General Confidentiality
For reasons of privacy and ethics, employees are responsible to observe confidentiality in all matters relating to the University, its employees and students. When the necessity to maintain confidentiality is in question, it is always preferable to do so. Breaches of confidentiality can result in disciplinary action, up to and including termination of employment.

Student Information Confidentiality
Student Education Records (FERPA, “Buckley Amendment”)
University policy regarding the release of confidential information concerning students is required to conform to the Family Educational Rights and Privacy Act of 1974, more familiarly known as the “Buckley Amendment.” The Act serves two purposes: it grants students the right to inspect and review their official education record; and it denies access to such records by all other persons without written consent of the individual student, with some exceptions in special circumstances (e.g., parents of dependent students). The definition of education records is extremely broad, and thus employees should not provide any student information to a third party without the student’s consent unless directed to do so by a supervisor or other administrative personnel with sufficient authority to permit the disclosure. The penalty for noncompliance with the Act may be the loss of all federal funds.

The University is required to establish an official policy in compliance with the Act. Employees who wish to may obtain a copy of the policy from the Office of Student Life on each campus, or refer to the policy in the Student Handbook online.

Student Financial Information (Gramm-Leach-Bliley Act)
Pursuant to a federal statute known as the Gramm-Leach-Bliley Act (“GLBA”), St. John’s University and its employees, trainees, students and volunteers who provide services to the University (“University Personnel”) are required to protect the privacy of non-public student financial information (“SFI”).

The University’s primary responsibility to safeguard SFI under these statutes is to refrain from disclosing such information to third parties outside the University community without the student’s consent. However, to help ensure that SFI is not disclosed to third parties, the University also prohibits the disclosure of SFI to University Personnel unless they require it to perform services for the University.

Definition of “Non-Public Student Financial Information”
Non-public student financial information (“SFI”) includes all personally identifiable financial information concerning a student other than that which is in the public domain.
for public consumption. This includes a student’s income, his/her parent’s income, the amount of financial aid the student is receiving (whether in the form of a grant, loan, or pursuant to a work-study program), the student’s social security number, credit card account numbers, banking account numbers, and any other financial information that could identify the student. Such information may not be disclosed to third parties without the student’s consent pursuant to the GLBA, and the University prohibits the disclosure of such information to University Personnel who do not require such information to perform services to the University.

SFI is covered by this Policy whether it is contained on paper, stored electronically, or transmitted verbally.

Obligations

All Personnel have an independent obligation:

1. Not to disclose SFI to third parties (i.e. outside of the University) without the express written permission of the student whose information is at issue, unless such disclosure is authorized by the Office of General Counsel. However, disclosure is permitted in connection with performing a financial transaction for which the SFI was provided to the University in the first place (e.g., student financial aid processing, collection agency matters, credit card authorizations).

2. Not to share SFI with other Personnel (or students), unless such persons have a need to know the confidential information to perform their job tasks.

3. Not to copy SFI in any form unless authorized to do so as part of one’s job duties.

4. To take precautions to prevent the disclosure of SFI beyond those individuals to whom it may be appropriately disclosed in compliance with this Policy. In this regard, Personnel are required, among other things, to:
   a. comply with University and departmental procedures regarding computer and other security measures;
   b. shred all paper documents containing SFI prior to disposing of them in the trash;
   c. keep drawers, cabinets and file rooms containing SFI secured when not in use; and
   d. send interoffice mail containing SFI in sealed envelopes marked “Confidential – Open By Addressee Only.”

5. To report activities by any individual that you have reason to believe may be violating the confidentiality of SFI. Such reports should be directed to your department head or, if not reasonable under the circumstances, to Maura Woods or Anthony Macaluso, the University’s Security Coordinators.

Related Policies

- **Verification of Employment Information**: See Policy #121 in the HR Policy Manual for information regarding the release of employment data.
- **Personnel Records**: See Policy #122 in the HR Policy Manual for information regarding access and privacy with respect to personnel records.
- **Health Insurance Portability and Accountability Act (HIPAA Complaint Procedures)**: See Policy #710 in the HR Policy Manual for information regarding the
safeguarding of individually identifiable health information and complaint procedures for suspected violations of HIPAA privacy rights.

- **Family Educational Rights and Privacy Act (FERPA)**: Contact the Office of Student Life for more information, or refer to Chapter 6 of the Student Handbook online under Academic Regulations for information on student’s rights pursuant to the Act.

- **Information Security Program (pursuant to the Gramm-Leach-Bliley Act)**: Contact the Office of General Counsel on the Queens campus at extension 5699 or the Security Coordinators listed in the policy, above, for a copy of the full program materials.