MOUNT HOLYOKE

EMPLOYEE CONFIDENTIALITY STATEMENT

Employees of Mount Holyoke College may in the course of their jobs have access to confidential or personally identifiable information about students, parents, staff, faculty, alumnae, donors, volunteers and customers. This information is protected by College policy and by law, including, but not limited to:

- the Family Educational Rights and Privacy Act (FERPA) of 1974, as amended
- the Gramm-Leach-Bliley (GLB) Act,
- the Fair and Accurate Credit Transactions Act of 2003 (FACTA)
- the Massachusetts Security Breach Law of 2007 and the regulations contained in the "Standards for the Protection of Personal Information of Residents of the Commonwealth (MA201)
- the "Identity Theft Red Flag Rules" of the Federal Trade Commission

Confidential information includes any information that identifies or describes the individual (other than "directory information" for current students who have not limited the release of such information). Personally identifiable information is defined as first and last name (or first initial and last name) in combination with any one 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.

Accessing, using and/or disclosing such information for any reason other than the legitimate pursuit of the individual's employment duties or in ways that jeopardize the security of such information constitutes misuse.

The College expects that all employees will comply with the safe computing practices identified in the document entitled "Working with Confidential Information".

All employees are expected to safeguard and refrain from disclosing passwords and other codes that allow access into College computer systems. Any access to electronic systems containing College data and made using an employee's login and password is that employee's responsibility. If there is a possibility that someone other than the employee has used his or her login information, the employee is responsible for immediately reporting the circumstances to the Networking and Systems Department in Library, Information, and Technology Services and requesting a new password.

An employee's access to confidential or personally identifiable information of the College is conditioned upon the employee's acceptance of the obligations described in this Confidentiality Statement. Obligations to protect confidential information continue after termination of an individual's employment. Any misuse or unauthorized release of such information, either during or subsequent to the conclusion of employment at Mount Holyoke College, may be grounds for legal and/or disciplinary action up to and including discharge from employment with the College and civil or criminal liability.

MHC Privacy/Security Committee
Revised 1/10/11