



SAINT LOUIS UNIVERSITY

Advancement Division

Confidentiality and Information Security Policy

Policy Number: FA
Classification:
Responsible University Official:
Vice President, University Advancement

Version Number: 1.0
Effective Date: 7.1.09

1.0 INTRODUCTION

This policy is designed to protect the privacy of alumni and other constituents of Saint Louis University (“SLU” or the “University”) and to maintain standards of confidentiality associated with Advancement Division operations and information.

The Advancement Division will, however, endeavor to provide assistance and support to those with a legitimate need for information to be used to promote and support the goals, programs, and overall mission of Saint Louis University.

2.0 PURPOSE

Saint Louis University’s Advancement Division utilizes and maintains databases, electronic information, paper records, and other confidential information. The information contained in these records is intended exclusively for purposes related to Saint Louis University’s programs.

All Saint Louis University employees have an ethical and professional obligation to respect the privacy of SLU constituents, and to protect and maintain the confidentiality of all information concerning constituents and related individuals.

This policy governs general Advancement Division operations and all access to constituent information as defined herein. University-wide policies and handbook provisions, including but not limited to, those related to confidentiality, information security and appropriate use, supersede this policy in all instances of conflict and omission.

3.0 DEFINITIONS

For purposes of this policy, capitalized terms are defined as follows:

Confidential Constituent Information: Confidential Constituent Information consists of any Constituent-related information:

- 1) Not specifically exempted in applicable legislation;
- 2) Not specifically exempted by University policy (e.g., the University’s official definition of “Directory Information”); and
- 3) Considered to be Personally Identifiable Information, as defined below, or marked “confidential.”

Confidential Information: Confidential Information consists of Confidential Constituent Information, as defined above, and all other proprietary University information, including non-public information related to Advancement operations and performance.

Constituent: Constituents include all University donors, prospective donors, alumni, students, faculty, staff, and volunteers.

Directory Information: Directory Information refers to information defined as such by the University’s official *Notification of Rights Under FERPA*. Unless otherwise indicated in writing by an individual student, Directory Information includes the following student data: name, home and school address, home and school phone number, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height (if student is a member of a University athletic team), dates of attendance, degrees and awards received (including Dean’s List), email address, and the most recent previous educational institution attended.

Personally Identifiable Information: Personally Identifiable Information consists of any information linked to an individual’s name (in whole or part), address, phone number, social security number, University ID number, or any other data that would reasonably associate the information with the individual.

4.0 DISCLOSURES TO SAINT LOUIS UNIVERSITY EMPLOYEES

4.1 Advancement Division Information Access

Direct and indirect access to Advancement Division databases, electronic information, paper records, and other Confidential Information (as defined herein) is granted exclusively to faculty, staff, and volunteers acting in the University’s interests and so recognized by Advancement Division officers.

Access to Advancement Division databases is authorized and granted, pursuant to University access policies and procedures, for SLU employees and agents who (a) have received authorization from the Advancement Division and (b) have been issued a unique and personal password (for password-protected systems). Information from these databases may only be shared with other employees and agents with a similar “need to know.” Advancement Division system passwords may not be shared with other users, including new employees who have not yet obtained their own passwords. Persons or

organizations accessing Advancement Division information must comply with Division's Restricted Use Policy Statement (as stated below), which in turn must accompany all Confidential Information delivered to third parties.

For quality control and tracking purposes, the Division's official data request forms should be completed for all data requests – including, but not limited to, mailing lists, gift lists, and custom reports.

4.2 Information Release to Other University Employees or Agents

Confidential Information, in any format, may not be distributed outside the Advancement Division without approval of the Vice President for University Advancement or his/her designee. Distributed information must be limited in form and content to that required for fulfilling specific University-authorized tasks. Confidential Constituent Information may be released for personal or non-University purposes only with the explicit approval of all persons whose data is being released.

Confidential Information provided to University agents or contractors (e.g., consultants, data screening vendors, mail houses, etc.) may not be reproduced, distributed, sold, or stored, electronically or otherwise, without the written consent of the Advancement Division. The Advancement Division's "Restricted Use Policy Statement," as set forth in section 7.6, below, must accompany all such provisions. Information provided on paper and other tangible media must be returned to the Advancement Division for archiving and/or disposal unless otherwise specified.

Memorial Donor Fund Information

On occasion, the family of the decedent for which a memorial gift fund is established may request donor contact and gift information for the purpose of sending thank-you letters. Under these circumstances, it is generally permissible to release only the names of non-anonymous donors. Addresses may be released with the explicit approval of the Vice President for University Advancement or his/her designee. Although personally identifiable gift amounts may not be communicated to non-University individuals, it is permissible to release the total raised for the memorial fund.

4.3 Information Usage Guidelines

- (a) Advancement Division information may not be released to unaffiliated organizations or individuals for uses construed as third-party fundraising, solicitation, or marketing of any kind. The use of such information for these purposes is limited to Saint Louis University in service of advancing its institutional mission and goals.
- (b) Advancement Division information may not be released to any person, group, or agency for political purposes.
- (c) Advancement Division information may not be used for any purpose other than that which has been officially approved.

4.4 Confidentiality Agreement

All recipients and users of Advancement Division databases and/or data must read and sign a confidentiality agreement. The Advancement Division confidentiality agreement applicable to Saint Louis University employees is attached hereto and incorporated herein as Appendix A.

5.0 DISCLOSURES TO THIRD-PARTIES

All third-party recipients and users of Advancement Division data must either 1) incorporate University-approved confidentiality clauses into their contracts and/or service agreements or 2) read and sign a University confidentiality agreement.

The Advancement Division confidentiality agreement applicable to third-party contractors is attached hereto and incorporated herein attached hereto and incorporated herein as Appendix B. The Advancement Division confidentiality agreement applicable to Saint Louis University students and/or volunteers is attached hereto and incorporated herein as Appendix C, which may be used to supplement the University's standard *Employee/Student Confidentiality and Nondisclosure Acknowledgement* as deemed necessary and prudent.

6.0 RESPONSIBILITIES AND ENFORCEMENT

It is the responsibility of Advancement Division representative(s) coordinating the distribution of Confidential Information to ensure that all distributed documents or data remain secure and are either returned or destroyed (i.e., shredded) as needed.

Appropriate action, including but not limited to, information access restrictions may be taken against any person found to be violating this policy.

7.0 PROCEDURES

7.1 Employee Agreements, Passwords, and Training

- (a) System passwords may not be issued prior to delivery of a signed confidentiality agreement.

7.2 Infrastructure Security

- (a) All Advancement Division areas housing confidential paper or electronic records must be reasonably secured during non-business hours.
- (b) It is the responsibility of designated staff members to maintain and regularly update Advancement Division inventories in a manner that

prevents and/or detects the theft of information-bearing computer equipment and portable electronic devices.

- (c) Advancement-owned information-bearing computer equipment is “scrubbed” prior to redistribution, long-term storage, and/or disposal.

7.3 Electronic Data Security

- (a) Advancement Division system users are prohibited from sharing and/or publicly posting passwords.
- (b) Computerized files containing Confidential Information are stored securely, accessible only to individuals authorized by the Vice President for University Advancement or his/her designee.
- (c) The Advancement Division’s database of record (“Banner”) is backed up and archived in accordance with the University’s enterprise system policies and procedures.

7.4 Document Control

- (a) All retrievals and returns of Constituent files stored in the Advancement Division file room must be documented on sign-out logs.
- (b) Sensitive documents intended for disposal must be shredded by a bonded disposal firm.
- (c) All unprocessed checks, pledges, and other payments must be stored in a central lockbox or safe during non-business hours. Generally, payments are processed and forwarded for deposit to the University cashier on the day received.

7.5 Third-Party Data Control

- (a) The release of all Confidential Information from the Advancement Division to non-University parties must be approved by the Vice President for University Advancement or his/her designee.
- (b) Mailing lists distributed to third parties are generally seeded to detect unauthorized use.

7.6 Restricted Policy Use Statement

All Confidential Information distributed by the University Advancement Division shall contain the following restricted policy use statement:

“This Confidential Information has been compiled by Saint Louis University for its exclusive use. It is not available for private use of any kind, including commercial solicitations or the expression of personal, political, social, or economic views. This information may not be reproduced, distributed, sold, or stored, either electronically or otherwise, without the written consent of an authorized representative of Saint Louis University.”

8.0 REFERENCES

Saint Louis University faculty and staff must also comply with the confidentiality provisions of all applicable federal, state, and local laws, rules, and regulations, including but not limited to, the Gramm-Leach Bliley Act and the Family Educational Rights and Privacy Act.

APPROVAL SIGNATURES

All policy exceptions must be approved by the Vice President for University Advancement or his/her designee.

This policy was approved by:

Thomas Keefe

Vice President, University Advancement

Saint Louis University