.S. Patent and Trademark Office

INDIVIDUAL COMPANIES AND INSTITUTIONS ENDORSING THESE GUIDELINES:

Houghton-Mifflin
John Wiley & Sons, Inc.
McGraw-Hill
Time Warner, Inc.

13. APPENDIX C – Austin Banner Council (ABC)

13.1 Section 1 – Name & Purpose

13.1.1 – Name: The group shall be called the *Austin Banner Council*, hereafter referred to as *ABC*.

13.1.2 – Purpose: The primary purpose of ABC shall be to facilitate effective management of the administrative computer system (hereafter referred to as *Banner*) for Concordia University Texas. To that end, ABC shall supervise Banner with regard to –

- ✓ *Policies and procedures directly related to Banner operation*
- ✓ *End-user access*
- ✓ *Training procedures*
- ✓ *Product development and Banner modification*
- ✓ *Process documentation*
- ✓ *Data and disaster recovery procedures*

As part of its supervisory responsibilities, ABC shall maintain appropriate communication with the Administrative Council by providing monthly status reports on committee activities and decisions. In addition, ABC shall develop ways to keep the entire campus community apprised of Banner development.

13.2 Section 2 – Organization & Management

13.2.1 – Membership: ABC shall consist of ten (10) voting members. The group will be comprised of one representative from each functional area within Banner:

1. *Admissions*
2. *Alumni/Development*
3. *Finance/Accounts Receivable*
4. *Financial Aid*
5. *Human Resources*
6. *Registrar's Office*
7. *Student Services*
8. *Information & Technology Services (ITS)*

Two representatives will sit on the council as voting members in recognition of their unique roles and responsibilities within the university:

9. *Registrar* – as campus FERPA officer
10. *College of Adult Education* – representing extended campus operations

The vice president responsible for each functional area shall appoint an individual to serve in the respective council voting position. Appointments shall be made annually and run for twelve (12) months to correspond with the university's fiscal year (July 1 – June 30). Individuals serving in each position shall be directly accountable to their respective vice president.

The council shall hold monthly meetings. At its July meeting, the council shall elect a chairperson, vice chairperson and recording secretary.

13.2.2 – Management & accountability: While individuals serving on ABC are accountable to their respective vice president, the group as a whole is directly accountable to the Administrative Council. All Banner policy decisions are subject to review and approval by the Administrative Council. ABC shall manage Banner operations within the constraints of the annual budget allocated by the Administrative Council. Any decisions that impact the university budget must have prior approval by the Administrative Council prior to any implementation.

13.3 Section 3 – Duties

13.3.1 – Chairperson: The chairperson shall facilitate all ABC meetings utilizing the latest edition of Robert's Rules of Order. While each council member has a responsibility to support and implement all ABC decisions, the chairperson shall work to facilitate compliance with Banner policies throughout the university. The chairperson shall create and distribute an agenda to all council members at least 24 hours prior to each ABC meeting.

13.3.2 – Vice chairperson: The vice chairperson shall serve in the capacity of chairperson should that individual be unable to perform their respective duties, chairing meetings when the chairperson is not present.

13.3.3 – Recording secretary: The recording secretary shall be responsible for maintaining an accurate record of all ABC meetings. Minutes, along with any council recommendations, shall be sent to all members of the Administrative Council within five (5) business days following an ABC meeting.

13.3.4 – Council members: Council members shall corporately and individually strive to:

- ✓ Protect the integrity of administrative data.
- ✓ Ensure data required by institutional, state and federal agencies are accurately maintained and appropriately accessible.
- ✓ Formulate and document standards, policies and procedures for entry, maintenance and disposal of shared data.
- ✓ Identify and appropriately address Banner issues within all university departments.
- ✓ Communicate information on Banner development and management utilizing forums, electronic messages, and other effective methods of communication within the university community.

13.4 Section 4 – Access Control

13.4.1 – Security: User access to Banner modules, screens, forms and views must be approved by the appropriate ABC representative. The areas and appropriate representatives are:

- ✓ **Admissions:** Admissions
- ✓ **Financial Aid:** Financial Aid
- ✓ **Finance:** Finance
- ✓ **General:** ITS
- ✓ **Housing:** Student Services

- ✓ **Human Resources:** Human Resources
- ✓ **Payroll:** Finance
- ✓ **Student:** Registrar's Office