University of Baltimore
UBalt III-3.4
Privacy Policy
Approved by President Schmoke on: July 4, 2025

UBalt III-3.4 Privacy Policy

Introduction

The University of Baltimore (UBalt) 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 care and in accordance with any applicable laws and regulations.

The purpose of the Policy is to:
- Define Personally Identifiable Information;
- Establish UBalt's general principles for protecting Personal Information; and
- Assign accountability for protection of Personal Information.

Definitions

a. **Data Subject:** the individual to whom a particular Personally Identifiable Information Record relates.
b. **Legitimate Basis or Legitimate Business Use**: UBalt has a contractual need, public interest purpose, business purpose, or other legal obligation to retain and/or process information or data in UBalt's possession, or a Data Subject has consented to the retaining and/or processing of information or data in UBalt's possession.
c. **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.

d. **Records**: information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.
e. **System**: an electronic or other physical medium maintained or administered by UBalt and used on a procedural basis to store information in the ordinary course of the business of UBalt.
f. **System of Record**:   a System that has been designated by UBalt 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 UBalt; and
- the technical and financial feasibility of implementing privacy controls and services within the System.

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.

Scope

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

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

This Policy applies regardless of the origin of the PII, including but not limited to, existing UBalt 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 UBalt 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.

Privacy Principles

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

1. Accuracy – UBalt will keep Personally Identifiable Information accurate, and where necessary, up to date.
2. Appropriate Access – All units of UBalt will apply the principle of least privilege when facilitating access to UBalt 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, UBalt 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 UBalt policies and regulations, including the Privacy Principles set forth in this Policy, UBalt Policy on Acceptable Use of Information Technology Resources, and all associated guidelines and procedures.
4. Minimization – UBalt 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 UBalt 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 UBalt's information resources.
7. Storage – Personally Identifiable Information will be deleted in accordance with UBalt'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 – UBalt will only collect information that is relevant for a specific purpose.
9. Transparency – UBalt is committed to being transparent about the information we collect and how it is used.

Disclosures

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

UBalt 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 UBalt, students, faculty, staff, and third parties, subject to applicable law and University policy.

UBalt 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.

Guidelines and Procedures

This Policy is supplemented by institutional Privacy Guidelines and Procedures. These privacy guidelines and procedures address the implementation of the institution's privacy program, including but not limited to: the Privacy Principles, access to specified data types, vendor management, incident response, and the exceptions process.

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

Exceptions

Where a legitimate need has been demonstrated, such as a novel use of an existing data set for health and safety purposes, the Chief Information Officer or designee, in consultation with appropriate stakeholders, may grant exceptions to this Policy and its Privacy Guidelines and Procedures.

When considering requests for exceptions, the Chief Information Officer or designee 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 UBalt 's legal obligations or circumstances that necessitate immediate access, UBalt 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.

Policy Violations

Suspected violations of this Policy or UBalt's Privacy Guidelines and Procedures will result in a review by UBalt in accordance with relevant UBalt policies and procedures.

UBalt employees or students who are found to have violated this Policy or UBalt's Privacy Guidelines and Procedures 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 Privacy Guidelines and Procedures may obligate the Unit to repay any and all costs associated with a security incident, or any penalties imposed by government agencies or regulators.

Notifications of Breach

If UBalt discovers or is notified of a security breach of a system of record, they shall follow the steps outlined in the Privacy Guidelines and Procedures.