



Complying with Privacy and Security Regulations Frequently Asked Questions

Q: I know I need to protect confidential information, but isn't it okay to share it with my co-workers at Mount Holyoke?

A: Maybe. Confidential information should only be shared when there is a legitimate business purpose—that is, when your colleague needs to know the information. Otherwise, it should not be shared.

Q: What about Five Colleges staff?

A: While Mount Holyoke is part of the Five Colleges consortium, sharing with your colleagues at the other colleges is not the same as sharing within Mount Holyoke. Information should not be shared unless there is a specific consortial purpose served by sharing. Convenience alone is not a specific consortial purpose.

Q: What should I do if someone identifies him/herself as a law enforcement officer and requests confidential information?

A: If you are not a department or division manager, refer the person to your manager. If you are the manager:

- Ask for credentials—is the person who they say they are?
- Do they have a subpoena or other document supporting the request?
- Tell them that you will consult with the College's attorney and get back to them.
- Discuss the request and the authority for the request with College counsel before responding.
- If you have questions, contact Mary Jo Maydew, Vice President for Finance and Administration, or Paul Ominsky, Director of Public Safety.

Note: Some offices receive routine requests for confidential information (e.g., subpoenas for student financial information in connection with a legal proceeding; requests for verification of transcripts/graduation). Each office should have a procedure in place to handle such requests.

Q: I occasionally get calls checking references on current or former employees, including student employees. How do I respond?

A: Verify that the individual has given permission for you to provide a reference, if you haven't already discussed it with him or her. Verification of dates of employment is permissible without the permission of the individual. If you wish to verify that the caller is legitimate, ask for a telephone number and return the call.

Q: How do I respond to a telephone request to discuss confidential information about a member of the College community?

A: Begin by asking questions that will help you verify the identity of the person you are talking to—e.g., the last four digits of the person's Social Security number or their mother's maiden name for access to financial information. Once you can confirm the person's identity, you can then determine whether you are free to share confidential information with them—discussing a dependent student's financial aid award with a parent, for example. Resist the impulse to be helpful and volunteer information outside your department; instead refer the caller to the appropriate office.

Q: Where should I refer people who are asking for confidential information?

A: Here is a partial list of the offices with specific responsibilities for confidential information:

- Registrar's Office—student grade/transcript information, verification of enrollment
- Dean of Students Office—student's presence on campus
- Dean of the College—other student information
- Health Center/Counseling Center—student health information
- Dean of Faculty—faculty information
- Student Financial Services—student financial information
- Human Resources—employment information
- Financial Services—employee financial information

Q: If I have a question about whether to release confidential information, whom should I ask?

A: Start with your supervisor. If he or she is unsure, there are several people on campus who can assist, including the Registrar, the Comptroller, the Director of Risk Management, the Director of Human Resources, the Dean of the College, the Dean of Faculty and the Vice President for Finance and Administration.

Q: What happens if I violate one of these regulations?

A: Several consequences are possible, depending on the particular violation. If confidential information is disclosed, lost or stolen, the College must promptly notify all individuals who might be affected. The College may face litigation and if found liable may have to pay damages, fines, penalties, etc. both to the individual whose privacy has been compromised and to the federal or state government. There may also be consequences for you as an individual employee, both at the College and legally.

Q: I know I should safeguard confidential information, but isn't it okay to send email to other people on campus who need the information?

A: Email is not a secure means of sharing confidential information (whether in the body of the message or as an attachment) unless it is sent using a secure method. Use SSH, SFTP or other SSL technology (putty or teraterm with SSH, secure IMAP on desktop email client or College web mail). Do not use telnet or FTP, which are not encrypted. Emailing within the campus does not automatically make the transmission secure. In addition, both ends of the transmission (yours as the sender and whoever is receiving the message) must be secure to assure protection. Once the message is received, it needs to be treated as confidential in the same ways that a hard copy of the same information would be handled.

Q: Is it okay to send confidential information via instant messaging (IM)?

A: No, IM transmissions are not encrypted, so it is not a secure method of sending information. In addition, IM messages are copied onto the hard drive of the receiver and may not be overwritten for some time, if at all, presenting a second security risk.

Q: Since it's difficult to remember multiple passwords, shouldn't I use the same password for everything?

A: No. Do not use the same password(s) you use at work on your home computers or on the Internet. You should develop a structure for password use that results in a manageable number of unguessable passwords that are changed when appropriate.

Q: How do I create unguessable passwords that I can remember?

A: One way to create memorable but unguessable passwords is to use a combination of letters (capital and lower case) and numbers that have meaning for you (which makes them easy to remember) but not to others (which makes them unguessable). Examples are the first one or two letters from a series of related things—your pets' names, the months of your children's birthdays, etc. An approach to avoid is to substitute numbers for letters, i.e., zero for the letter "o" or 1 for the letter "I", since password-cracking programs use these rules. You can then develop additional passwords or make periodic changes to your passwords by varying the order and the case or by adding a number into the sequence. Don't leave written passwords near your computer. If you must write them down, keep them in a protected location. If you need help in remembering infrequently used passwords, write down a hint for yourself.

Q: How can I be sure that I'm sending confidential information safely?

A: First, take steps to insure that your computer is not compromised by making sure that Windows updates are current; that anti-virus and anti-spyware software is current and is run frequently; and that peer-to-peer file sharing software is not present. Use the auto update feature of your computer to download Windows updates automatically. If your office computer does not already use Track-It! for automatic updates of anti-spyware software, contact LITS for assistance in adding Track-It! to your machine. Be cautious about downloading software you're unfamiliar with, including tool bars, screen savers and recreational software. Don't let students or any unauthorized person add software to your computer.

Second, be sure that the information you're working with is not shared with anyone without a legitimate business purpose.

Third, use a secure method of transmission—putty or teraterm with SSH or SFTP, or secure IMAP that can be set on modern email clients like Mozilla Thunderbird.

Fourth, pay careful attention to email addresses to insure that you don't inadvertently send information to the wrong people. Use tools like auto completion and forwarding to a group with caution. Review the addresses in your message before sending.

Fifth, be careful of embedded messages and what they may contain when forwarding messages to others. A message with other messages embedded may contain confidential information that you forgot was included.

Q: What steps should I take to be sure I share confidential information appropriately?

A: First, don't talk to anyone about the information unless there is a legitimate business purpose—not your co-workers, not your friends, not your family. Second, insure that your computer can't become the source. Follow the steps listed above to assure you safely transmit confidential material. In addition, don't leave confidential information visible on your computer screen when others can view it. Don't use "Confidential" in the subject line of an email message. When you're away from your computer, close the application you're working with or lock your computer. Keep paper records and remote storage devices (disks, CD's, etc.) in locked file cabinets or otherwise secured. When disposing of paper records, keep material to be shredded separate from other trash or recyclables and either shred or put into "to be shredded" containers frequently. And remember that an easy way to gain access to confidential information is to steal the computer it resides on. Don't put confidential information in the name of any file or document.

Q: How can I tell when an email message or an attachment is likely to be dangerous?

A: The College's system identifies many but not all attachments with high risk characteristics and flags the message as potentially containing a virus. Delete those messages without opening the attachments. Do not set your browser to open attachments automatically. Do not open attachments ending in .exe, which are executable files. Do not open attachments from sources you don't recognize. Do not open unexpected attachments from sources you recognize without checking with the sender. Many viruses have forged headers that look legitimate. If you're unsure about the legitimacy of any attachment, check with the sender.

Q: How do I know if my computer is corrupted? How do I get it fixed?

A: If your computer does not function properly or becomes very slow in responding, you should suspect that it might be corrupted and contact the Help Desk in LITS for assistance.

Q: How can I protect myself against identity theft?

A: Protect your own confidential information in the same way you would that of others. Don't share it unless the other person has a legitimate need to have the information. Never give out personal information in response to an email message or to a website reached from a link within an email message. Instead connect to the website directly.

Q: If I have a firewall, does that mean my files are safe?

A: Not necessarily. A firewall provides one layer of protection, by making your computer invisible to other computers. However, if you engage in risky behavior—like using peer-to-peer file sharing software, your computer is still at risk of corruption and your files remain vulnerable.

Q: What should I do if I believe that confidential information might have been compromised or that a violation of regulation may have occurred?

A: Talk with your supervisor. If for any reason, you are uncomfortable doing this, talk with the Director of Human Resources, the Comptroller or the Vice President for Finance and Administration.

Q: How can I minimize the amount of spam I receive?

A: The College filters known spam sites. In addition, use the spam filters available with your email client or browser and take advantage of filtering based on the spam scores the College assigns to messages. (Remember to check the filtered messages regularly, so you can respond to any legitimate messages that were screened out of your inbox). Avoid signing up for commercial mailing lists.

Q: How can I become more educated about computer security issues?

A: Be attentive to newspaper, magazine and television reports involving these issues. In addition, you can review the following web sites:

<http://isc.sans.org>

<http://www.cert.org>

Q: I believe I may become involved in a legal matter related to my work for the College. What should I do about any relevant electronic information?

A: As part of your regular work routine, you should practice good computing habits: saving useful information; removing unneeded information; filing saved materials for ready access; and backing up files appropriately. However, once you become aware that there may be a legal issue, everything must be retained. Do not delete any relevant electronic files or dispose of any paper files until the matter is resolved.

Q: I have personal files on my computer and possibly the College server that may be related to a legal action. Does the College have any right to access them?

A: Yes. Refer to the Policy on the Responsible Use of Computing Resources at Mount Holyoke College (www.mtholyoke.edu/lits/network/doc/policies/) for more details.

**THE Campus Privacy
and Security Committee
Revised 6/25/07**