

# MOUNT HOLYOKE<sup>SM</sup>

## Complying with Privacy and Security Regulations Glossary of Terms

### **Anti-spyware Software**

Software identifies and removes most spyware from computers. Examples include Spybot and Ad-Aware. Anti-spyware software should be run at least weekly to protect your computer from contamination.

### **Anti-virus Software**

Software identifies and in most cases removes computer viruses. The College uses McAfee's VirusScan software. On campus computers owned by the College are set to provide automatic daily updates. Off-campus and personally owned computers should also be set to provide automatic daily updates to provide maximum protection against contamination. At a minimum, anti-virus software should be run weekly.

### **Confidential Information**

Information identifies or describes an individual. Examples of confidential information include birth date, Social Security number, income tax information, salary information and home address and telephone number when linked with any of the other information.

### **Directory Information**

FERPA permits disclosure of directory information without the consent of the student. Directory information (which is defined in the Bulletin and Course Catalogue) includes: name; class year; home address and telephone number; campus address and telephone number; major; dates of attendance at Mount Holyoke; degrees, honors and awards received; participation in officially recognized sports and activities; and previous educational institution most recently attended. In addition, student heights are considered directory information when used in connection with athletic teams. Student identification numbers, while not directory information, may be used (for identification purposes only) internally and externally on a business need basis.

### **FACTA**

The Fair and Accurate Credit Transfer Act of 2005. FACTA defines appropriate methods of disposing of information obtained from consumer reporting agencies for business purposes. Such information must be burned, pulverized or shredded. Information obtained by College employees in the course of their jobs and through their own investigations is not subject to FACTA.

### **FERPA**

The Family Educational Rights and Privacy Act of 1974. FERPA protects the privacy of student educational records, including student employment records. FERPA does not cover criminal or medical records.

## **Firewall**

A firewall is a tool (usually a combination of hardware and software) that secures access to a local network or computer. A firewall guards the local network by analyzing the data leaving and entering, allowing authorized traffic through while keeping unauthorized traffic out.

## **Gramm-Leach-Bliley (GLB)**

The Financial Services Modernization Act of 1999. GLB requires financial institutions to ensure the security and confidentiality of customer records and information. GLB has both privacy and security requirements.

**Peer-to-Peer File Sharing Software (P2P)** Software enables users to find and access each other's hard drives and to share information directly without a central server. Examples are KaZaA, Limewire, Gnutella, and Windows file sharing. While there are legitimate P2P uses, much P2P activity involves music and movie sharing in violation of copyright law. In addition, use of such P2P file sharing leaves computers extremely vulnerable to contamination from worms and viruses.

## **Privacy**

Individual's expectation that certain information about them is protected from public disclosure without their consent. Both the FERPA and GLB regulations require that academic, financial and other information about individuals be treated as confidential.

## **SSL Technology**

Secure Sockets Layer (SSL) is a [protocol](#) for transmitting private documents via the [Internet](#) using a [cryptographic](#) system. All information is encrypted. Both [Netscape Navigator](#) and [Internet Explorer support SSL](#), and many [Web sites](#) use the protocol to obtain confidential user information, such as credit card numbers. By convention, [URLs](#) that require an [SSL connection](#) start with *https:* instead of *http:* Desktop email clients, especially those used from off-campus, must be set to use secure IMAP (port 993).

## **Track-It! Deploy**

Software provides delivery of updates of various applications, including anti-spyware software and other office applications. Track-It! Deploy provides an efficient mechanism for assuring that updates are done regularly and that the College is in compliance with its software licenses.

## **USA PATRIOT Act**

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. The USA PATRIOT Act increases the power of law enforcement agencies to perform surveillance, computer-related searches and seizures, electronic evidence gathering and voluntary disclosure of information by institutions that would previously have been considered confidential.