Limit access to your computer by others
Consider using a screen-saver password to insure that your computer is not used by others. (Consult your computer's Help menu) Turn your computer off when not in use. Currently, student network accounts do not accommodate passwords.

Be sensitive to sharing bandwidth
If student computers on the network run peer-to-peer file-sharing software like Limewire to download large files, they may be consuming excessive network bandwidth. This may well affect the performance of students trying to complete class assignments or other academic endeavors.

Turn off or delete unneeded software features, such as file sharing
If your peer-to-peer file-sharing program is configured to share downloaded files, even greater amounts of bandwidth will be used, since the peer-to peer software will automatically offer that downloaded file to the world. When many others download the file from your computer, even greater amounts of bandwidth is used, slowing things down for all users. Not to mention your legal liability if you share *_copyrighted material_*. (see inside for details)

Download with care
Don't download anything from a website that you don't know or trust. Such files often include worms or viruses. If your computer is not secured as described above, these files can disrupt or even damage your computer. Your computer could then be used remotely to spread the infection to scores of other student computers. Your computer may become a busy file-swapping server or spam relay, sending out thousands of messages, and in the process using excessive network bandwidth. Or, perhaps, sending out copies of your personal Word documents or private email messages!

My computer is connected to the network... So, what are my responsibilities?
When you choose to connect your personal computer to Muhlenberg College's campus network, you accept responsibility for your computer as an integral part of this network. *_**The College's Electronic Communication**_* Policy states, in part, "users are prohibited from performing any action that directly or indirectly results in adverse effects upon the System or its Users." Thus, you are responsible for maintaining the security on your computer that protects your computer from others, and you are responsible for maintaining the security on your computer that protects others' computers from your computer. You are responsible for any viruses your computer contracts and spreads to other user's computers. You are responsible for excessive bandwidth used by your computer as a result of viruses or other computer maladies.

Further, you are responsible for any liability you may incur as a result of others illegally accessing *_**copyrighted material from your computer**_*. Negligence in these matters can have significant consequences, affecting you and other users.

Always log in (authenticate) with your college network account
Student computers must pass through the established process for networking and registration**, this is a one time process**. When problems are detected with computers on the residential network, this information allows OIT to quickly identify and notify students whose computers are involved. It also allows OIT to keep unauthorized users from disrupting this vital service.

Maintain your anti-virus software and keep it up-to-date
Computer viruses travel through the residence halls faster than colds! You are required to install anti-virus software on your PC and keep it updated. Freeware and Shareware may not be the best choice for this critical task. Configure this software to scan all executable files for viruses before running them. Installing more than one product may cause your pc to run slowly.

Keep your computer operating system up-to-date
Recent attacks upon computers took advantage of operating system exposures - even up-to-date anti-virus software was not sufficient to ward off these attacks.

As resource allows, we monitor the network for obvious problem-computers, and notify the student owners of the problem. (another reason to authenticate - so that we can identify and notify you if your PC is causing problems).
OIT views quality residential computing as a cooperative effort between IT staff and students - working together to insure its integrity and security for all.
*see inside for details

---

office of
INFORMATION TECHNOLOGY

Safe and Responsible Computing

A Student's Guide to Security and Liability on Muhlenberg's Network

Use great caution in opening e-mail attachments.

Your parents used to tell you "Don't talk to strangers!" That remains important advice. According to the CERT® Coordination Center at the Software Engineering Institute, operated by Carnegie Mellon University, you should only read a message that passes all of these tests:

The **Know** test: Is the email from someone that you know?
The **Received** test: Have you received email from this sender before?
The **Expect** test: Were you expecting email with an attachment from this sender?
The **Sense** test: Does email from the sender with the contents as described in the Subject line and the name of the attachment(s) make sense? For example, would you expect the sender - let's say your Mother - to send you an email message with the Subject line "Here you have, ;o)" that contains a message with attachment - let's say AnnaKournikova.jpg.vbs? A message like that probably doesn't make sense. In fact, it happens to be an instance of the Anna Kournikova worm, and reading it can damage your system.
The **Virus** test: Does this email contain a virus? To determine this, you need to install and use an anti-virus program.

* _You and Your Computer_ *

Campus System users are responsible for any content placed by them in an area of public access on the campus network, or published to a public area of the campus website. If this content is material protected by copyright, **YOU** are committing copyright infringement by illegal distribution!

If **YOU** have any of these peer-to-peer programs installed on **YOUR** computer, **YOU** may be **violating copyright law**.

Notification of Infringement

The College does not employ tools to detect copyright violations. However, agents and representatives of copyright holders (such as the Recording Industry Association of America) routinely monitor file-sharing activities to detect infringement involving copyrights held by those they represent.
Once detected, infringing activity can be reported by agents of copyright holders to the Service Provider of the infringing user. In the case of YOU being detected as having infringed upon a copyright, the notice is served upon the College.

The College's procedure upon receipt of a valid notice of infringement (first offense), is to:

1) Use the (internal IP) information contained in the infringement notice to identify the involved campus user.

2) Draft a Letter of Notice to the user – student is notified to report to the Dean of Students Office to pick up their Letter of Notice- including a copy of the infringement notice specifying the copyrighted material infringed.

3) Require, as stated in the Letter of Notice, that the user remove access to the infringing material, and any other copyrighted material for which they do not have rights of distribution, within 48 hours of receipt of the Letter of Notice.

4) Require written confirmation to the Chief Business Officer of the College within 48 hours of receipt of the Letter of Notice confirming that access to such material has been removed.

5) After 48 hours, if the user has not complied with the Letter of Notice, the user's network access will be revoked until compliance is effected and reported per the Letter of Notice.

The College's procedure upon receipt of repeat infringement notices for a user (second offense):

1) Use the (internal IP) information contained in the infringement notice to identify the involved campus user.

2) Draft a Letter of Notice – Second Offense to the user – student is notified to report to the Dean of Students Office to pick up their Letter of Notice**- including a Notice of Fine [$50]** and a copy of the infringement notice specifying the copyrighted material infringed.

3) Suspend user's network access for a period of one week, commencing upon the date of the Letter of Notice.

4) Require, as stated in the Letter of Notice, that the user remove access to the infringing material, and any other copyrighted material for which they do not have rights of distribution, within 48 hours of receipt of the Letter of Notice.

5) Require written confirmation to the Chief Business Officer of the College within 48 hours of receipt of the Letter of Notice confirming that access to such material has been removed.

6) After one week, if the user has complied with the Letter of Notice and paid the fine, the user's network access will be restored; if all conditions have not been met, network access remains suspended until compliance is effected.

The College's procedure upon receipt of repeat infringement notices for a user (third or greater offense):

1) Use the (internal IP) information contained in the infringement notice to identify the involved campus user.

2) Draft a Letter of Notice – Third Offense to the user – student is notified to report to the Dean of Students Office to pick up their Letter of Notice- including a copy of the infringement notice specifying the copyrighted material infringed.

3) Suspend user's network access pending judicial review, commencing upon the date of the Letter of Notice.

4) Require, as stated in the Letter of Notice, that the user remove access to the infringing material, and any other copyrighted material for which they do not have rights of distribution, within 48 hours of receipt of the Letter of Notice.

5) Require written confirmation to the Chief Business Officer of the College within 48 hours of receipt of the Letter of Notice confirming that access to such material has been removed.

6) Refer all material for Judicial Review.

7) Network access remains suspended pending recommendations from Judicial Review.