Copyright Infringement Policies and Sanctions

Any distribution of copyrighted material without proper licensing or permission from the owner/author/software manufacturer is prohibited by law. Any students accused of copyright violation or infringement will be required to resolve matters on their own without involvement from the institution.

Summary of Civil and Criminal Penalties for Violation of Federal Copyright Laws
Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

For more information, please visit the U.S. Copyright Office Web site at www.copyright.gov

Peer-to-peer (P2P) file-sharing allows users to share files online through an informal network of computers running the same software. File-sharing can give you access to a wealth of information, but it also has a number of risks. You could download copyright-protected material, pornography, or viruses without meaning to. Or you could mistakenly allow other people to copy files you don't mean to share. If you're considering P2P file-sharing, please review the following information:

- **Install file-sharing software carefully**,
  so that you know what's being shared. Changes you make to the default settings of the "save" or "shared" folder might cause you to share folders and subfolders you don't want to share. Check the proper settings so that other users of the file-sharing network won't have access to your private files, folders, or sub-folders.

- **Use a security program from a vendor you know and trust**;
  and keep that software and your operating system up-to-date. Some file-sharing software may install malware or adware, and some files may include unwanted content.

- **You may want to adjust the file-sharing program's controls**
  so that it is not connected to the P2P network all the time. Some file-sharing programs automatically open every time you turn on your computer and continue to operate even when you "close" them.

- **Consider setting up separate user accounts**,
  in addition to the administrator's account, if your computer has multiple users. Limiting rights on user accounts may help protect your computer from unwanted software and your data from unwelcome sharing.

- **Back up data**
  you don't want to lose in case of a computer crash, and use a password to protect any files that contain sensitive information.

P2P File-Sharing: Evaluate the Risks

Every day, millions of computer users share files online. Whether it is music, games, or software, file-sharing can give people access to a wealth of information. To share files through a P2P network, you download special software that connects your computer to other computers running the same software. Millions of users could be connected to each other through this software at one time. The software often is free. However, file-sharing can have a number of risks. For example, when you are connected to file-sharing programs, you may unknowingly allow others to copy private files — even giving access to entire folders and subfolders — you never intended to share. You may download material that is protected by copyright laws and find yourself mired in legal issues. You may download a virus or facilitate a security breach. Or you may unwittingly download pornography labeled as something else. To secure the personal information stored on your computer, industry professionals suggest that you:

Install file-sharing software carefully

When you load a file-sharing application onto your computer, any changes you make to the P2P software's default settings during installation could cause serious problems. For example, if you change the defaults when you set up the "shared" or "save" folder, you may let other P2P users into any of your folders — and all its subfolders. You could inadvertently share information on your hard drive — like your tax returns, email messages, medical records, photos, or other personal documents — along with the files you want to share. And almost all P2P file-sharing applications will, by default, share the downloads in your "save" or "download" folder — unless you set it not to.

Use security software and keep it and your operating system up-to-date.

Some file-sharing programs may install malware that monitors a user's computer use and then sends that data to third parties. Files you download may also hide malware, viruses, or other unwanted content. And when you install a P2P file-sharing application, you might be required to install "adware" that monitors your browsing

habits and serves you advertising.

Malware and adware can be difficult to detect and remove. Before you use any file-sharing program, get a security program that includes anti-virus and anti-spyware protection from a vendor you know and trust and make sure that your operating system is up to date. Set your security software and operating system to be updated regularly. Make sure your security software and firewall are running whenever your computer is connected to the Internet.

Delete any software the security program detects that you don't want on your computer. And before you open or play any downloaded files, scan them with your security software to detect malware or viruses.

Close your connection

In some instances, closing the file-sharing program window does not actually close your connection to the network. That allows file-sharing to continue and could increase your security risk. If you have a high-speed or "broadband" connection to the Internet, you stay connected to the Internet unless you turn off the computer or disconnect your Internet service. These "always on" connections may allow others to copy your shared files at any time. To be sure your file-sharing program is closed, take the time to "exit" the program, rather than just clicking "X" or "closing" it. What's more, some file-sharing programs automatically open every time you turn on your computer. As a preventive measure, you may want to adjust the file-sharing program's controls to prevent the file-sharing program from automatically opening.

Create separate user accounts

If more than one person uses your computer, consider setting up separate user accounts, in addition to the administrator's account, and give those user accounts only limited rights. Since only a user with administrator rights can install software, this can help protect against software you don't want on your computer. It also can keep users from accessing other users' folders and subfolders, since users with limited rights generally don't have access to each other's information. Also use a password to protect your firewall and security software so no one else can disable them or grant themselves rights that you don't want them to have on your machine.

Back up sensitive documents

Back up files that you'd want to keep if your computer crashes. Store them on CDs, DVDs, or detachable drives that you keep in a safe place.