

eSupport immediate help online: <http://support.cumc.columbia.edu>
5-Help (212-305-4357) 5help@columbia.edu <http://www.cumc.columbia.edu/it>

SMDEP students have access to a variety of technical resources at CUMC during the course of the program. They are provided for academic purposes, and students must comply with CUMC computer and network use policies while using these resources.

- **Columbia University Network ID or UNI** - your UNI grants you access to all of the technical resources including the campus network. Please activate your UNI at <http://uni.columbia.edu> as soon as possible.
- **Wired network** - after activating your UNI, please register for wired via the "Bradford" form using the computer that you will be bringing to campus: <http://www.cumc.columbia.edu/it/bradford>. Registering for wired involves downloading a small, non-permanent program to scan your computer and verify that it meets basic security policies, see the links at the bottom of the Bradford form for full details. If you don't register before arriving, your computer's browser will be directed to the form when you first plug in to wired.
- **Wireless network** - Bard Hall, the CUMC IT Service Desk and the Library have wireless access available. Please visit <http://www.cumc.columbia.edu/it/wireless> for full instructions on configuring your computer.
- **Technical Support** - SMDEP students receive free technical support for the duration of the program. To reach us, you can contact the CUMC IT Service Desk at extension 5-Help (212-305-4357), visit <http://support.cumc.columbia.edu> to instantly connect to a technician online, email 5help@columbia.edu, or come by the service desk on the 2nd floor of the Hammer Building (right above the Library).
- **Printing** - the NINJa printing system at the Service Desk, Library and Bard Hall requires a printing quota and UNI login. SMDEP students receive a 700 printer page quota and can purchase more pages if needed. Please see <http://www.cumc.columbia.edu/it/printing> for complete information.

Computer and Network Use Policies

This document contains important information to help you keep your computer and data safe both on and offline. When you activate your UNI and connect a computer to the CUMC network, you gain many privileges - which come with considerable responsibility. Being informed and responsible when using the network prevents your computer from falling prey to malicious behavior. In addition, you must be aware of certain legal issues related to network activity, or you risk losing network connectivity and running into legal as well as academic trouble.

- **Computer Security is Your Responsibility** – The security of the Columbia network depends on the security of each computer connected to it. You are ultimately responsible for all of the network traffic that passes through your system and must maintain the security of any computer you connect to the campus network. If you fail to do this, your system could become infected with a malicious program that might destroy data or steal financial and other personal information.
- **The Columbia University Computer and Network Use Policy**, which governs all online activities at Columbia University, can be found at <http://www.columbia.edu/cu/policy>. In addition, because the CUMC campus shares its network with New York Presbyterian Hospital and must comply with Health Insurance Portability and Accountability Act (HIPAA) regulations, there are further security procedures that must be followed:
 - **No gaming or networking devices (routers, wireless access points, etc.)** can be set up on the CUMC network.
 - All systems must run current antivirus and antispyware programs.
 - All systems must run operating system updates to ensure that any critical flaws are patched.

For more information regarding network access please contact the CUMC IT Service Desk directly.

- **Be aware of copyright and intellectual property laws.** If you purchased an item, such as a pre-recorded CD or DVD, you may keep an electronic copy on your computer. If you do not have a purchased copy, you may not have a copy on your computer – that is copyright infringement, a federal crime. Even if you own a copy of an item, it is illegal to download or share it.

SMDEP and Computing at CUMC

- **Do not enable file sharing on your computer if it allows access to others' copyrighted works.** In the past few years, Columbia University has received hundreds of complaints of copyright infringement from the music, software and motion picture publishing associations as a result of people sharing or possessing copyrighted material on their computers. You can immediately lose access to the Columbia University network if you violate copyright laws. In addition, you can be sued by the copyright holder for damages if you are found possessing and/or sharing copyrighted material that is not legally yours. Please see <http://www.columbia.edu/cu/policy/copyright-info.html> for more information.
- **Unacceptable behavior in a non-cyber setting is also unacceptable in a cyber setting.** The consequences of harassing, stalking, or threatening someone online result in the same legal consequences as they do offline. Attempts to compromise systems and networks are also considered serious offenses, and can result in suspension from the University and even criminal prosecution.

System Security

Here are some important steps you can take when using your computer to protect the system itself, your data, and your personal information:

- **Avoid opening web site links from an email or instant message.** Be wary of email and IM messages containing URLs that you weren't expecting. Opening a web page from an email message can be just as dangerous as opening an attachment. The past years have seen a significant rise in "Phishing", where a web site or email seems authentic but is really an attempt to steal personal identity information.
- **Use an antivirus program.** Software such as Symantec or the free AVG antivirus (<http://free.grisoft.com/>) will go a long way in protecting your computer. You must also be sure that your antivirus program you use is regularly scanning your computer for viruses and receiving new, updated information about recent viruses.
- **Use an antispyware program.** Microsoft's Windows Defender anti-spyware program has received great reviews and is available for free at: <http://www.microsoft.com/defender>. This application protects your computer from spyware, trojans, keystroke loggers and other malicious programs, as well as unwanted cookies.
- **Keep your operating system patched and up to date.** New vulnerabilities in operating systems are regularly discovered and exploited. To prevent virus infection or worse due to this, use a built-in update program and set it to update automatically: Windows Update for Windows and Software Update for Mac OS X are two examples. You can learn how to use these programs at <http://security.columbia.edu>.
- **Protect your laptop.** Never leave your laptop unattended. They are easily stolen, even when locked - cable locks can be cut off and easily removed.

Account Security

Any logon ID and password you use are potential keys to a great amount of personal information about you, such as your grades, financial information, home address and Social Security Number. Here are some important yet simple ways to protect yourself and your account information:

- **Keep your password secret.** Never give this password to anyone, not even a spouse or best friend. Be sure to use strong passwords that are at least 6 characters long and contain both letters and numbers – and use different passwords to access different accounts or systems.
- **Do not save your email password on your computer.** Enter it every time you open your email program, even if you think no one else has access to your computer.
- **Log out of public terminals completely!** Otherwise, you may have just given the next person unlimited access to your accounts.
- **Never send confidential information via email even when the messages are encrypted.** There's no telling what a recipient will do with that information, whether by accident or with malicious intent.
- **Use a screensaver password.** This is strongly recommended. Do not use your email password for your screensaver! In Vista, right click your desktop and click Personalize - Screensaver, then On resume password protect option. In Windows XP, select the "Password Protected" option under the Screen Saver tab in Display Control Panel to enable this feature. For Macs, go to System Preferences - Security - Require password to wake this computer from sleep or screensaver.