MOUNT VERNON
NAZARENE UNIVERSITY

Privacy of Constituent Information Policy

It is the policy of Mount Vernon Nazarene University to hold in sacred trust that information it possesses on its constituents (e.g., alumni, donors, employees, current and prospective students, etc.) by:

- Complying with applicable governmental regulations.
- Exercising reasonable safeguards for the protection of individual information in all forms of media.
- Promoting privacy awareness throughout the University.
- Disclosing to the public the University's Privacy of Constituent Information Policy.

The Privacy of Constituent Information Policy is to be implemented in close harmony with the Policies on Technology Infrastructure, and Records Retention.

The following outlines the roles and University position assigned to the role.

Role	University Position
Executive sponsor	Vice President for Enrollment Management
Secondary sponsor	Vice President for Finance and Chief Financial Officer

The Privacy of Constituent Information Policy applies to the following functional areas or positions.

Functional Areas or Positions	Specific Policy Application
Vice President for Enrollment Management	To execute the Privacy of Constituent Information Policy.
Senior Leadership Team	To define and implement the Privacy of Constituent Information Policy in divisional responsibilities.
All University employees	To adhere to the Privacy of Constituent Information Policy and its supporting procedures.

Compliance with the Privacy of Constituent Information Policy is critical and includes the following.

Action	Guideline
Defining employee responsibilities	Each employee who has access to constituent information through the University's databases and technology infrastructure will guard that information, sharing the information only with individuals with a documented need to know.
Disclosing the Privacy of Constituent Information to the public	Include the policy on the website, *Catalog*, and other key public documents (e.g., applications for admission, applications for employment, etc.)

Monitoring compliance and responding to reported violations	Unit managers will remind employees regularly of best practices on protecting the confidentiality of constituent information, and will take prompt corrective actions when a possible violation has been identified.
Complying with the Privacy of Constituent Information Policy	Policy compliance standards and expectations are defined and described in the *Faculty Handbook*, *Staff Handbook*, and *Student Handbook*.

The following documents provide the critical means of implementation of the Privacy of Constituent Information Policy.

Required Documents	Purpose
Annual Family Educational Rights and Privacy Act (FERPA) communiqué to students	To define what information on students is considered public and what is considered as confidential as provided by the Family Educational Rights and Privacy Act and subsequent amendments.
Catalog	To declare that a student is considered to be the guardian of his/her records, to define what records are public and which are private, and to identify means by which information generally considered personal and private by FERPA may be shared with parents, guardians or other interested individuals to comply with federal legislation.
Crisis response and imminent harm protocols	To define actions, lines of authority and communication channels that will be implemented` if a crisis or imminent harm incident occurs.

Additional Documents	Purpose
Unit operation manuals	To describe the protocols and actions units will take to assure that the information each possesses is protected to maintain confidentiality and minimizes the University's exposure to risk associated with violations of privacy.
Information technology protocols	Units with significant information technology responsibilities will define protocols that protect the integrity of electronic data, provide access through a table of permissions only to those with a documented need to know, and to provide a methodology for recovering of electronic information should a disaster incident occur that involves the University's infrastructure.
Email and voice mail distribution guidelines	To provide wise counsel to campus participants on best and safe practices appropriate for public and private communication.
Email disclaimer statements	To identify that information, shared through email and similar electronic technologies, is considered to be confidential, and not to be forwarded or shared, unless specific permission to share is granted.

There are no exclusions or exceptions of the Privacy of Constituent Information Policy, unless there is an emergency or situation that poses significant threats of the safety and well-being of campus participants, and then only critical or essential information will be shared with persons having documented interests.

The following individuals can be contacted for questions on the Privacy of Constituent Information Policy as outlined here.

For	Contact
Any question	Unit managers
Questions related to divisional application	Unit manager or Senior Leadership Team member assigned to the divisional responsibility
Reporting misuse of the Privacy of Constituent Information Policy	Unit manager or Director of Human Resources

The following outlines the approval, review, and revision history of the Privacy of Constituent Information Policy.

Version	Approval Date of Version	Version Type
1	January 2010	Initial Release