Excerpted from Southwestern College Policy Manual

Computing Policies

Policy Statement

Southwestern College expects all members of its community to use electronic communications in a responsible manner. The college may restrict the use of its computers and network systems for electronic communications, in response to complaints presenting evidence of violations of this policy or state or federal laws. Specifically, the college reserves the right to limit access to its networks through college-owned or other computers, and to remove or limit access to material posted on college-owned computers.

Southwestern College cherishes the diversity of values and perspectives endemic in an academic institution and is respectful of freedom of expression. Therefore, it does not condone censorship, nor does it endorse the inspection of files other than on an exceptional basis. As a result, Southwestern College cannot protect individuals against the existence or receipt of material that may be offensive to them.

Purpose of the Policy

Southwestern College seeks to enforce its policies regarding harassment and the safety of individuals; to protect the college against seriously damaging or legal consequences; to prevent the posting of proprietary software or the posting of electronic copies of literary works in disregard of copyright restrictions or contractual obligations; to safeguard the integrity of computers, networks, and data, either at Southwestern or elsewhere, and to ensure that use of electronic communications complies with the provisions of other policies and codes for maintaining public order or the educational environment.

Individuals Covered by this Policy

This policy applies to Southwestern College students, staff, administrators, and faculty, as well as others who have been approved for access to Southwestern's network.

Overview of the Policy

Policy Definitions

These definitions apply to these terms as they are used in this policy.

1. **Education Records.** Records specifically related to a student and maintained by an educational institution or a party acting on its behalf. These records are protected by the Family Educational Rights and Privacy Act of 1974.

2. **Electronic Communications.** The use of computers and network systems in the communicating or posting of information or material by way of electronic mail, bulletin boards, or other such electronic tools.

3. **Network Systems.** Includes voice, video and data networks, switches, routers and storage devices.

4. **System or Network Administrator.** A college employee responsible for managing the operation or operating system environments of computers or network systems, respectively.

5. **College Computers and Network Systems.** Computers, networks, servers, and other similar devices that are administered by the college and for which the college is responsible.

6. **Southwestern College Community.** Southwestern College students, staff, administrators, and faculty, as well as others who have been approved for access to Southwestern's network.

7. **CIC.** Computer Information Center.

Introduction to the Policy

Computers and network systems offer powerful tools for communication among members of the Southwestern College community and of communities outside of the college. When used appropriately, these tools can enhance dialog and communications. Unlawful or inappropriate use of these tools, however, can infringe on the rights of others. The college expects all members of its community to use electronic communications in a responsible manner.

The use of computers or network systems in no way exempts any member of the Southwestern College community from the normal requirements of ethical or legal behavior in the Southwestern community. In particular, data, software, and computer capacity have value and must be treated accordingly. Use of a computer and network system that is shared by many users imposes certain additional obligations.

Legitimate use of a computer or network system does not extend to whatever an individual is capable of doing with it. Although some rules are built into the system itself, these restrictions cannot limit completely what an individual can do or can see. In any event, each member of the community is responsible for his/her actions whether or not rules are built in, and whether or not they can be circumvented.

Policy Specifics

Southwestern College reserves the right to limit access to its networks when applicable college policies or codes, contractual obligations, or state or federal laws are violated, but does not monitor or generally restrict the content of material transported across those networks.

Southwestern College reserves the right to remove or limit access to material posted on college-owned computers when applicable college policies or codes, contractual obligations, or state or federal laws are violated, but does not monitor the content of material posted on college-owned computers.

Southwestern College does not monitor or generally restrict material residing on college computers housed within a private domain or on non-college computers, whether or not such computers are attached to campus networks.

Principles of Behavior

Members of the college community are expected to follow certain principles of behavior in making use of computers and network systems, in particular, to respect, and to observe policies and procedures governing:

a. the privacy of or other restrictions placed upon data or information stored in or transmitted across computers and network systems, even when that data or information is not securely protected;

b. an owner's interest in proprietary software or other assets pertaining to computers or network systems, even when such software or assets are not securely protected;

c. the finite capacity of computers or network systems by limiting use of computers and network systems so as not to interfere unreasonably with the activity of other users.

Members of the college community also are expected to follow all other policies, rules, or procedures established to manage computers or network systems, including those established to control access to, or the use of, computer data, files, or other information.

Those who cannot accept these standards of behavior will be denied use of Southwestern College computers or network systems. Violators may also be subject to penalties under college regulations and under state and federal laws.

Appropriate Use of Electronic Communications Services

The college recognizes the complexity of deciding what constitutes appropriate use of electronic communications services. What is appropriate or inoffensive to some members of the community may be inappropriate or offensive to others.

Caution: Having open access to network-based services implies some risk. In a community of diverse cultures, values, and sensitivities, the college cannot protect individuals against the existence or receipt of material that may be offensive to them.

Southwestern College does not condone censorship, nor does it endorse the inspection of electronic files other than on an exceptional basis (i.e., if required to ensure the integrity, security, or effective operation of college systems).

Nevertheless, the college reserves the right to place restrictions on the use of its computers and network systems in response to complaints presenting evidence of violations of this policy or other college policies or codes, or state or federal laws. Once evidence is established, the college authorities responsible for overseeing these policies and codes will be consulted on the appropriateness of specific restrictions, which could include the removal of material posted on a computer and/or limiting access to the college's networks.

Caution: In exceptional cases, CIC personnel may detect evidence of a violation while performing his or her duties operating or maintaining a system. In such instances, the individual should contact the vice president for information technology for further guidance.

Caution: This policy does not abrogate local policies governing the operation and maintenance of college systems provided they do not conflict with the precepts of college policy. Departments and administrative units may wish to develop ancillary procedures that support organizational requirements. Specifically, procedural guidelines with regard to security, privacy, and other areas of critical importance to the administration of these systems are not addressed as part of this policy, nor are violations of principles of network etiquette.

Policy Violations

This section presents a list of the kinds of violations covered by this policy. For reporting procedures see the section on reporting procedures.

Violations Targeted at a Specific Individual(s)

1. Sending repeated and unwanted (harassing) communication by electronic mail or other electronic communications. (See the section on harassment for additional information.)

2. Sending repeated and unwanted (harassing) communication by electronic mail or other electronic communications that is sexual in nature. (See the section on harassment for additional information.)

3. Sending repeated and unwanted (harassing) communication by electronic mail or other electronic communications that is motivated by race, ethnicity, religion, gender, or sexual orientation. (See the section on harassment for additional information.)

4. Posting or otherwise disseminating personal or sensitive information about an individual(s). (See the section on posting personal or sensitive information for additional information.)

Violations Causing Harm to the Activities of Others

1. Propagating electronic chain mail. (See the section on sending chain e-mail for additional information.)

2. Interfering with freedom of expression of others by "jamming" or "bombing" electronic mailboxes. (See the sections on e-mail bombing and interfering with the activities of others for additional information.)

3. Forging, fraudulently altering, or willfully falsifying electronic mail headers, electronic directory information, or other electronic information generated as, maintained as, or otherwise identified as college records in support of electronic communications. (See the section on forgery for additional information.)

4. Using electronic communications to forge an academic document. (See the section on forgery for additional information.)

5. Using electronic communications to hoard, damage, or otherwise interfere with academic resources accessible electronically.

6. Using electronic communications to steal another individual's works, or otherwise misrepresent one's own work.

7. Using electronic communications to work together on examinations, papers or any other academic work unless permission to do so has been granted by the instructor.

8. Using electronic communications to fabricate research data.

Violations Involving Illegal, Proprietary, or Damaging Material

1. Electronically distributing or posting copyrighted material in violation of license restrictions or other contractual agreements. (See the sections on copyright rules, copyright infringement, and software piracy for additional information.)

2. Launching a computer worm, computer virus or other rogue program.

3. Downloading or posting illegal, proprietary or damaging material to a college computer. (See the sections on copyright rules, copyright infringement, and software piracy for additional information.)

4. Transporting illegal, proprietary or damaging material across Southwestern's networks. (See the sections on copyright rules, copyright infringement, and software piracy for additional information.)

D. Violations Targeted at Classes of Individuals

Posting hate speech regarding a group's race, ethnicity, religion, gender, or sexual orientation. (See the section on hate speech for additional information.)

Adult Material

Adult Pornography. Pornography is a generic term for erotic material of all types. In general, pornography receives full First Amendment protection, but there are several important exceptions. For example, see the sections on child pornography, distribution or pornography to minors, and obscenity.

Possession of adult material is not a violation of Southwestern College policy or code unless the material is illegal. Any activity that is illegal is a violation of Southwestern College policy. Offenders may be investigated and/or prosecuted by the appropriate local, state or federal authorities. Southwestern College does not monitor or censor discussion groups, newsgroups, electronic mail or any other electronic communications.

Southwestern does not censor or filter adult materials.

Child Pornography. Child pornography, material that depicts minors in a sexually explicit way, is illegal. Under the federal child pornography statute 18 USC section 2252, anyone under the age of 18 is a minor. States also have child pornography statues and the age of minority varies by state. Knowingly uploading or downloading child pornography is a federal offense. It is also illegal to advertise or seek the sale, exchange, reproduction or distribution of child pornography. Lewd exhibition of genitals can constitute sexual conduct and therefore, any graphic files containing images of naked children could violate the federal child pornography statute.

Distribution of Pornography to Minors. Possession of non-obscene adult pornography is legal, but it is illegal to distribute to minors.

Obscenity. Obscenity, by definition, is a type of pornography that is not protected by the First Amendment. Virtually every state and municipality has a statute prohibiting the sale and distribution of obscenity, and the federal government prohibits its interstate transportation. The Supreme Court in Miller v. California, 413 U.S. 15, (1973), narrowed the permissible scope of obscenity statutes and applied this three part test to determine constitutionality: (a) whether the average person applying contemporary community standard would find the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes in a patently offensive way sexual conduct specifically defined in applicable state law; and (c) whether the work taken as a whole lacks serious literary, artistic, political, or scientific value.

The contemporary community standard is historically the standard of the community in which the material exists. Many on-line activists argue that the contemporary community standard in cases that arise on-line ought to be determined by the on-line community. However, a federal prosecution of a California couple that offered a members-only bulletin board service, concentrating on pornography, resulted in a conviction of the California couple under the federal obscenity statute and Tennessee community standards. In that case a postal worker in Memphis downloaded some material from this California bulletin board service. See United States v. Thomas, 1996 U.S. App. LEXIS 1069 (6th Cir. Jan. 29, 1996).

Harassment

Harassment, is any verbal or physical conduct, on or off campus, which has the intent or effect of unreasonably interfering with an individual's or group's educational or work performance or which creates an intimidating, hostile, or offensive educational or work environment. Harassment on the basis of race, color, gender, disability, religion, national origin, sexual orientation, or age includes harassment of an individual in terms of a stereotyped group characteristic, or because of that person's identification with a particular group. With reference to sexual harassment, the definition also includes unwelcome sexual advances and requests for sexual favors, which might be perceived as explicitly or implicitly affecting educational, or employment decisions concerning an individual.

Sending unwanted and/or offensive e-mail or messages may constitute harassment and is in violation of the intended use of the system. In general, communication targeted at a specific individual with the intent to harass or threaten is a violation of Southwestern College policy.

Hate Speech

Uncivil, antagonistic or derogatory speech that is disrespectful of classes of people is commonly referred to as hate speech. Although hate speech may be extremely offensive (particularly to members of the targeted group), posting hate speech does not generally constitute a violation of this policy. This is because, especially as an educational institution, Southwestern is committed to the protection of freedom of expression. In exceptional cases, however, the college may decide that hate speech directed to classes of individuals presents such a hostile environment that certain restrictive actions are warranted. Certain types of postings or communications may constitute harassment, which is a violation of this policy, and in some cases, state or federal laws. Contact the vice president for information technology for additional information or assistance.

Copyright Rules

It is the policy of Southwestern College that faculty, administration, staff, and students shall rigorously respect the licensing agreement under which computer software is purchased and used. Except that such action is specifically allowed in writing by the license agreement or authorized written exception thereto, it shall be against this policy to:

a. Make copies of copyrighted computer disks.

b. Make copies of copyrighted manuals.

c. Load disks into computers other than the computer for which the license is granted.

d. Remove any copyrighted material from its proper custodian or custodial area.

e. Lend any copyrighted material to another person without the permission of the proper custodian.

f. Prepare derivative works based upon the copyrighted material. This includes alternate hardware versions.

g. No college device shall be used to copy material in violation of any license agreement, even if that copyrighted material is owned by another.

See the section on copyright infringement for additional information.

Specific Examples of Violations of Southwestern College Policy

This section describes what activities constitute violations of this policy.

Examples (not a comprehensive list) of policy violations include:

Commercial use of college resources. Non-sanctioned commercial use of college computers and network systems is considered a violation of policy. Using e-mail to solicit sales or conduct business, setting up a web page to advertise or sell a service, or posting an advertisement to a news group all constitute commercial use. Even if you use your own personal computer, but you use the college's network (either from a dorm room, office or via dial-in access from home), you are in violation of the policy.

Computer theft (including theft of computer services, intellectual property such as copyrighted material, and any other property)

Computer trespass (unauthorized use of computers to delete or alter data or interfere with others' usage)

E-mail bombing. Flooding someone with numerous or large e-mail messages in an attempt to disrupt them or their site is known as "e-mail bombing". Often this is done to retaliate because someone has done something annoying. But more often than not e-mail bombing will either cause problems for your local system or disrupt service for thousands of other innocent bystanders.

Foreign Wireless Access Points. Using non-college-owned/installed devices to access the computer network via a wireless link.

Forgery. Altering electronic communications to hide your identity with the intent to defraud or to impersonate another person is considered forgery. All e-mail, news posts, chat sessions, discussion groups, or any other form of communication should contain your name and/or username. Southwestern recognizes that there are situations where maintaining ones anonymity may be advisable and even required for safety reasons. Some examples include AOL Instant Messenger and other chat software that will not accept real names. Situations like these, where the intent is not to defraud or to impersonate, are not considered violations of this policy. However, forgery includes using another person's identity. Forgeries intended as pranks or jokes are still considered violations.

Illegal activities. Everything listed under what is illegal under local, state, and federal laws is a violation of Southwestern College policy. This is not a comprehensive list, but it contains the activities most frequently asked about.

Interfering with activities of others. This can be any activity that disrupts a system and interferes with other people's ability to use that system. In some cases, consuming more than your "fair" share of resources can constitute interference. Some examples are:

a. e-mail bombing that causes a disk to fill up, the network to bog down, or an e-mail application to crash;

b. taking advantage of a network split to take over a chat channel and then kicking off or blocking other users;

c. posting many messages to a single news group, discussion group, or mailing list making it difficult for subscribers to carry on their normal discussion;

d. flooding a chat channel with a continuous stream of messages so that it disrupts the conversation.

e. sending a large number of e-mail messages to one or more individuals causing the network to bog down. (Contact the Vice president for information technology for assistance in seeking alternative methods of disseminating large amounts of information.)

Making more copies of licensed software than the license allows (i.e. software piracy)

Misleading transmittal of names or trademarks (falsely identifying yourself or falsely claiming to speak for a person or organization by using their name, trademark, logo, or seal)

Modifying or reconfiguring the software or hardware of a college computer. No one should modify the hardware, operating system, or application software of a college computer unless they have been given permission to do so by the department or individual that is in charge of the machine. The other users with whom you share the machine, and the technicians, on whom you rely for support, are expecting to find it set up exactly the way they left it.

Posting or otherwise disseminating personal or sensitive information about an individual(s). Examples include postings of an individual's academic records; medical information; social security number; or similar information of a personal or confidential nature that, if disseminated, could have legal or otherwise damaging implications either for the targeted person or the institution. Personal expression by an individual about another, even if posted in a public manner, is not subject to limitation or restriction under this policy, although a targeted person may have recourse under other campus policies or codes, or state or federal laws regarding harassment.

Preventing others from accessing services (e.g. taking over a chat channel and kicking other users off.

Releasing a virus, worm or other program that damages or otherwise harms a system or network

Sending a crippling number of files across the network (e.g. e-mail "bombing")

Sending chain e-mail and virus hoaxes. The most important thing to remember is if you get chain e-mail, do not help propagate it. Chain e-mail usually contains phrases like "pass this on", "forward - do not delete", "don't break the chain", "this is safe, don't worry", "let's see how long this takes to get back to the start", "this has been around the world 20 times", "7 years of good luck!", "I don't wanna die", "your mom would want you to do this", etc. Often there is some story about how lucky a person has been since they forwarded the chain e-mail, or how unlucky they were because they didn't. Sometimes chain e-mail is disguised - it tells of some kid who is dying and wants post cards, or it warns about e-mail viruses or Internet shutdowns. Don't fall for it. It's all chain mail and it's designed to get you to forward it.

In recent years, chain mail hoaxes of various sorts have become widespread on the Internet. Some are virus warnings like "Good Times", "PenPal", and "Irina". Others are like the "Naughty Robot" that claims to have all your credit card numbers. They tell you to forward the "warning" to everyone you know. Most hoaxes start out as pranks, but often live on for years, getting passed around by new people who have just joined the Internet community. Don't believe every warning you get via e-mail. You should not pass these warnings on unless you verify the authenticity. You should contact the computer information center for additional information.

Sharing usernames and passwords (unauthorized use). Your username and password are provided only for your personal use. Passwords provide access to a wide range of services that are restricted for use by you personally or are restricted for use by the Southwestern College community (such as e-mail, PowerCAMPUS, library services, news, chat, and discussion groups). If you share your password with spouses, family members, friends or roommates, then you are giving them access to services they are not authorized to use. They will also have access to all of your personal information. They may even embarrass you by posting to a news group in your name or by posing as you in a chat session, or discussion group. If you forget your password, the CIC will only give the password to you. CIC will NEVER request your username and password or other personally identifiable information through email.

Tapping phone or network lines. Running a network "sniffer" program to examine or collect data from the network is considered tapping a network.

Unauthorized access. As stated in this policy, legitimate use of a computer or network does not extend to whatever an individual is capable of doing. In some cases, operating systems have security holes or other loopholes that people can use to gain access to the system or to data on that system. This is considered unauthorized access. If someone inadvertently turns on file sharing on their personal computer, you do not have the right to read or delete their files unless you have been given explicit permission from the owner.

Unauthorized access to data or files even if they are not securely protected (e.g. breaking into a system by taking advantage of security holes, or unauthorized access to financial or personal data)

Using college resources for unauthorized purposes (e.g. using personal computers connected to the campus network to set up web servers for illegal, commercial or profit-making purposes).

What are NOT Violations of Southwestern College Policy?

Breaches of network etiquette. Things like off-topic postings to lists and news groups, advertising by posting the same message to numerous lists (also known as "spamming"), rude or impolite behavior, heated arguments (or flame wars), and some forms of hate speech will often annoy others. Remember that the Internet spans the globe as well as numerous diverse cultures and societies. What is acceptable in one may be totally inappropriate in another. Keep in mind that it is easy to misunderstand electronic communications due to the lack of personal contact involved. You can avoid problems by "listening" for a while when you join a group. After you determine what is acceptable, then go ahead and post. If you participate in a discussion and someone posts off-topic, be polite in pointing out the mistake and do not assume it is deliberate.

Southwestern College is not in a position to control etiquette. When these sorts of problems come up, you should try to work them out with the other people involved, just as you do in other areas of your life.

In some cases, rude behavior can cause disruptions. Any behavior that interferes with the ability of others to access or use a system is a violation of policy.

Hate Speech. Posting hate speech does not generally constitute a violation of this policy. Although certain postings or communications may be offensive to members of the community, Southwestern College is respectful of expression in its own right. See the section on hate speech for more information.

Unsolicited e-mail or junk e-mail. The amount of unwanted or unsolicited e-mail (junk mail) has been increasing as more people join the Internet community. You get things like this in the U.S. Postal mail on a regular basis - catalogs, advertisements, solicitations, and political propaganda are some examples. This form of speech is usually protected under the first amendment, even though some people may find some of the content objectionable. Southwestern College does not monitor or censure e-mail and therefore cannot prevent the flow of junk mail.

Remember that junk mail is NOT illegal and it is NOT a violation of Southwestern College policies or codes. You can either delete and ignore junk e-mail (this is the recommended approach) or contact the sender and ask to be removed from any mailing list they have—just as you would do with U.S. Postal mail. Many people ask why the college does not put a stop to junk mail. Most junk mail comes from sites around the Internet, not from within Southwestern. We have no control over what these sites send and cannot distinguish unwanted junk mail from e-mail that people want to receive. It needs to stop at the source. In fact, a growing number of people around the Internet are trying to get junk mail outlawed. If junk mail becomes illegal, it will then become a violation of Southwestern College policy as well since any illegal activity constitutes a violation of policy.

What Is Illegal Under Local, State and Federal Laws?

Any activity that is illegal is a violation of Southwestern College policy. Offenders may be investigated and/or prosecuted by the appropriate local, state or federal authorities.

Examples (not a comprehensive list) of policy violations include:

Bomb Threats and Hoaxes. It is illegal to send a message via e-mail that threatens other persons or property. While this might seem obvious, every year a number of individuals send what they believe are "hoax messages". Such messages may be investigated by federal authorities with the result that the senders end up with their names in the files of the FBI and/or CIA. This is not an exaggeration!

It is a violation of this policy to send certain kinds of hoax messages (for example, April Fool's jokes that appear to be from a professor or some other college official). Such hoaxes constitute forgery and will be referred for appropriate disciplinary action.

Child Pornography. Knowingly uploading or downloading child pornography is a federal offense. See the section on child pornography for more information.

Copyright Infringement. Almost all forms of original expression that are fixed in a tangible medium are subject to copyright protection, even if no formal copyright notice is attached. Written text (including e-mail messages and news posts), recorded sound, digital images, and computer software are some examples of works that can be copyrighted. Unless otherwise specified by contract, the employer generally holds the copyright for work done by an employee in the course of employment.

Copyright holders have many rights, including the right to reproduce, adapt, distribute, display, and perform their work. Reproducing, displaying or distributing copyrighted material without permission infringes on the copyright holder's rights. However, "fair use" applies in some cases. If a small amount of the work is used in a non-commercial situation and does not economically impact the copyright holder it may be considered fair use. For example, quoting some passages from a book in a report for a class assignment would be considered fair use. Linking to another web page from your web page is not usually considered infringement. However, copying some of the contents of another web page into yours or use of video clips without permission would likely be infringement.

Distribution of Pornography to Minors. Possession of non-obscene adult pornography is legal, but it is illegal to distribute to minors. See the section on adult material for more information.

Federal Computer Security Violations. The primary federal statute regarding computer fraud 18 USC section 1030 was amended in October 1996 to protect computer and data integrity, confidentiality and availability. Examples of violations are:

a. theft of information from computers belonging to financial institutions or federal agencies, or computers used in interstate commerce;

b. unauthorized access to government computers;

c. damage to systems or data (intentionally or recklessly);

d. trafficking in stolen passwords;

e. extortionate threats to damage computers.

Obscenity. Obscenity is illegal. See the section on obscenity for more information.

Scams and Pyramid Schemes. Beware of moneymaking "opportunities" on the Internet. A common scam is the pyramid scheme. You get an e-mail message with a subject like "MAKE MONEY FAST" and it instructs you to send money to the people on the list and then add your name to the bottom of the list and send it on to some number of people. At Southwestern College, this is considered chain mail, but it is also illegal under 18 USC section 1302. The US Postal Service and the Federal Trade Commission

provide information to help individuals identify scams and report them. Pyramid schemes that use US Postal mail to send money are considered mail fraud and can be reported to the USPS

Software Piracy. Unauthorized duplication, distribution or use of someone else's intellectual property, including computer software, constitutes copyright infringement and is illegal and subject to both civil and criminal penalties. The ease of this behavior on-line causes many computer users to forget the seriousness of the offense. As a result of the substantial amounts of money the software industry loses each year from software piracy, the software companies enforce their rights through courts and by lobbying for and getting stiffer criminal penalties.

Video and Audio Recording Piracy. Another form of copyright infringement is the unauthorized duplication and distribution of sound recordings. Online piracy is increasing as many people use the Internet to illegally distribute digital audio files (e.g. MP3 format). The Recording Industry Association of America (RIAA) monitors the Internet daily and scans for sites that contain music. They have been successful in getting the sound recordings removed from those sites. You can report violations to the RIAA directly.

Federal copyright law grants the copyright owner in a video and audio recording (typically, a record company) the exclusive right to reproduce, adapt, distribute and, in some cases, digitally transmit their sound recordings. Therefore, the following activities, if unauthorized by the copyright owner, may violate their rights under federal law:

a. Making a copy of all or a portion of a video and audio recording onto a computer hard drive, server or other hardware used in connection with a web site or other online forum. This includes converting a sound recording into a file format (such as a .wav or mp3 file) and saving it to a hard drive or server;

b. Transmitting a copy or otherwise permitting users to download video and audio recordings from a site or other forum; and/or

c. Digitally transmitting to users, at their request, a particular sound recording chosen by or on behalf of the recipient.

If you reproduce or offer full-length video or audio recordings for download without the authorization of the copyright owner, you are in violation of federal copyright law and could face civil as well as criminal penalties. Placing statements on your web site, such as "for demo purposes only" or that the video and audio files must be "deleted within 24 hours," does not prevent or extinguish this liability.

There are several entities you may need to contact before you can use recorded music online. First, you should understand that the copyright in a sound recording is distinct from the copyright in the recording's underlying musical composition. Thus, even if you have secured the necessary licenses for publicly performing musical compositions (from, for example, ASCAP, BMI and/or SESAC) or for making reproductions of musical compositions (from, for examples, the Harry Fox Agency), these licenses only apply to the musical composition, not the audio recording.

Licenses to utilize particular video and audio recordings must be secured from the video and audio recording copyright owners—generally the record company that released the recording.

Reporting Procedures

All violations of this policy should be reported to the vice president for information technology. The vice president for information technology will determine if other college officials, or state or federal

authorities should be contacted. Consultations with the vice president for information technology are confidential.

Unwanted or Harassing E-mail. If you receive unwanted e-mail or other form of communication, you may want to consider notifying the sender that it is unwanted. Many times a person will not realize that their communication is unwanted unless you tell them. If the sender continues to communicate after being placed on notice, or if you feel uncomfortable confronting the sender, the incident should be reported to the vice president for information technology. Save electronic copies of anything that can be used as evidence.

Caution: The return address on an e-mail message may not be the real source of the e-mail. E-mail can be forged, and detecting a forgery can be difficult. Contact the vice president for information technology for more information and assistance.

The vice president for information technology can act upon a complaint only if the sender of the material is a member of the Southwestern College community. If the sender is not a member of the Southwestern community, the vice president for information technology will assist you by referring you to the appropriate sources of help outside the college.

Complaints about unwanted or harassing e-mail must be filed by the targeted person. If appropriate, please encourage the targeted person to contact the vice president for information technology for information or assistance.

Chain E-mail. If you get chain e-mail from someone with a Southwestern College e-mail address, you can report it to the CIC. Save a copy of the chain e-mail as evidence. If you get chain e-mail from someone not affiliated with Southwestern College, you can reply to the sender and let them know you are not happy about getting chain e-mail from them, or you can delete and ignore it. Contact the vice president for information technology for additional information or assistance.

Potential Consequences of Violations. For faculty, administration, staff, and students, as well as others who have been approved for access to Southwestern’s network, violations of this policy will result in disciplinary action in accordance with established policy and/or legal action. This action may include suspension from the privilege of using the college's computers and/or network for a specific period of time. It is recognized this suspension may mean a student will fail a course because of the inability to use the college’s computers and/or network.

For students, violations of this policy may result in one or more of the following actions:

a. A written warning to the offender.

b. A restriction of system access for a specified term.

c. A revocation of all system privileges for a specified term.

d. A statement of charges to the student's account, which could lead to other penalties up to and including probation or suspension.

Violations of these policies incur the same types of disciplinary measures as violations of other college policies or state or federal laws, including criminal prosecution in serious cases.

Policy Update Procedures. It is the responsibility of the vice president for information technology to ensure that this policy remains current and consistent with existing technology. Comments and suggestions should be directed to the vice president for information technology.

Laptop Use and Computer Center Helpdesk

Items Related to General Use

a. You are responsible for backing up files and documents you don't want to lose.

b. Keep all data files in the "My Documents" folder, since that is the default directory. This will speed up the backup process.

c. Call the Laptop Resource Center before buying or installing software for your laptop in order to assure software compatibility.

d. If you have a question or problem with a software program specified by an instructor for a class, please contact the instructor for assistance.

e. CIC staff reserves the right to remove software including reformatting (erasing) the entire hard drive and reinstalling our standard software if we deem necessary.

Items Related to Repair

a. All laptops must be brought to the Laptop Resource Center in Christy for repair. Be sure to bring the power adapter and cables in the carrying case. Remove all personal items from the case. Be sure CDs and DVDs are removed from the laptop.

b. CIC personnel cannot be responsible for loss of disks, CDs and personal items.

c. Not all repairs can be made "while you wait." It may be necessary to send the computer to a service center for repair. The repair process could last a week. You will be provided with a loaner laptop if one is available.

d. Remember the importance of backing up your files. If the unit needs to be sent in for repair, chances are all files on your hard drive will be erased.

Purchasing Computer Hardware and Software

No hardware or software purchase is to be made for the college without the written authorization of the vice president for information technology.

Administration

To implement this policy the following procedures are necessary:

a. Any software purchases must be made by a college purchase order to a recognized vendor. This purchase order must be countersigned by the vice president for information technology. Shipping address should be the computer center so that a copy of the license agreement may be logged. If a purchase is to be made from a private individual, the purchase order must be countersigned by the vice president for finance and human resources. This signature requirement is made so as to insure the private individual has the right to sell the software.

b. A copy of all software licensing agreement shall be forwarded to the CIC procurement specialist.

c. All original software media shall be stored by the CIC procurement specialist for safe keeping.

Web Site Disclaimer

Southwestern College has provided on-line information and services on the Internet for communication purposes only. The college does exert editorial control over pages on the official SCKANS site and has not participated in the development of other Internet sites. The college disclaims any and all liability for injury and other damages that result from information obtained therein.

The content of and links from personal web pages do not represent official statements or views of the college. Furthermore, the college disclaims all responsibility for any violations of copyright laws for any data that users may provide.

The Internet

The college makes the Internet available as part of its continuing effort to provide collections, resources, and services that meet the informational, educational, cultural, and recreational needs of the campus community.

Basic to our policy are the Library Bill of Rights and The Freedom to Read Act. In keeping with those policies, the college does not monitor and has no control over the information accessed through the Internet and cannot be held responsible for its content. As with all formats of information, patrons must respect copyright laws and licensing agreements and abide by general rules of acceptable Internet conduct.

E-Mail Address Retention

Faculty, staff, and administrators who have retired or left the college to pursue other endeavors may retain a Southwestern College e-mail address if they so desire, under the following conditions:

1. Those persons whose length of service to Southwestern College is five years or greater or who are retiring are eligible for this benefit.

2. E-mail accounts will not automatically be continued for qualifying individuals. A request will need to be made in writing to the vice president for information technology.

3. In those cases where the existing mailbox name is well known to persons outside the college as a means to convey information to a college department, the college reserves the right to issue the employee a new mailbox address. Thirty days notice will be given to the employee in order that he or she may have sufficient time to notify others of the address change.

4. Employees leaving involuntarily are not eligible for this benefit.

5. The college reserves the right, upon thirty days notice, to discontinue providing an e-mail account under the provisions of this policy.

6. E-mail accounts for which a request to continue has not been received by August 1 of any year will be purged as of that date.

7. Decisions regarding eligibility for continuance of an e-mail account and the user name of the account (point 3 above) will be the responsibility of the vice president for information technology.