



Working with Confidential Information for Employees, including Student Employees

The “Policy on Responsible Use of Computing Resources at Mount Holyoke College” generally defines appropriate computer use practices. However, when working with personal or confidential information, a higher standard of practice is required to insure compliance with federal and state privacy and security regulations.

In order to insure that confidential and personal information is properly safeguarded, it is important to comply with the following guidelines, both at work and at home. It is particularly important to be vigilant when working at home with confidential information, since the system protections available at the College are typically not present.

Computers must be regularly updated with the most current version of anti-virus and anti-spyware software, all announced patches and bug fixes installed promptly and anti-spyware software run regularly to detect and remove spyware. For College machines, LITS is implementing technology that will provide automatic updates for these applications. For personal machines, it is your responsibility to insure that the applications are current and are run regularly. Complying with these practices will insure that the College’s data are secure and minimize the risk of corruption of your computer.

The College uses McAfee’s VirusScan anti-virus software, which should be run at least weekly. Employees may install this on home computers at no cost.

Keep current with all critical security patches (e.g., Windows and MacIntosh updates), which are announced periodically by the vendor. Never install patches sent by email; these are viruses.

Run anti-spyware programs semi-monthly (e.g., Spybot).

Computers must be password protected, with a password that is unguessable and changed regularly. Passwords for accessing College information should not be used for other purposes. (For example, your campus email password should not be the same as the one you use for access to your AOL account, your Blackberry or Amazon.com). Do not keep passwords in places where others can find them.

Computers should be turned off when not used for any extensive period of time and secured from unauthorized access when the employee is away from his/her office or home workspace. Security measures include securing the space (e.g., locking the office or room door) and/or securing the information on the machine (e.g., by closing the application or locking the computer) so that others can't access the information. Computers and printers should be turned off at the end of the work day unless overnight reports are being run.

Staff who plan to work at home with files that contain personally identifiable information for employees, students, or alumnae (examples: name, address, telephone number, account number, social security number, etc.) should discuss this with the department manager and receive his/her approval to do so.

All files containing personal or confidential information need to be used, stored and disposed of properly.

Paper files taken home must be stored in a secure place (e.g., a locked file cabinet) when not in use. The files must be returned to the office in an appropriate time frame, with no copies retained at home. Discarded paper files should be returned to the office for disposal through appropriate office channels, unless they are shredded at home. Do not throw in home garbage or home recycling.

When working with electronic files on shared home computers, a firewall (either software, hardware or both) must be installed and enabled and the files must be password protected. In addition, when naming files, remember that file names are inherently insecure and should never contain confidential or sensitive information.

When the work is completed (using a home machine), all work-related files must be removed from all media used (hard drive, floppy disks, etc.). While putting the files in the computer trash bin and then emptying the trash removes the data from the visible files, remember that specialized software may still be able to retrieve the files. When removing data that, if recovered, could result in identity theft, utility software (e.g., Norton Utilities) should be used to remove the files completely.

Prior to being replaced, an office machine containing confidential information should have that information removed using software like the Spybot shredder capability. This provides added assurance that confidential data cannot be accessed between the time the machine is removed from the individual's office and when LITS completely erases its hard drive before disposal. Working with confidential information on the ambr server rather than the desktop will prevent this problem (unless the work is then backed up to the desktop).

Any file containing confidential information on a removable medium (floppy disk, CD, memory stick, etc.) must be stored in secure place (e.g., locked drawer or cabinet).

Files must be transmitted by secure method (use teraterm with SSH, SFTP or other SSL technology). Do not use telnet, FTP or instant messaging (IM), which are not encrypted.

Files should not be opened or saved on computers running peer-to-peer file sharing programs (e.g., KaZaA), because of the inherent risk of such software. See “Employee Use of Peer-to-Peer File Sharing Software” for more information.

Browsers should not be set to remember passwords or data in forms.

If you suspect that your computer has been compromised by a worm, virus or other invasive software, report the problem immediately to LITS. By law, the College has reporting and other responsibilities if personal or confidential data are accessed by unauthorized users.

Resources:

More information about the various topics mentioned above is available at www.mtholyoke.edu/lits/tsr/pdfs/SecureSystem.pdf.

For more information about secure server technology, see www.mtholyoke.edu/lits/network/doc/access.txt.

**THE Campus Privacy
and Security Committee
Revised 1/8/08**