



COMPLYING WITH PRIVACY AND SECURITY REGULATIONS

Overview
(Revised 4/4/06)

MOUNT HOLYOKE[™]



What Regulations?

- FERPA-protects privacy of student records
- Gramm/Leach/Bliley-protects security and confidentiality of customer financial records
- FACTA-defines appropriate methods of disposing of information from credit reporting agencies



Question

You find a folder in the trash that contains information about a faculty member's former advisees, including name, address, Social Security number, date of birth, grades, etc.

How do you respond?



What is Confidential Information?

- Information that identifies or describes the individual, including:
 - Home address and telephone number (when linked with other confidential information)
 - Birth date
 - Social Security number
 - Income tax information
 - Salary information
 - Student academic information



What is Directory Information?

- FERPA permits disclosure of directory information for current students without consent, including:
 - Name
 - Class year and major
 - Home address and telephone number
 - Campus address and telephone number
 - Dates of attendance at Mount Holyoke
 - Previous educational institution most recently attended
 - Honors, awards and participation in sports and activities
 - Heights for athletes



Principles for Working with Confidential Information

- Use confidential information appropriately
- Safeguard the information, in both paper and electronic form, from inappropriate uses by practicing safe computing habits



Appropriate Use of Confidential Information

- Access, use and disclose confidential information only as a legitimate part of your job
- Do not share confidential information with anyone who does not have a legitimate need to have the information
- Dispose of confidential information properly

Safeguarding Confidential Information

(at work and at home)

- Keep current on security software—anti-virus, anti-spyware, bug fixes, patches
- Passwords—unguessable and changed as appropriate
- Control access—turn off machine, lock screen, locked file cabinets, secure space, firewall on shared computers

Safeguarding Confidential Information (continued)

- Transmit, store and dispose of files properly
- Do not open or save files on computers running peer-to-peer software
- Do not set browsers to remember passwords or data in forms
- Do not transmit confidential material via instant messaging—it's not secure
- If you have a problem, report it immediately



Question

The College's student health insurance provider asks you to email them a list of participating students, including name, birth date and social security number.

How do you respond?



Question

An FBI agent comes to your office and begins to question you about an international student.

How do you respond?



When Can Confidential Information Be Shared?

- When there is a legitimate business purpose
- When you receive a duly executed subpoena from an authorized government agent
- When you believe that there is imminent danger of death or serious physical injury to someone

What's Peer-to-Peer File Sharing?



- Allows users to find and access each other's hard drives and to share information directly without a central server
- P2P software includes KaZaA, Limewire, Gnutella, Windows file sharing



Why is P2P File Sharing a Problem?

- Violation of copyright laws
- Slowing or disruption of network
- Risk of contamination
- Support costs of restoring contaminated computers



College's P2P Policy

- Use of P2P software by employees on any machine connected to College network is prohibited unless academic or job-related
- Job-related uses for staff should be cleared with Senior Staff member



Some Do's

- Do use unguessable passwords and change them as appropriate
- Do shred confidential documents when disposing of them
- Do use confidential material at home only when absolutely necessary
- Do be vigilant about protecting computer security



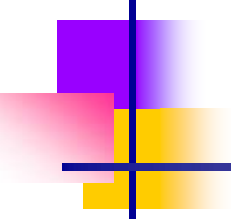
Some Don'ts

- Don't give anyone else your password or write it down where others can find it
- Don't share confidential information (with co-workers, with spouses, with friends)
- Don't work with confidential information on a computer running P2P file sharing software
- Don't set browsers to remember passwords or data on forms



Responsible Computer Use Policy

- Comply with laws, regulations and policies
- Use only authorized resources in an authorized manner
- Respect privacy of other users
- Respect the finite capacity of resources



Responsible Computer Use Policy (continued)

- Do not use resources for personal commercial purposes
- Do not speak on behalf of the College or use College trademarks/logos unless authorized to do so
- Be alert to indications that your computer is compromised



Written Policy Statements

- Employee Confidentiality Statement
- Working with Confidential Information
- Employee Use of Peer-to-Peer File Sharing Software
- Policy on Responsible Use of Computing Resources at Mount Holyoke College
- All are available on-line at www.mtholyoke.edu/go/ps



Question

A journalist whose work you admire calls. She is researching a famous alumna and has learned that she was a student intern in your office. The journalist begins asking you questions about your experience with the alumna.

How do you respond?



Question

You receive the Following email message:

Date: October 20, 2005
From: Network Administrator
To: Mary Jo Maydew
Subject: Virus Alert

Your machine has been detected on our network with a virus.
Please run the following attachment to remove the virus or we will
remove your machine from the network.

An attachment is included.

How do you respond?



Questions/Discussion
