Frederick Community College

Protection of Personally Identifiable Information Policy and Procedures

BOT Approved: 11/15/2017
Revised: 8/7/2018

Table of Contents

Protection of PII Policy and Procedures

I. Philosophy and Scope

Frederick Community College ("FCC" or the "College") is committed to protecting the personally identifiable information (PII) of all students, staff members, and any other individual whose PII is collected by the College in carrying out its mission.

This Protection of PII Policy and Procedures is comprehensive in that it establishes overarching standards that affect a wide range of student and personnel records, information technology, and financial processes. This Policy and Procedures identifies related College policies and procedures that are associated with the overarching protection of PII.

The purpose of this Protection of PII Policy and Procedures is to provide a structure for and guidance about the protection of and access to sensitive data, information, and records in the possession of the College. The Chief Information Officer and the Vice President for Finance are charged with overall PII management and enforcement.

II. Definitions for the Purpose of this Policy and Procedures

A. **"Gramm Leach Bliley Act (GLBA)"** refers to a Federal law (primarily the Privacy Rule [16 CFR 313] and the Safeguards Rule [16 CFR 314]) requiring all financial institutions to develop, implement, and maintain safeguards to protect customer information. Because the College is in compliance with FERPA to protect the privacy of student records, FCC is deemed to be in compliance with GLBA.

B. **"Individual"** refers to a person for whom the College retains PII.

C. **"Need to Know"** refers to the need for information in a record for the purpose of performing the required task(s) and responsibilities during the course of an employee's job.

D. **"Periodic compliance checks"** refers to unscheduled inspections conducted by the appropriate Senior Leader to examine whether safeguards are adequately protecting PII.

E. **"Personally Identifiable Information"** refers to data or information which includes, but is not limited to: an individual's name; the name of the individual's other family members; the address of the individual or individual's family; a personal identifier, such as the individual's social security number, identification number, or biometric record; financial data including student loans, banking information, credit card or credit information; other indirect identifiers, such as the individual's date of birth, place of birth, and mother's maiden name; other information that, alone or in combination is linked to a specific individual that would allow a person, who does not have personal knowledge or the relevant circumstance, to identify the individual with reasonable certainty; or information requested by a person whom the College reasonably believes knows the identity of the individual to whom the record containing PII relates.

F. **"Record"** refers to any educational information or data recorded in any medium.

G. **"Red Flags Rule"** refers to a federal regulation issued by the Federal Trade Commission (FTC) as part of the implementation of the Fair and Accurate Credit Transaction (FACT) Act of 2003. The Red Flags Rule requires financial institutions

and creditors to implement a written Identity Theft Prevention Program and to provide for the continued administration of this Identity Theft Prevention Program. The College is subject to this rule because it holds student accounts that do not require full payment at the time of enrollment, and because it administers student loans.

H. **"Senior Leadership Team (SLT)"** refers to the President's Senior Leadership Team, comprised of the President; the Provost/Executive Vice President for Academic Affairs, Continuing Education, and Workforce Development; the Vice President (VP) for Finance; the VP for Human Resources; the VP for Learning Support; the Chief of Operations; the Chief Information Officer; and the Special Assistant to the President for Institutional Effectiveness.

I. **"Sole Possession Record"** refers to a record that is kept in the sole possession of the maker, is used only as a personal memory aid, and is not accessible or revealed to any other person except a temporary substitute for the maker of the record.

III. Required Strategies for the Protection of Personally Identifiable Information

A. Minimizing PII Use

Staff should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish a specific business purpose and mission. The likelihood of harm caused by a breach involving PII is greatly reduced if the College minimizes the amount of PII it uses, collects, and stores. When creating a new form, PII should only be requested if the presence of that information is absolutely necessary and has been approved by the Chief Information Officer or Vice President for Finance.

B. Categorizing PII

All PII is not created equal. Some types of PII have the potential to subject individuals and/or the College to harm if inappropriately accessed, used, or disclosed. When PII is requested, the Chief Information Officer or the Vice President for Finance will evaluate the context of use and determine if the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated is appropriate and aligns with this policy and other policies and procedures linked within this document.

C. Access to and Location of PII

Prior approval is required from the Chief Information Officer or Vice President for Finance to collect and/or house data on any server or system not maintained, owned, or controlled by the College.

D. Evaluation of PII Use

When evaluating a request to use PII, the following factors must be considered:

1. The purpose of the data collection;
2. Whether there is another source of pre-existing data (deals with reduction of duplicative information);
3. Whether all information requested is required (minimizing collection to only what is required);

4. How the data are being stored, for how long, and in what state (deals with physical location, type of device, encryption, and retention);
5. How the data are being transmitted (if applicable) and in what state (deals with encryption);
6. Whether agreements bind the College with third parties (deals with software or web applications or forms); and
7. Whether the use of the PII has been vetted and approved by either the Chief Information Officer or Vice President for Finance.

E. **Administrative Safeguards**

Administrative safeguards include pertinent policies to safeguard PII, training to increase awareness of and compliance with policies and procedures related to safeguarding PII, and communication of philosophy, policies, and procedures related to PII to both internal and external stakeholders.

Administrative safeguards are created to ensure the College complies with the protection of PII in general, FERPA, and by extension the GLBA, and the FTC Red Flags Rule.

F. **Technical Safeguards**

Technical safeguards include the development of information technology policies and procedures, implementation of tools to monitor and control access to PII, and strategies to retain and back up critical PII.

Technical safeguards, wherever possible, are treated as confidential to limit exploits that might lead to unintended or malicious exposure of PII.

G. **Physical Safeguards**

Physical safeguards include the development of standard operating procedures to provide physical control and destruction of PII, including but not limited to access control, secure storage facilities, shred bins, and broad-spectrum surveillance in support of physical security for PII.

Physical safeguards, wherever possible, are treated as confidential to limit exploits that might lead to unintended or malicious exposure of PII.

H. **Employee Training**

Annual PII training is required of all employees. In addition, existing and new policies and procedures will be reviewed to incorporate training elements specific to that policy.

IV. Associated College Policies and Procedures

A. Policies and Procedures Related to Academic Affairs, Continuing Education, and Workforce Development

The following College policies and procedures are related to Academic Affairs, Continuing Education, and Workforce Development records that contain PII:

1. Academic Assessment and Placement Policy and Procedures (deals with test scores and student disability status)
2. Academic Standards Policy and Procedures (deals with awarding of grades, credits, and degrees)
3. Code of Student Conduct Policy and Procedures (deals with academic integrity)
4. College Travel and Transportation Services Policy and Procedures (rosters, waivers, medical information)
5. Complaint Policy and Procedures for Students (policy linked with FERPA)
6. International Travel Policy and Procedures (rosters, waivers, medical information)

Since the policies and procedures are associated with this overarching Protection of PII Policy and Procedures, they will be reviewed by the Provost/Executive Vice President for Academic Affairs, Continuing Education, and Workforce Development annually as part of the periodic scheduled review. The Provost/Executive Vice President for Academic Affairs, Continuing Education, and Workforce Development will also conduct periodic compliance checks related to PII.

B. **Policies and Procedures Related to Learning Support**

The following College policies and procedures are related to Learning Support records that contain PII:

1. Admissions Policy and Procedures (deals with student PII)
2. Alcohol, Tobacco, Opioid, and Other Drug Use and Awareness Policy and Procedures (deals with reporting for students for ATODA concerns)
3. Behavioral Evaluation and Response Team Policy and Procedures (deals with student health status)
4. College Travel and Transportation Services Policy and Procedures (rosters, waivers, medical information)
5. Name for Student Records Policy and Procedures (covers collection and use of PII)
6. Non-Discrimination Policy and Procedures (deals with complaints and investigations for students)
7. Posthumous Awards for Students Policy and Procedures (deals with student academic progress records)
8. Privacy and Access to Education Records Policy and Procedures (FERPA)
9. Residency Policy and Procedures (requires capture and storage of PII)
10. Student Withdrawal Policy and Procedures (linked to BERT and FERPA-protected student PII)
11. Title IX Sexual Misconduct Policy and Procedures (deals with confidentiality and investigations of students)

12. Video Monitoring of College Premises Policy and Procedures (deals with controlled access to video monitoring and use of collected information)

Since the policies and procedures are associated with this overarching Protection of PII Policy and Procedures, they will be reviewed by the Vice President for Learning Support annually as part of the periodic scheduled review. The Vice President for Learning Support will also conduct periodic compliance checks related to PII.

C. **Policies and Procedures Related to Finance**

The following College policies and procedures are related to Finance records that contain PII:

1. Records Retention Policy and Procedures (deals with PII)
2. Travel and Expense Reimbursement Policy and Procedures (collects PII for reimbursement)
3. Tuition and Fees Policy and Procedures (linked to financial records and tied to Red Flags Rule and GLBA)

Since the policies and procedures are associated with this overarching Protection of PII Policy and Procedures, they will be reviewed by the Vice President for Finance annually as part of the periodic scheduled review. The Vice President for Finance will also conduct periodic compliance checks related to PII.

D. **Policies and Procedures Related to Human Resources**

The following College policies and procedures are related to Human Resources records that contain PII:

1. Auxiliary Benefits Policy and Procedures (deals with employee health status and insurance)
2. Complaint Policy and Procedures for Employees (deals with Title IX issues as well as investigations)
3. Employee Code of Ethics (addresses control of confidential information)
4. Employee Misconduct Policy and Procedures (deals with HR actions)
5. Leave Benefits Policy and Procedures (deals with health and HR actions)
6. Non-Discrimination Policy and Procedures (deals with complaints and investigations for staff)
7. Separation from Employment Policy and Appeal Procedure for Involuntary Separation from Employment (in relation to appeal procedure)
8. Sick Leave Bank Policy and Procedures (captures and stores employee health PII)
9. Title IX Sexual Misconduct Policy and Procedures (deals with confidentiality and investigations of staff)

Since the policies and procedures are associated with this overarching Protection of PII Policy and Procedures, they will be reviewed by the Vice President for Human

Resources annually as part of the periodic scheduled review. The Vice President for Human Resources will also conduct periodic compliance checks related to PII.

E. **Policies and Procedures Related to Information Technology:** The following College policies and procedures are related to Information Technology records that contain PII:

1. Student Personal Electronic Account Privacy Policy (deals with electronic data and access)
2. Technology Use Policy and Procedures (deals with College data storage, access, and use)

Since the policies and procedures are associated with this overarching Protection of PII Policy and Procedures, they will be reviewed by the Chief Information Officer annually as part of the periodic scheduled review. The Chief Information Officer will also conduct periodic compliance checks related to PII.

F. **Policies and Procedures Related to Institutional Effectiveness:** The following College policies and procedures are related to Institutional Effectiveness records that contain PII:

1. Advertising by External Parties Policies and Procedures (obtains PII from external sources)
2. Institutional Review Board Policy and Procedures (deals with the PII of individuals involved in research projects at the College)

Since the policies and procedures are associated with this overarching Protection of PII Policy and Procedures, they will be reviewed by the Special Assistant to the President for Institutional Effectiveness annually as part of the periodic scheduled review. The Special Assistant to the President for Institutional Effectiveness will also conduct periodic compliance checks related to PII.

V. Procedures for the Protection of Personally Identifiable Information

A. Periodic Scheduled Reviews

This Policy and Procedures in its entirety, including associated policies and procedures, will be reviewed annually by the Senior Leadership Team. This annual effort will include a compliance review to improve training, communication, and performance related to safeguarding the PII of all individuals.

B. Periodic Compliance Checks

Senior Leaders will ensure that compliance checks related to this policy and procedures and associated policies and procedures are conducted at least three times per year. These compliance checks will be conducted using the rubric or checklist approved by the Senior Leadership Team. The results of the compliance checks will be used to continuously improve processes, procedures, training, communication, and infrastructure related to the protection of PII.

The documentation from the compliance checks will be retained according to the IT retention schedule by the Chief Information Officer and used to identify trends and PII compliance target training and in the annual scheduled policy review conducted by the Senior Leadership Team.

C. **Incident Response**

Specific steps on how the College responds to incidents concerning PII are found within the Information Security Incident Response Procedures, a standard operating procedure document maintained by the Chief Information Officer and Executive Director of Network Infrastructure and IT Security Officer.

D. **Consequence for Failure to Comply with this Policy**

Any individual who becomes aware of non-compliance with this policy and procedures has a responsibility to report it to the Chief Information Officer and/or the Vice President for Finance. Employee or student violators of this Policy and Procedures are subject to College disciplinary policies. Based on the nature and extent of the offense, employees are subject to appropriate personnel action, up to and including separation from employment. Students are subject to disciplinary action in accordance with procedures established under the Code of Student Conduct, up to and including expulsion. Violations of this Policy and Procedures may be subject to the initiation of legal action by the College (See the Technology Use Policy and Procedures).