Policy Title: IT6010 - Data Privacy Policy

Subject Area: Information Technology

Responsible Official(s): Chief Information Officer

Responsible Office(s): Information Technology Services

Policy Statement

As the University of Memphis pursues its academic and research goals, we must understand our ethical, academic, and compliance-related obligations regarding privacy requirements and standards over data and information. This policy represents the University's commitment to respecting and protecting the privacy of its students, faculty, staff, alumni, research subjects, and anyone from whom the University may collect or receive Personal Information. The University prioritizes compliance and privacy and strives to ensure all Personal Information under our control is protected according to applicable laws, regulations, and University policies.

The University of Memphis builds trust by safeguarding its Personal Information. We understand the responsibility entrusted to us when managing Personal Information from students, faculty, staff, alumni, and anyone interacting with the University. We demonstrate this commitment by maintaining the confidentiality and integrity of all Personal Information in our care.

This policy ensures we manage Personal Information responsibly, complying with all laws, regulations, and University guidelines. It reflects our commitment to confidentiality, integrity, and accountability.

Definitions

Data Subject - A person who can be identified using Personal Information.

Data Steward - University Personnel with designated roles in collecting, entering, and managing data for their specific areas.

Disclosure - Disclosing, transferring, giving access to, or otherwise communicating Personal Information.

Personal Information - Any University information that could be used to identify an individual. These can include digital data and paper documents. Personal Information includes but is not limited to:
Name
Date of birth
Preferred gender
Ethnicity
Nationality
Sexual orientation
Address
Contact information (e.g., mobile phone, home phone)
Healthcare and health insurance information (e.g., medical diagnosis)
Biometric data (i.e., DNA, Retinal scan, Fingerprints, Voice signature)
Email address
Bank account number
Credit card number
Identification number (i.e., U.S. Social Security Number, Employee ID number, Insurance Number, Driver's license number, National Identity Card, Passport Card, Student ID number)
Political party
Religious Affiliation
Social organizations
Marital status
Employment records
Criminal records
IP (Internet Protocol) address

Restricted Information - Information includes data governed by specific laws (HIPAA, FERPA, GLBA, …) and data whose disclosure could significantly harm the University's operations. Additionally, the University may designate other information as restricted if deemed necessary.

University Personnel - Anyone affiliated with the University of Memphis, including faculty, researchers, staff, students (graduate and undergraduate), student workers, temporary employees, graduate assistants, volunteers, and third-party vendors or partners working on the University's behalf.

Use - The utilization of Personal Information for the purposes for which it was collected.

Scope and Application

To comply with the many data privacy laws that apply to the University of Memphis' activities,

we follow federal, state, and local regulations. These data privacy laws govern how we collect, use, store, share, and dispose of Personal Information. Types of Personal Information covered by these privacy laws include name, address, date of birth, gender, ethnicity, social security number, and any other information that can be used to identify an individual (see Personal Information in the Definition section for other examples). These data privacy laws apply to anyone affiliated with the University of Memphis, including faculty, researchers, staff, students (graduate and undergraduate), student workers, temporary employees, graduate assistants, volunteers, and third-party vendors or partners working on the University's behalf.

This policy serves as the foundation for the University's data privacy approach, outlining core principles and best practices. It works with University policies that address specific data privacy and security requirements, and University Personnel should review and comply with the following related policies and procedures.

Data Storage Guidelines contains requirements for using, storing, and transmitting Restricted Information.

AA3022 - Privacy of Education Records (Compliance with FERPA) further describes student information, outlining what student information is protected, who can access it and when, the rights students have over data.

BF4023 - Payment Card Industry (PCI) Compliance outlines the requirements for university units that process credit cards. These requirements follow the standards set by major credit card brands to protect cardholder data.

University Personnel with multiple roles (researcher, faculty, staff) must consider data use carefully. Privacy requirements can vary depending upon the specific role at a given time.

Policy

The University prioritizes data privacy. University personnel are accountable for following all policies and procedures regarding the collection, possession, usage, and management of Personal Information. The following core principles guide the University’s approach to Personal Information collection, use, disclosure, retention, and disposal. University Personnel must follow these principles when managing Personal Information. Exceptions are only allowed by law, regulation, or with approval from the Data Stewards.

Restrict the collection of Personal Information to achieve the specified goal. University Personnel should only collect Personal Information that is needed for the task at hand.

Personal Information should only be used for the purpose for which it is collected. University Personnel must safeguard the privacy and confidentiality of all Personal Information they access for their jobs.

Personal Information should only be accessed for job duties and only for the reason it was collected. University Personnel with multiple roles have an extra responsibility. Make sure you only access Personal Information collected and used for your specific role at a particular time. Example: To protect student privacy, faculty can only use student data from their classes for research if students consent to be involved.

Provide the least amount of data needed to fulfill requests when disclosing Personal Information. University Personnel should only share the Personal Information that is necessary for the request and always check if they are authorized to do so first.

Personal Information should only be disclosed to individuals authorized to receive that data. Before disclosing Personal Information, the identity of the individual receiving the data should be verified, and the individual's authorization to receive said data should be established. This includes verification of University Personnel.

Personal Information should be encrypted in transit and any devices containing Personal Information should use encrypted storage. Any device containing University Personal Information should be encrypted to prevent accidental loss of this data. This includes desktops, laptops, mobile devices, and removable storage. Personal Information should also be encrypted when transferred in a digital format. Please contact your designated Local Technical Support Provider (LSP) or the Service Desk at umtech@memphis.edu with questions regarding encrypting Personal Information.

Retain Personal Information in accordance with BF4005 - University Records Management Program**.** University Personnel should follow records retention requirements and keep Personal Information only for as long as necessary and dispose of it properly when it is no longer needed.

Dispose of Personal Information securely when no longer needed. University Personnel should dispose of Personal Information that no longer needs to be retained per BF4005 - University Record Management Program and the disposal must be done in a secure manner, such as by shredding paper documents, or by purging electronic data. Contact your designated LSP or the Service Desk at umtech@memphis.edu to securely dispose of electronic devices containing Personal Information.

When collecting Personal Information in a digital format, link to the University Privacy Notice**.** University Personnel should provide a clear notification about the Personal Information that will be collected, how it will be used, who it might be shared with, and the security measures in place to protect it.

Personal Information should not be sold.

Follow University guidelines for unsolicited Personal Information. Either securely destroy Personal Information that is not relevant, or follow Data Storage Guidelines for secure storage

if the data should be kept. As an example, University Personnel who receive an unsolicited email with Personal Information that is not relevant to their job should delete the email and any attachments promptly.

All data privacy incidents should be reported promptly. University Personnel must report all possible or actual data privacy incidents as defined in these principles of the policy statement to the Office of the CIO at cio@memphis.edu no later than 24 hours after the incident has been identified.

Colleges and departments can set stricter guidelines or procedures for handling Personal Information if needed in their area. Any additional guidelines or procedures must comply with all appropriate laws, regulations, or this policy. University of Memphis colleges and departments should consult with the Office of the CIO at cio@memphis.edu for guidance before developing any stricter guidelines or procedures.

To minimize privacy risks, it is critical to identify and assess potential privacy concerns before implementing new systems, technologies, or processes. The Office of the CIO at cio@memphis.edu should be involved early whenever University Personnel plan to manage Personal Information through new projects or initiatives.

Data Subject Rights

Data Subjects are granted rights concerning their data under existing data privacy laws (HIPAA, FERPA, GDPR). The right to access, delete, correct, restrict data usage, and be notified if their Personal Information is accessed without authorization are among the rights granted to Data Subjects under these laws.

Upon receiving a request to exercise a Data Subject's rights, the University will verify their identity and respond promptly. All responses must comply with applicable laws and regulations. Please contact the Office of the CIO at cio@memphis.edu with any questions.

Third Parties

When the University of Memphis partners with third-party vendors, consultants, or independent contractors that will be overseeing Personal Information, applicable data privacy language must be included in contracts in accordance with this policy.

Reporting

University Personnel who believe that this Data Privacy policy has been violated or have other data privacy concerns should contact the Office of the CIO at cio@memphis.edu. University Personnel should report any incidents or violations as soon as possible, and within 24 hours of an incident or violation having been identified.

Violations of Policy

University Personnel are accountable for following this Data Privacy policy regarding how the University collects, uses, accesses, stores, keeps, and disposes of Personal Information. Failure to comply may result in corrective action, disciplinary measures, or even termination of employment. Instances of failure to comply by University Personnel may also be referred to relevant administrative offices for further review.

Roles and Responsibilities

The Office of the CIO - Develop and review exceptions to the policy. Monitor compliance with this policy and provide ongoing communication and training to support University Personnel in following the policy and related procedures effectively.

University Personnel - Should act in accordance with this policy. University Personnel should promptly report any data privacy concerns, violations, or incidents to the Office of the CIO at cio@memphis.edu as outlined in this policy. University Personnel should get clarification from their supervisor or the Office of the CIO if it is unclear if something is permitted in the handling of Personal Information.

Supervisors, department chairs, and Deans - Set expectations that University Personnel are to follow this Data Privacy policy and demonstrate that the University of Memphis can be trusted with individuals' Personal Information and their privacy. Promptly report any data privacy concerns, violations, and incidents to the Office of the CIO at cio@memphis.edu as outlined in this policy.

Related Documents, Policies and Forms

AA3022 - Privacy of Education Records (Compliance with FERPA)
BF4005 - University Records Management Program
BF4013 - Red Flag Policy
BF4023 - Payment Card Industry (PCI) Compliance
Classification of University Data
Controlled Unclassified Information (CUI)
Data Storage Guidelines
Family Educational Rights and Privacy Act (FERPA)
IT6000 - Data Access
IT6003 - Acceptable Use of Information Technology Resources
IT6004 - Security and Protection of Electronic Information Resources
IT6005 - Data Security Policy
ITS Security Procedures and Best Practices
State of Tennessee Data Security Law
University Privacy Notice

Last Revision Update Log:
IT6010 – June 3, 2024