Section:	VIII.2.7
Title:	Information Privacy
Effective Date:	May 22, 2017
Approved By:	President
Responsible Unit:	Office of the General Counsel (609) 771-2734; ogc@tcnj.edu
Related Documents:	• FERPA Policy • N.J. Stat. Ann. §56:8-163

History:		
Version	Date	Notes
1.0	May 22, 2017	New Policy; Initial release

I. INTRODUCTION

The College of New Jersey (the "College" or "TCNJ") is committed to the privacy of its students, faculty and staff. Information plays an important role in the College's educational and administrative activities. The College recognizes the importance of safeguarding this information while also preserving the free exchange of information encouraged in an academic environment. The College requires compliance with numerous laws that govern the responsible collection, use, retention, disclosure (collectively "Use") and disposal of information. The College has implemented measures to promote compliance with the requirements of federal and state privacy laws including the Family Educational Rights and Privacy Act ("FERPA")[1], Gramm-Leach-Bliley Act ("GLBA")[2], the New Jersey Library Confidentiality Statute, and the Federal Trade Commission ("FTC") "Red Flag Rules"[3]. Compliance with these laws and regulations is required by this policy and as outlined in related College policies, procedures, and other guidance documents.

II. DEFINITIONS

Personally Identifiable Information (PII) – Information that can be used to (either alone or in combination with other information) to identify, contact, or locate a specific individual, including: (i) An individual's first and last name (ii) the name of an individual's parent or other family members; (iii) the address of an individual or individual's family; (iv) a personal identifier, such as a Social Security

[1] U.S. Dept. of Education, Laws and Guidance, Family Educational Rights and Privacy Act (http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html)
[2] Federal Trade Commission, Gramm-Leach-Bliley Act (https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act)
[3] Federal Trade Commission, Red Flags Rules (https://www.ftc.gov/tips-advice/business-center/privacy-and-security/red-flags-rule)

number, driver's license number, college or state issued ID card number, or financial account number.

School Official – Under FERPA, a person employed by the College in an administrative, academic, or support staff position (including campus police, campus health providers, and student employees); a person or company with whom the College has contracted (such as an attorney, auditor, or collection agent) and been so designated in that contract; a person serving on the Board of Trustees; a student serving on an official school committee such as the all-college academic integrity board; or a person assisting another school official in performing his or her tasks.

III. POLICY

A. Information Privacy

i. General Policy

College employees shall limit the Use of PII to purposes that reasonably serve the College's (i) academic functions; (ii) administrative functions, including student, employee and governance support, and other operations; or (iii) other legally required purpose. Such Use must comply with applicable federal and state laws and regulations, and College policies. In general, PII maintained by the College should be treated as confidential, protected from unauthorized access and shared only on a "need-to-know" basis.

The College may disclose information in the course of investigations and lawsuits, in response to subpoenas and court orders, for the proper functioning of the College, to protect the safety and well-being of individuals or the community, and as otherwise permitted by law.

Agreements with third party vendors, consultants, or other business partners (collectively "Agents") who will have access to PII must ensure that the Agent is subject to obligations of confidentiality that will enable the College to continue to comply with its own obligations under applicable laws and regulations. All Agents who will have access to PII included in a student education record must be identified as a School Official, either through consultation with the Privacy Officer or through contractual arrangement, with a legitimate educational purpose in accessing the record.[4]

[4] For more information on education records and school officials, see the *FERPA policy*

ii. Prohibited Information

Employees shall not Use an individual's social security number or driver's license number as a personal identifier unless: (i) such use has been preapproved by the cognizant Vice President and Privacy Officer, and (ii) that employee has been authorized to Use such numbers.

Employees should be aware that certain security measures may be required when Use of prohibited information is permitted or authorized by this policy. Employees are required to follow all data security requirements as mandated by the Data Classification and Security Policy.

iii. Education Records

Students have a right to access their own education records under FERPA. In addition, FERPA protects against disclosure of a student's PII from education records to others, subject to limited exceptions (e.g., disclosure to School Officials with a legitimate educational purpose and disclosure of directory information to others). Employees shall comply with these rights and restrictions as outlined in the College's FERPA Policy.

iv. Other Categories of Information

Certain categories of information generally Used by a limited number of College units require specific guidance in order to ensure the College's compliance with all federal and state laws and regulations.

1. **Health Information.** Individuals have rights with respect to the privacy of their health information and employees shall comply with all applicable provisions of federal and state laws, regulations and professional codes of conduct and licensure requirements protecting health information privacy. Student health records are considered education records and are protected from unauthorized disclosure under FERPA. College units shall not conduct activities that would result in classification of the College (or any unit thereof) as a "covered entity" or "business associate" under the Health Insurance Portability and Accountability Act ("HIPAA") or otherwise require compliance with HIPAA without first contacting the Privacy Officer.

2. **Financial Services Records.** Employees shall comply with the applicable provisions of the Gramm-Leach-Bliley Act which requires that the College

protect the privacy and security of information collected in the course of providing certain financial services, such as student financial aid. In addition, employees shall comply with all requirements of the Payment Card Industry Data Security Standard (PCI DSS), which requires technical and operational controls to protect financial cardholder account information.

3. **Library Records.** Employees shall comply with the applicable provisions of the New Jersey Library Confidentiality Statute (NJSA 18A:73-42) which requires that the College protect the privacy of library records, which include all information collected in the course of providing library services to students, faculty, staff, or community members.

4. **FTC Red Flags.** Employees shall comply with applicable provisions of the Red Flags Rule which requires creditors to identify and respond to transactions or other activities that indicate the possible existence of identity theft.

When handling information, all students, faculty, and staff must properly classify and protect the information in accordance with College policies.

v. Open Public Records Request

The Open Public Records Act, N.J.S.A. 47:1 A-1, *et seq.*, ("OPRA"), identifies the types of records that are open to the public and procedures for requesting such records. The College, in compliance with OPRA, may make available to the requesting party requested records other than those identified by OPRA as exempt or as exceptions to government records subject to required disclosure, and those protected from disclosure by federal or other state law.

vi. Training

The Privacy Officer shall develop and administer appropriate privacy training for the College. Administrative unit leaders , with support from the Privacy Officer, are responsible for ensuring that all members of their workforce (including, as applicable, students, faculty, staff, and volunteers) complete training on the College's privacy policies and practices to the extent necessary and appropriate for them to carry out their required job functions. Units shall maintain adequate records of workforce training.

B. Violations of this Policy

Failure to comply with this Policy or other College policies and procedures concerning access, storage and transmission of information may result in disciplinary action.

Students, faculty, and staff who believe that this policy has been violated should report such violations to the Privacy Officer.