Information Privacy Policy
ADM 21.0
Information Technology

Policy Type: Administrative
Applies to: Faculty, staff, student employees and relevant third parties

POLICY DATES

Issued: 09/10/2018
Revised:
Edited: 01/2/2019
Reviewed:

University of Mount Union (the "University") collects, uses, stores, processes and distributes information essential to the performance of University business. The University respects the privacy of its constituents' data and continuously improves its methods of protecting such data. Although a large portion of University information is public, a portion of information is not public or otherwise protected by state, federal, and international laws ("Applicable Laws"). To comply with Applicable Laws and protect the University community, the University has the right and obligation to protect, manage, secure, and control information (whether in hard copy or stored in electronic format) in its possession, as well as shared with third parties for the purposes stated in this Information Privacy Policy ("Policy"), required by a contractual relationship, or as otherwise required by Applicable Laws. This Policy governs the collection, use, storage, processing and distribution of information or data.

Definitions

Term	Definition
GLBA	Gramm-Leach-Bliley Act which protects consumer financial information
HIPAA	Health Insurance Portability and Accountability Act which protects personal health information
GDPR	General Data Protection Regulation which requires business to protect personal data (as defined under GDPR) and privacy of EU and EEA (European Economic Area) citizens who are Customers
FERPA	Family Educational Rights and Privacy Act which protects personally identifiable student records
EU	European Union – a political and economic union of 28-member states that are located primarily in Europe. For purposes of this Policy "EU" includes the EEA
Custodian/Data Owner/Data Controller	Individual or unit that maintains any customer identifiable Records
Directory Information	Term defined under FERPA; which allows certain information about students to be published or released by the institution without consent of the student.
Customer	Includes student, employee, faculty, alumni (and family members) and third parties, including University vendors and service providers.
PHI	Personal Health Information, having the same meaning under HIPAA.
Data Protection Officer	As required by the GDPR, the institution's CIO and Director of IT for Security is currently assuming the role of the institution's Data Protection Officer. They are the governing officer of this Policy, who has the responsibility of enforcing this Policy and compliance with Applicable Laws.

Policy Details

I. Generally

Applies to: Faculty, staff, student employees and relevant third parties

A. Confidential Information (defined below) protected by Applicable Laws may only be shared with authorized persons in compliance with University policies and Applicable Laws. Applicable Laws include the Federal Privacy Act which protects social security numbers, the Gramm-Leach-Bliley Act (GLBA) which protects consumer financial information (as defined under GLBA), the Health Insurance Portability and Accountability Act (HIPAA) which protects personal health information (as defined under HIPAA), the General Data Protection Regulation (GDPR) which requires businesses to protect the personal data and privacy of EU citizens, and the Family Educational Rights and Privacy Act (FERPA) which protects personally identifiable student records.
B. All records pertaining to Customer data ("Records") that are collected, used, transmitted, stored, or maintained by the University and each of its individual offices are proprietary official University records, as such, remain the property of the University unless otherwise stated by Applicable Laws.
C. All employees, faculty and staff bear responsibility for protecting Confidential Information from unauthorized disclosure. This is true whether Confidential Information is stored on paper or in electronic format on any device. "Confidential Information" means non-public, proprietary, and/or sensitive data of the University and Customer data which includes, but is not limited to:
    - Records
    - Social Security Numbers
    - Disability Status
    - Health and Medical Information
    - Student Grades
    - Student Disciplinary Records
    - Consumer Financial Information
    - Student Identification Numbers
    - Trade Secrets
    - Credit and Debit Card Numbers
D. University relationships with third party vendors and service providers: All faculty, staff, and employees are strongly encouraged to evaluate third parties and new initiatives with data privacy and protection as a critical consideration. Projects should be designed from the outset with privacy and security built into the outcome and function of the project. Vendors and service providers should be properly vetted in cooperation with the Director of IT for Security to ensure that such party is capable of complying with Applicable Laws and University policies with respect to Confidential Information, including conducting a privacy impact assessment as required by Applicable Laws. All agreements with vendors and service providers that involve handling of Confidential Information must address data security and privacy subject to the final approval of the VP of Business Affairs, CIO and Director of IT for Security.
E. Customer Rights: Customers have certain rights and control over their respective Records. The University will post these rights in such locations as necessary to adequately inform Customers of these rights and the purposes under which a Customer Record will be collected, used, processed, stored, and maintained, including sharing with third parties performing services on the University's behalf. Faculty, staff and employees of the University should make themselves aware of the time frames upon which the University is required to investigate and respond to a Customer, depending on Applicable Laws.
    1. The right to be informed: This means anyone processing Customer Records must make clear what Records they are processing, why the processing is necessary and for a legitimate purpose, and other parties that may have access to the Records. On an annual basis the University will provide Customer an annual notice of rights with respect to their Records in accordance with Applicable Laws.
    2. The right of access (to inspect and review): This is the right of Customer to see what Records are held about them by the University as Custodian. Customers are granted the right to inspect and review their Records upon request and in accordance with Applicable Laws.
    3. The right to rectification (challenge information in Record): Customers have a right to challenge the content of their Record if they consider the information contained therein to be inaccurate, misleading, or inappropriate. This process may include an opportunity for amendment of the Record or insertion of written explanation by Customer. The right to

challenge grades (student) does not apply under FERPA unless the grade assigned was inaccurately recorded, under which condition the Record will be corrected.

4. The right to erasure (right to be forgotten): Under certain circumstances a Customer can ask for his or her Record to be deleted. Such circumstances are:
    a. If their Record is no longer required for the purposes it was collected
    b. If the Customer withdraws consent for the processing of the Record, if consent was the basis for the Record to be collected, used, and stored
    c. The Record has been unlawfully processed by the University or a third party on behalf of the University
    d. If the University is relying on legitimate interests as the University's basis for processing, the Customer objects to the processing of their Record, and there is no overriding legitimate interest to continue this processing
    e. If the University is processing the Record for direct marketing purposes and the Customer objects to that processing
5. The right to restrict processing: This gives the Customers the right to ask for a temporary halt to processing of his or her Record, such as in the case where a dispute or legal process involving the Record is in process, or the Record is being corrected.
6. The right to data portability: A Customer has the right to ask for any Record supplied directly to the University by him or her, to be provided in a structured, commonly used, and machine-readable format.
7. The right to object: The Customer has the right to object to further processing of the Record which is inconsistent with the primary purpose for which it was collected, including profiling, automation, and direct marketing
8. Rights related to automated decision making and profiling: Customers have the right not to be subject to a decision based solely on automated processing.

F. Release Without Consent: Customers have a limited right with respect to use, processing and disclosure of Records, such as:
    1. Requests in compliance with a lawful subpoena or judicial order.
    2. Requests in connection with a student's application for or receipt of financial aid.
    3. Requests by parents of a dependent student, as defined in Section 152 of the Internal Revenue Code of 1954.
    4. In the case of emergencies, the University may release all or a portion of a Record to appropriate persons in connection with an emergency, if the knowledge of such Record is necessary to protect the health or safety of a student or other persons.
    5. Requests by state authorities and agencies specifically exempted from the prior consent requirements by FERPA.
    6. To authorized federal officials who have need to audit and evaluate federally-supported programs.
    7. Records submitted to accrediting organizations.

G. Each faculty, employee, and staff member must assume responsibility for protecting Confidential Information from unauthorized exposure. This means faculty and staff must:
    1. Understand and follow Mount Union's Technology Resources Acceptable Use Policy;
    2. Understand and follow Mount Union's Credit Card Security Policy
    3. Understand and follow Mount Union's Data Incident Response Policy
    4. Understand and follow Mount Union's Information Security Policy
    5. Understand and follow Mount Union's FERPA guidelines, https://www.mountunion.edu/about-mount/leadership/administration/academic-affairs/ferpa
    6. Consult with the Director of IT for Security if uncertain whether information is confidential
    7. Consult with Director of IT for Security if uncertain how to safeguard Confidential Information
    8. Protect your network and system passwords and change them according to standards published by the Office of Information Technology
    9. NOT provide access to Confidential Information to any other person unless authorized to do so.
    10. Collect only the amount of Customer Record data points as is necessary to process the Record under University policies and Applicable Laws.

11. Periodically audit and review the Records and purge Records which either have not been utilized by the University or which are required by Applicable Laws or University's Data Retention Policy to delete.

H. Applicable Laws require the University to take certain actions in the event of unauthorized disclosure of Confidential Information. Faculty, staff, employees, students, and all third parties engaged by the foregoing MUST report any suspected unauthorized disclosure, theft, or loss of Confidential Information to the Director of IT for Security or a member of the incident response team identified in the Data Incident Response Policy immediately. In addition, the University may be required to report the theft or loss of any laptop, external hard drive, thumb drive, or other media that contains Confidential Information not only to the Director of IT for Security but also to the appropriate law enforcement authorities. It shall be the University's sole determination as to its reporting requirements, and all faculty, staff, employees and students will defer to the University to report any breach of Confidential Information.

I. Accountability
    1. It is the responsibility of all faculty, staff, employees, student employees and third-party contractual agents of the University to be informed of and follow the requirements under Applicable Laws to protect Confidential Information of the University and Customers.
    2. Any person or third party who violates this Policy may be subject to disciplinary action, including but not limited to, termination of employment and/or potential criminal prosecution under applicable federal, state, and local laws.
    3. Students who violate this policy are subject to disciplinary action under the Code of Student Conduct and/or potential criminal prosecution under Applicable Laws.
    4. Other individuals and entities to whom this Policy applies who violate this Policy are subject to appropriate sanctions, including but not limited to, termination of the relationship with the University and/or potential civil action and criminal prosecution under Applicable Laws.

PROCEDURE

Issued: 9/10/2018
Revised:
Edited: 01/2/2019
Reviewed:

I. Annual Notice to Students
    A. The annual notice is sent from the University Registrar to enrolled students at the start of each fall semester to explain the rights of students with respect to Records maintained by the University.

II. Conspicuous Notice to Customers
    A. The University will maintain and provide necessary and proper notices and disclosures to Customers under this Policy.

III. Customer Inspection and Review of Records
    A. A request to review Records must be made separately, in writing, to each office maintaining such Records. Unless otherwise required by Applicable Laws, each office holding the applicable Record must respond to requests to review and inspect as soon as possible and no later than 45 days.
    B. Information contained in Records will be fully explained to the customer by University staff or employees having control over the Record.
    C. Customers have the right to review only their own Records unless otherwise governed by Applicable Laws. When a Record contains information about more than one Customer, disclosure cannot include information regarding the other Customer(s), unless authorized by the University or in accordance with Applicable Laws.

IV. Challenge of Record
    A. Customers challenging information in their Records must submit, in writing to the office having control over the Record, a request for a meeting to review and discuss the challenged information, listing the specific information in question and the reasons for the challenge.

Applies to: Faculty, staff, student employees and relevant third parties

B. Customers will be afforded a full and fair opportunity to present evidence relevant to the reasons for the challenge.
C. The decision will be rendered in writing, noting the reason and summarizing all evidence presented within a reasonable period of time after the challenge is filed, as required by Applicable Laws.

V. Complaints, Concerns or Suggestions
A. Any Customer who has reason to believe that the University is not complying with Applicable Laws or this Policy should inform the University Registrar, Human Resources, Alumni, CIO or the Director of IT for Security.
B. Allegations will be promptly reviewed in compliance with Applicable Laws and University policy. If there is a conflict between Applicable Laws and University policies, Applicable Laws will control.

VI. Training
A. All employees must seek out the appropriate University provided training regarding their legal obligations based on their role. If in doubt as to appropriate training, please contact Human Resources.
B. Additional information and training may be requested by contacting Human Resources.

VII. Maintaining and Disposing of Customer Records
A. Records must be maintained, stored, retained and destroyed according to the University Records Retention and Document Destruction Policy found here:

Responsibilities

Position or Office	Responsibilities
Office of Information Technology	

Contacts

Subject	Office	Telephone	E-mail/URL
Information Privacy	Office of Information Technology	330-823-2854	**IT@mountunion.edu**

History

All changes must be listed sequentially, including edits and reviews. Note when the policy name or number changes.
Issued:

Revised:

Edited:

Reviewed: