Marietta College
Policy Governing the Collection, Storage and Use of Social Security Number Data
June 2007

INTRODUCTION
Marietta College recognizes that it collects and maintains confidential information relating to its student, employees, and individuals associated with the College and is dedicated to ensuring the privacy and proper handling of this information. The purpose of this policy is to document procedures, promote awareness, and maintain compliance with the Family Educational Rights and Privacy Act of 1974 (FERPA) and other security measures related to Social Security Numbers (SSNs) and related confidential information pertaining to students, employees, and other individuals associated with the College. The following objectives apply:

- Broad awareness of the confidential nature of SSNs;
- Minimal reliance on the use of Social Security numbers for identification;
- Consistent application of this policy across all uses of SSNs at Marietta College;
- Confidence among students, employees and other individuals associated with the College that SSNs are handled in a confidential manner.

RESPONSIBLE PERSONS
Each Cabinet officer is responsible for overseeing the collection, maintenance, and use of SSNs in his/her division and for assuring compliance with FERPA. The Cabinet officer may delegate related day-to-day activities but the officer must maintain current familiarity with the current uses of SSNs in his/her division. The officer shall also approve any proposed new use of SSNs prior to implementation and shall make regular attempts to reduce the use of SSNs for identification in current applications.

Cabinet officers will also assure that the employees in his/her division are sufficiently trained in the confidentiality and use of SSNs. The officer may collaborate with Human Resources and Information Technology in accomplishing training.

The Chief Information Officer (CIO) is responsible for management and protection of SSNs within the Datatel administrative software system and the Vice President for Advancement (VPAdv) is responsible for management and protection of SSNs within the Blackbaud Raisers Edge software system. Because the CIO and the VPAdv may have more routine active involvement with the day-to-day handling of SSNs within their respective computing and software systems, they shall advise other Cabinet officers in a timely manner of activities affecting SSNs in the officer's division. The CIO and the VPAdv may delegate duties and responsibilities related to SSNs, but maintain accountability for SSN use and security as described herein. The CIO and the appropriate Cabinet officer must authorize any new use of SSNs within College software systems.

The FERPA officer will serve as a resource person to Cabinet officers and the CIO to assure FERPA compliance in management of SSNs.

MARIETTA COLLEGE IDENTIFICATION NUMBERS (MCIDs)
The College assigns a unique MCID to each student and employee and as needed to other individuals associated with Marietta College. Each MCID is assigned as soon as possible following the first point of contact between the individual and the College. The MCID remains unique to the individual until the relationship between the individual and the College ends. The MCID is used in as many applications as possible in lieu of the SSN to identify the student,

employee or other associated individual. The following rules govern ownership, assignment, and use of MCIDs:

- MCIDs are the property of Marietta College and their use is at the discretion of the College within the parameters of the law;
- MCIDs are used to identify individuals and to provide authentication;
- To the maximum extent possible, the College will use MCIDs for identification and authentication in day-to-day operations including the Datatel and Raisers Edge administrative software systems;
- In circumstances where the College is currently using SSNs for identification and authentication, the College will as soon as practicable determine the feasibility of using MCIDs and will within a reasonable period cease the use of SSNs in favor of MCIDs for identification and authentication;
- Grades and other items of personal information will not be publicly posted or displayed in a manner where the SSN or MCID identifies the individual associated with the information, except to that individual;
- SSNs will be electronically transmitted only through encrypted mechanisms;
- College forms and documents that collect SSNs will contain language (see below) that explains reason(s) for collection and will indicate whether collection is mandatory or voluntary, the use(s) of SSNs, and the security and confidentiality governing the collection, storage and use of SSNs by the College;
- At reasonable intervals and subject to the availability of resources, paper and electronic documents containing SSNs will be disposed of in a secure manner such as cross-shredding (paper) or deletion from the database (electronic). If disposal is not readily possible, said documents containing SSNs will be maintained in log-in and password protected electronic files and/or locked storage systems (file cabinets);
- Except in cases where the College is legally required to collect SSNs and in which students, employees or other associated individuals are required to provide their SSN to the College in order for the College to accomplish its work, individuals may provide their SSN to the College on a voluntary basis and will not be denied access to College services if they refuse to provide their SSN;
- SSNs will be released to outside entities only as required by law, when permission is granted by the individual to whom the SSN is assigned, when College legal counsel has approved release, or when the outside entity is acting as the College's contractor or agent in accomplishing College work that requires the SSN. Each Cabinet officer will maintain a current list of said outside entities;
- SSNs will be used as required by law and to permit the College to accomplish its work. SSNs may also be used from time to time to identify students, employees and other associated individuals when other means of identification are not available.
- This policy does not preclude the College from using SSNs to identify students, employees or other associated persons when other means of identification are not available.

SSN DATA MANAGEMENT

The CIO will determine and document appropriate security protocol for managing SSN data and for displaying SSNs on computer screens and written reports. SSNs will appear on screens or reports only if required by law or if necessary for completion of College work. When SSNs appear on screens or reports only the last five (5) digits will appear unless all digits (9) are required by law or if necessary for completion of College work.

SSN data input will be accomplished only by employees who have within the past twelve months cleared a criminal and credit background check. Students will not input SSN data into College software systems.

Employees or students who breach the confidentiality of SSNs may be subject to disciplinary action up to and including discharge or dismissal. College employees who fail to report a known breach of the confidentiality of SSNs may be subject to disciplinary action up to and including discharge.

NOTIFICATION REGARDING USE OF SSNs

The following language will be placed on appropriate forms and in indicated College publications to inform employees, students and other associated individuals of College policy and practice regarding collection, management and use of SSNs:

In all activities potentially involving the acquisition and use of social security numbers (SSNs), Marietta College strives to uphold the legal requirement to maintain confidentiality of SSNs imposed by the Family Educational Rights and Privacy Act (FERPA).

General use of social security numbers: Marietta College is committed to protecting the privacy of each member of its campus community, including students, employees, alumni, trustees, volunteers, and other affiliates. At any time in which Marietta College requests your social security number, you will be advised if reporting your SSN is mandatory or voluntary. If Marietta College collects your SSN, it will to its best ability protect the privacy of your SSN and will not disclose your SSN to others unless required by law, or if not required by law, without your prior permission. Under most circumstances, the College will not use your SSN as a primary means to identify you unless your Marietta College ID (MCID) number is not available or is insufficient to clearly identify you. Each student and each employee is assigned a MCID number. The College will specifically avoid the use of your SSN as an identifier in favor of your MCID number.

Use of student social security numbers: Furnishing a social security number (SSN) is voluntary and not required for enrollment. However, Marietta College is required by law to report to the Internal Revenue Service (IRS) the name, address, and SSN of persons from whom tuition and related payments are received. Law also requires the College to report to the IRS the SSN of persons to whom the College pays compensation. Marietta College will not disclose a SSN for any purpose not required by law without prior consent of the person to whom the SSN applies.

Use of employee social security numbers: Marietta College is required by law to report income along with a corresponding social security number (SSN) for each employee to whom compensation is paid, including student employees. Employee SSNs are maintained and used by the College for payroll and benefits purposes and are reported to federal, state and local agencies only as required by law. Marietta College will not disclose a SSN for any purpose not required by law without prior consent of the person to whom the SSN applies.

Reviewed by Legal Counsel 25Jun07
Approved by Cabinet 03Jul07