Frostburg State University

Privacy Policy

I. Introduction

Frostburg State University (the University) has adopted this Privacy Policy to govern the handling of our community's private personal information. The institution takes the privacy of any Personally Identifiable Information very seriously and will take any steps necessary to ensure that all information entrusted to the institution is handled with the utmost case and in accordance with any applicable laws and regulations.

The purpose of the Policy is to:

- Define Personally Identifiable Information;
- Establish the University's general principles for protecting Personal Information; and
- Assign accountability for protection of Personal Information.

II. Definitions

"Data Subject" means the individual to whom a particular PII Record relates.

"Legitimate Basis or Legitimate Business Use" means that the University has a contractual need, public interest purpose, business purpose, or other legal obligation to retain and/or process information or data in the University's possession, or a Data Subject has consented to the retaining and/or processing of information or data in the University's possession.

"Personally Identifiable Information" (PII) includes any information that, taken alone or in combination with other information, enables the identification of an individual, including:

1. a full name;
2. a Social Security number;
3. a driver's license number, state identification card number, or other individual identification number;
4. a passport number;
5. biometric information including an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity;
6. geolocation data;

7. Internet or other electronic network activity information, including browsing history, search history, and information regarding an individual's interaction with an Internet website, application, or advertisement; and
8. a financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account.

Personally Identifiable Information does not include data rendered anonymous through the use of techniques, including obfuscation, delegation and redaction, and encryption, so that the individual is no longer identifiable.

“Records” means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

“System” means an electronic or other physical medium maintained or administered by the University and used on a procedural basis to store information in the ordinary course of the business of the University.

“System of Record” means a System that has been designated by the University as a System of Record. Determination that a System is a System of Record is based on the following criteria:

- the risk posed to individuals by the Personally Identifiable Information processed and stored on the System;
- the relationship of the System to the overall function of the University; and
- the technical and financial feasibility of implementing privacy controls and services within the System.

III. Statutory Conflict

If at any point this policy conflicts with local, state, federal, or international laws or regulations, the applicable laws and regulations shall control.

IV. Scope

This Policy applies to all University employees, agents, representatives, contractors, third-party providers of services, students, guests of the University, and any other person with access to Personally Identifiable Information owned or controlled by the University.

This Policy applies to all Personally Identifiable Information collected, maintained, transmitted, stored, retained, or otherwise used by the University regardless of how the information was collected, the media on which that information is stored, or the relationship between the University and the Data Subject.

This Policy applies regardless of the origin of the PII, including but not limited to, existing University data sets, newly collected data sets, and data sets received from or created by third parties.

This Policy applies to all locations and operations of the University including but not limited to applications, projects, systems, or services that seek to access, collect, or otherwise use Personally Identifiable Information.

However, this policy does not apply to Personally Identifiable Information that:

- is publicly available information that is lawfully made available to the general public from federal, State, or local government Records;
- an individual has consented to have publicly disseminated or listed;
- except for a medical record that a person is prohibited from redisclosing under § 4-302(d) of the Health--General Article, is disclosed in accordance with the federal Health Insurance Portability and Accountability Act;
- is disclosed in accordance with the federal Family Educational Rights and Privacy Act;
- is clinical information; or
- is information related to sponsored research.

V. Privacy Principles

This University has adopted the following principles to help guide decisions regarding the collection, storage, and use of Personally Identifiable Information.

1. Accuracy – the University will keep Personally Identifiable Information accurate, and where necessary, up to date.
2. Appropriate Access – All units of the University will apply the principle of least privilege when facilitating access to University PII: that is, users and applications should have the minimum access needed to perform their functions.
3. Expectation of Privacy – To promote academic freedom and an open, collegial atmosphere, the University recognizes and acknowledges that its employees, affiliates, students, and guests have a reasonable expectation of privacy. This expectation of privacy is subject to applicable state and federal laws in addition to University policies and regulations, including the Privacy Principles set forth in this Policy, the University's Policy on Acceptable Use of Information Technology Resources, and all associated standards and guidelines.
4. Minimization – The University will only collect the minimal amount of information that is necessary for a specific purpose and dispose of any PII when no longer needed for a previously authorized purpose.

5. Responsibility – Whomever requests Personally Identifiable Information has the responsibility to ensure that the collection, storage, and use of such data follows the appropriate University Policies and Guidelines as well as Federal and State laws and regulations.
6. Shared Responsibility – Everyone has a role in ensuring data quality, data protection, and the responsible handling of the University's information resources.
7. Storage – Personally Identifiable Information will be deleted in accordance with the University's retention/deletion policy when no longer needed for its originally collected purpose and not authorized, by the relevant Data Subjects, to be used for a new purpose.
8. Relevancy – The University will only collect information that is relevant for a specific purpose.
9. Transparency – The University is committed to being transparent about the information we collect and how it is used.

VI. Disclosures

Some Personally Identifiable Information may be subject to disclosure under the Maryland Public Information Act or other federal and state laws or regulations.

The University reserves the right to access and use Personally Identifiable Information in its sole discretion to investigate actual or suspected instances of misconduct or risk to the University, students, faculty, staff, and third parties, subject to applicable law and University policy.

The University reserves the right to disclose any relevant information, including PII, when required by law enforcement or to satisfy appropriate subpoenas, warrants, or other legal requirements.

VII. Organizational Structure

Chief Privacy Officer – There is a Chief Privacy Officer (CPO) who is responsible for the daily operations of the University's Privacy Office. It is the responsibility of the Chief Privacy Officer to provide technical, legal, and regulatory guidance to the University's leadership and business units concerning privacy matters. Additionally, the Chief Privacy Officer shall participate in and provide recommendations to the Institutional Privacy Council regarding this Policy, any of its supplemental documentation, and other privacy related topics.

Privacy Office – The Privacy Office is responsible for the day-to-day implementation and functioning of this Policy and the University's overall privacy program by handling privacy requests and providing the community with effective tools, appropriate resources, and training.

Institutional Privacy Council – The Institutional Privacy Council is responsible for the privacy governance program of the institution and will work with appropriate stakeholders to further the privacy program. For duties and responsibilities of the Council see “Institutional Privacy Council Responsibilities” below. The Chief Privacy Officer is the chair of the Institutional Privacy Council.

The Institutional Privacy Council is made up of the following:

1. Chief Privacy Officer
2. Chief Information Officer
3. Legal Counsel
4. Chief Human Resources Officer
5. Registrar
6. Director of Financial Aid
7. Director of Admissions
8. VP of Institutional Advancement (Alumni and Donor Records)
9. Director of Institutional Research (Oversight of Required Reporting)

VIII. Institutional Privacy Council Responsibilities

The Institutional Privacy Council has oversight authority of the privacy governance program of the University. The Privacy Council will ensure that the privacy governance program:

1. Identifies and supervises the management of every System of Record in the institution;
2. Identifies and documents the purposes for processing PII in any System of Record;
3. Ensures that the collection of PII is limited to only to the minimum amount of information necessary for the purpose of collection;
4. Ensures that any PII collected is accurate, relevant, and complete;
5. Oversees the process for Data Subjects to request all data about the Data Subject held in a System of Record;
6. Provides a process for Data Subjects to request correction of any inaccurate information or, make a note of any disputed information;
7. Provides a process to opt-out of the sharing of information with third parties if the University does not have a legitimate basis to process the information;
8. Provides a process for Data Subjects to request deletion of information if there is no legitimate basis for the University to continue having the information;
9. Governs the appropriate disclosure of PII to third parties; and
10. Oversees the institution’s privacy standards and guidelines and the institutional privacy statement.

IX. Standards and Guidelines

This Policy is supplemented by institutional Privacy Standards and Guidelines. These privacy standards and guidelines address the implementation of the institution’s privacy program, including but not limited to: the Privacy Principles identified in Section IV, access to specified data types, vendor management, incident response, and the exceptions process.

The Chief Privacy Officer or their designee may issue, amend, or rescind such Privacy Standards and Guidelines as the Chief Privacy Officer deems necessary to comply with legal obligations and University Policy.

X. Exceptions

Where a legitimate need has been demonstrated, such as a novel use of an existing data set for health and safety purposes, the [appropriate official(s)] or designee, in consultation with appropriate stakeholders, may grant exceptions to this Policy and its [supplemental materials].

When considering requests for exceptions, the [appropriate official(s)] or designee, in consultation with the Institutional Privacy Council, will conduct a privacy impact assessment that measures the documented purpose of the exception against the privacy risks to the individuals affected.

Any exceptions must be the minimum necessary to achieve the goals of the proposed use while still adhering to the principles outlined in this Policy.

Subject to the University's legal obligations or circumstances that necessitate immediate access, the University will attempt to provide advance notification to an individual prior to the use of the individual's PII pursuant to an exception request. In certain instances, individuals may be unavailable to receive such advance notification, or such notification may not be reasonably practicable. In such cases, use of the data may occur without notification, consistent with applicable law.

XI. Policy Violations

Suspected violations of this Policy or the University’s Privacy Standards and Guidelines will result in a review by the University in accordance with relevant University policies and procedures.

University employees or students who are found to have violated this Policy or the University’s Privacy Standards and Guidelines may be subject to disciplinary action in accordance with relevant University policies and procedures. Furthermore, certain violations may be referred to the appropriate State or Federal law enforcement for investigation.

Unit Heads who are found to be responsible for knowingly, intentionally, or recklessly violating this Policy or its associated [supplemental guidelines] may obligate the Unit to repay any and all costs associated with a security incident, or any penalties imposed by government agencies or regulators.

Revision History

Version Number	Date	Author	Description
1.0	June 2024	Lori Bennett	Initial Document
1.1	September 2024	Lori Bennett	Approved 9/30/2024