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. The strictest standards apply to personally identifiable information, which is specifically regulated by both Federal and state law. Personally identifiable information includes first and last name (or first initial and last name) plus any of the following: Social Security number; driver's license or state identification card number; or a financial account, credit or debit card number ,with or without any required security code, password or PIN number that would permit account access.

In order to insure that confidential and personally identifiable 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. Do not work on home computers with personally identifiable information.

Computers must be regularly updated with the most current version of anti-virus and anti-malware software, all announced patches and bug fixes installed promptly and anti-virus and anti-malware software run regularly to detect and remove invasive software.

- For College machines, LITS provides automatic updates for anti-virus software. The College uses McAfee's VirusScan anti-virus software, which employees may install on their home computers at no cost and will run automatically. Otherwise, anti-virus software should be run at least weekly.

- 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-malware programs (the College uses Malwarebytes, Anti-malware software) weekly.

- If a College-owned machine show signs of compromise (unexpected pop-up windows, suddenly sluggish response, or other anomalous behavior), run the anti-malware program and notify LITS. If your computer has access to personally identifiable information, unplug the machine from the network, don't touch the machine further and notify LITS immediately.

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 PDA or non-Mount Holyoke email account.). 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 confidential information for employees, students, or alumnae should discuss this with the department manager and receive his/her approval to do so. Personally identifiable information should not be accessed or worked with on a home computer. If you need to work from home using personally identifiable information, there are options, including Remote Admin and Microsoft Remote Desktop, that will allow you to access your office computer remotely. Contact your supervisor or LITS for details.

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 personally identifiable, confidential or otherwise sensitive information.

When the work is completed (using a home machine), all work-related files must be removed from the local hard drive. 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 files containing confidential data, utility software (e.g., Norton Utilities) should be used to remove the files completely.

Prior to being replaced, an office machine containing confidential or personally identifiable information should have that information removed using software like the Spybot shredder capability. This provides added assurance that the 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 or personally identifiable information on the ambr server rather than the desktop will prevent this problem (unless the work is then backed up to the desktop).

If at all possible, avoid storing personally identifiable information on laptops, PDA's, flash drives or any other portable device. If it is unavoidable, the storage area on the device must be encrypted. Any portable device on which confidential or personal information resides must also be physically stored in secure place (e.g., locked drawer or cabinet).

The College does not provide technical support for encrypting email. Files containing personally identifiable information should not be sent as email attachments.

Files should not be opened or saved on computers running peer-to-peer file sharing programs, 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 personally identifiable or confidential data are accessed by unauthorized users.

MHC Privacy/Security Committee
Revised 1/11/11