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
Last Revised: 12/01/2021
Reviewed: 12/01/2021

This policy is reviewed annually by the Director of IT for Security, CIO, VP of Business Affairs, and VP of Marketing. This is an administrative type of policy and any major changes to this policy is approved by members of Presidents Council.

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 Officers. They are the governing officer of this Policy, who has the responsibility of enforcing this Policy and compliance with Applicable Laws. Also "Data Owners" within each administrative office who oversee data are also assumed data protection officers for their specific data

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

Term	Definition
Account	Means a unique account created for you to access Mount Union services.
Cookies	Small files that are placed on your computer, mobile device or any other device by a website, containing the details of your browsing history on that website among its many uses.
Data Controller	For the purposes of the GDPR (General Data Protection Regulation), refers to the Company as the legal person which along or jointly with others determines the purposes and means of the processing of personal data.
Device	Means any device that can access the service such as a computer, cellphone or a digital tablet.
Facebook Fan Page	Is a public profile named University of Mount Union specifically created by Mount Union on the Facebook social network, accessible from https://facebook.com/universityofmountunion/
Personal Data	Is any information that relates to an identified or identifiable individual. For GDPR, Personal Data means any information relating to you such as a name, an identification number, located data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.
Website Service	Refers to Website(s)
Service Providers	Means any natural or legal person who processes the data on behalf of Mount Union. It refers to third-party companies or individuals employed by Mount Union to facilitate the service, to provide the service on behalf of Mount Union, to perform services related to the service or to assist Mount Union in analyzing how the service is used. For the purpose of the GDPR, service providers are considered data processors.
Third-party Social Media Service	Refers to any website or any social network website through which a user can log in or create an account to use the service.
Usage Data	Refers to data collected automatically, either generated by the use of the service or from the service infrastructure itself. (for example, the duration of a page visit).
Website	Refers to University of Mount Union, access from https://www.mountunion.edu and other web sites for this domain.
You	Means the individual accessing or using the service, or other legal entity on behalf of which such individual is accessing or using the service, as applicable. Under GDPR, you can be referred to as the Data Subject or as the User as you are the individual using the service.

Policy Details

I. Generally

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.

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

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, CIO and VP of Business Affairs 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. Faculty, Staff and employees must also follow Mount Union's Purchasing Policy.

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, staff and student employee who has access to confidential data part of their role at the university and those individuals who come across confidential data knowingly or unknowingly must assume responsibility for protecting confidential Information from unauthorized exposure. This means they 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. Do 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 and CIO 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 and CIO 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. 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.
   2. Students who violate this policy are subject to disciplinary action under the Code of Student Conduct and/or potential criminal prosecution under Applicable Laws.
   3. 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.

II. Website(s) Collecting and Using Your Personal Data

While using our website(s), we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you. Personally identifiable information may include, but is not limited to:

Email address
First name and last name
Phone Number
Address, State, Province, ZIP/Postal code, City
Usage Data

Usage Data

Usage Data is collected automatically when using the website(s). Usage Data may include information such as your device's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our service that you visit, the time and date of your visit, the time spent on those pages, unique-device identifiers and other diagnostic data.

When you access the website/service by or through a mobile device, we may collect certain information automatically, including, but not limited to, the type of mobile device you use, your mobile device unique ID, the IP address of your mobile device, your mobile operating system, the type of mobile internet browser you use, unique device identifiers and other diagnostic data. We may also collect information that your browser sends whenever you visit our website/service or when you access the service by or through a mobile device.

Tracking Technologies and Cookies

We use Cookies and similar tracking technologies to track the activity on our service and store certain information. Tracking technologies used are beacons, tags, and scripts to collect and track information and to improve and analyze our Website(s)/Service. The technologies we use may include:

- Cookies or Browser Cookies: A cookie is a small file placed on your device. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some parts of our website(s)/service, unless you have adjusted your browser setting so that it will refuse cookies, our service may use cookies.

- Flash Cookies: Certain features of our service may use local stored objects (or Flash Cookies) to collect and store information about your preferences or your activity on our service. Flash Cookies are not managed by the same browser settings as those used for Browser Cookies. For more information on how you can delete Flash Cookies, please read " Where can I change the settings for disabling, or deleting local shared objects?" available at https://helpx.adobe.com/flash-player/kb/disable-local-shared-objects-flash.html

- Web Beacons: Certain sections of our website(s)/service and our emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit the University, for example, to count users who have visited those pages or opened an email and for other related website statistics (for example, recording the popularity of a certain section and verifying system and server integrity).

Cookies can be "persistent" or "session" cookies. Persistent cookies remain on your personal computer or mobile device when you go offline, while session cookies are deleted as soon as you close your web browser.

We use both persistent and session cookies for the purposes set out below:

Necessary/Essential Cookies
Type: Session Cookies
Administered by: Mount Union
Purpose: These cookies are essential to provide you with services available through the website and to enable you to use some of its features. They help to authenticate users and prevent fraudulent use of user accounts. Without these cookies, the website(s)/services that you have asked for cannot be provided, and we only use these cookies to provide you with those services.

Cookies Policy/Notice Acceptance Cookies
Type: Persistent Cookies
Administered by: Mount Union
Purpose: These cookies identify if users have accepted the use of cookies on the website.

Functionality Cookies
Type: Persistent Cookies
Administered by: Mount Union
Purpose: These cookies allow us to remember choices you make when you use the website, such as remembering your login details or language preference. The purpose of these cookies is to provide you with a more personal experience and to avoid you having to re-enter your preferences every time you use the website.

Tracking and Performance Cookies
Type: Persistent Cookies
Administered by: Third-Parties
Purpose: These cookies are used to track information about traffic to the website and how users use the website. The information gathered via these cookies may directly or indirectly identify you as an individual visitor. This is because the information collected is typically linked to a pseudonymous identifier associated with the device you use to access the website. We may also use these cookies to test new pages, features or new functionality of the website to see how our users react to them.

Use of Your Personal Data

Mount Union may use personal data for the following purposes:

- To provide and maintain our services, including to monitor the usage of our services.
- To manage your registration as a user of the service. The personal data you provide can give you access to different functionalities of the service that are available to you as a registered user.
- To contact you by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products or contracted services, including the security updates, when necessary or reasonable for their implementation.
- To provide you with news, special offers and general information about other goods, services and events which we can offer that are similar to those that you have already purchased or enquired about unless you have opted not to receive such information.
- To attend and manage your requests to Mount Union.
- To deliver targeted advertising to you. We may use your information to develop and display content and advertising (and work with third party vendors who do so) tailored to your interests and/or location and to ensure its effectiveness.
- We may use your information for business purposes.

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

- We may use your information for other purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns and to evaluate and improve our service, products, services, marketing and your experience.

We may share your information in the following situations for business purpose:

- We may share your personal information with service providers to monitor and analyze the use of our service, to advertise on third party websites to you after you visited our service, to contact you.
- We may share your information with our business partners to offer you certain products, services or promotions.
- When you share personal information or otherwise interact in the public areas with other users, such information may be viewed by all users and may be publicly distributed outside. If you interact with other users or register through a third-party social media service, your contacts on the third-party social media service may see your name, profile, pictures and description of your activity. Similarly, other users will be able to view descriptions of your activity, communicate with you and view your profile.
- We may disclose your personal information for any other purposes with your consent.

Retention of Your Personal Data

Mount Union will retain your personal data only for as long as is necessary for the purposes to conduct Business for purposes set out in this privacy policy. We will retain and use your personal data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies. Mount Union will also retain usage data for internal analysis purposes. Usage data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of our website(s)/services or we are legally obligated to retain this data for longer time periods.

Transfer of Your Personal Data

Your information, including personal data, is processed by Mount Union's operating offices and in other places where the parties involved in the processing are located. It means that this information may be transferred to and maintained on computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from your jurisdiction.

Your consent to this privacy policy followed by your submission of such information represents your agreement to that transfer.

Mount Union will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy and no transfer of your personal data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information.

Disclosure of Your Personal Data

Under certain circumstances, Mount Union may be required to disclose your personal data if required to do so by law or in response to valid requests by public authorities (e.g., a court or a government agency).

Mount Union may disclose your personal data in the good faith belief that such action is necessary to:

- Comply with a legal obligation
- Protect and defend the rights or property of Mount Union
- Prevent or investigate possible wrongdoing in connection with the services
- Protect the personal safety of users of the services or the public
- Protect against legal liability

Security of your personal data is important to us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While we strive to use commercially

acceptable means to protect your personal data, we cannot guarantee its absolute security.

III. Website(s) Processing of Your Personal Data

The service providers we use may have access to your personal data. These third-party vendors collect, store, use, process, and transfer information about your activity on our website(s)/services in accordance with their privacy policies.

Website Third-Party Service Providers

We may use third-party service providers to monitor and analyze the use of our website(s)/services.

- **Google Analytics**
  Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. Google uses the data collected to track and monitor the use of our website(s)/services. This data is shared with other Google services. Google may use the collected data to contextualize and personalize the ads of its own advertising network. You can opt-out of having made your activity on the services available to Google Analytics by installing the Google Analytics JavaScript (ga.js, analytics.js and dc.js) from sharing information with Google Analytics about visits activity. For more information on the privacy practices of Google, please visit the Google Privacy & terms web page: https://policies.google.com/privacy
- **Blueconic**
  Their privacy Policy can be viewed at https://www.blueconci.com/priacy-policy

We may use your personal data to contact you with newsletters, marketing or promotional materials and other information that may be of interest to you. You may opt-out of receiving any, or all, of these communications from Mount Union by following the unsubscribe link or instructions provided in any email we send or by contacting us.

We may use Email Marketing Service Providers to manage and send emails to you.

Third-Party vendors with which Mount Union is currently working and the locations of their privacy policies are below:

Advancement: Anthology: https://www.imodules.com/s/1333/19/1col2.aspx?cid=157&gid=1&pgid=230
Enrollment: Slate: https://slate.com/privacy
Student Affairs: Adirondack: https://www.adirondacksolutions.com/privacy-policy
Academics, Financial-Aid, Finance, HR, Payroll: Ellucian: https://www.ellucian.com/privacy
Advancement: Blackbaud: https://www.blackbaud.com/company/privacy-policy/north-america
Athletics: FrontRush: https://www.frontrush.com/web/privacy-policy.html
Graduway: https://graduway.com/privacy-policy-notice/
Prestosports: https://www.prestosports.com/privacy-policy
University Store: MBS: https://www.mbsdirect.net/disclaimer/privacy-policy.php
Microsoft: https://privacy.microsoft.com/en-us/privacystatement
WUFOO: https://www.wufoo.com/privacy/2016-01-18/

Online Payment Processing

We may provide paid products and/or services within the website(s)/services. In that case, we use third-party services for payment processing (e.g. payment processors).

We will not store or collect your payment card details. That information is provided directly to our third-party payment processors whose use of your personal information is governed by their privacy policy. These payment processors adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, MasterCard, American Express and Discover. PCI-DSS requirements help ensure the secure handling of payment information.

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

Below are the payment providers the University of Mount Union uses for credit card processing:
Stripe: https://stripe.cm/us/privacy
Square: https://squareup.com/legal/privacy-no-account
Touchnet: https://www.touchnet.com/en/privacy-policy

Behavioral Remarketing
Mount Union uses remarketing services to advertise to you after you accessed or visited our website(s)/services. We and our third-party vendors use cookies and non-cookie technologies to help us recognize your device and understand how you use our website(s)/services so that we can improve our services to reflect your interests and serve you advertisements that are likely to be of more interest to you.

These third-party vendors collect, store, use process and transfer information about your activity on our website(s)/services in accordance with their privacy policies and to enable us to:

- Measure and analyze traffic and browsing activity on our website(s)/services)
- Show advertisements for our products and/or services to you on third-party websites or apps
- Measure and analyze the performance of our advertising campaigns

Some of these third-party vendors may use non-cookie technologies that may not be impacted by browser settings that block cookies. Your browser may not permit you to block such technologies. You can use the following third-party tools to decline the collection and use of information for the purpose of serving you interested-based advertising.

- The NAI's opt-out platform: http://www.networkadvertising.org/choices/
- The EDAA's opt-out platform http://www.youronlinechoices.com/
- The DAA's opt-out platform: http://optout.aboutads.info/?c=2&lang+EN

You may opt-out of all personalized advertising by enabling privacy features on your online identifiers collected on our website(s)/services with these third-party vendors. This allows our third-party vendors to recognize and deliver you ads across devices and browsers. To read more about the technologies used by these third-party vendors and their cross-device capabilities please refer to the privacy policy of each vendor listed below:

Google Ads (AdWords): (AdWords) remarketing service is provided by Google Inc. You can opt-out of Google Analytics for display advertising and customize the Google display network ads by visiting the Google Ads Settings page: http://www.google.com/settings/ads. Google also recommends installing the Google Analytics Opt-out browser add on at https://tools.google.com/dlpage/gaoptout. For more information on the privacy practices of Google, please visit the Google Privacy & Terms web page: https://policies.google.com/privacy.

Facebook: Facebook remarketing service is provided by Facebook Inc. You can learn more about interest-based advertising from Facebook by visiting https://www.facebook.com/help/516147308587266
To opt-out from Facebook's interest-based ads, follow these instructions from Facebook: https://www.facebook.com/help/568137493302217.
Facebook adheres to the self-regulatory principles for online behavioral advertising established by the Digital Advertising Alliance. You can also opt-out from Facebook and other participating companies through the Digital Advertising Alliance:

- In the USA by going to http://www.aboutads.info/choices/.
- In Canada at http://youradchoices.ca/.
- In Europe at http://www.youronlinechoices.eu/

For more information on the privacy practices of Facebook, please visit Facebook's Data Policy: https://www.facebook.com/privacy/explanation.

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

AdRoll: AdRoll remarketing service is provided by NextRoll, Inc. You can opt-out of AdRoll remarketing by visiting this AdRoll advertising Preferences web page: http://info.evidon.com/pub_info/573?v=1&nt=1&nw=false or the Opt Out of Personalized Advertising web page: https://help.adroll.com/hc/en-us/articles/216599538-Opting-Out-ofPersonalized-Advertising. If you are a California resident, please read the "information For California Residents Only" section in the Privacy Policy of NextRoll, Inc.: https://www.nextroll.com/privacy#service-13 For more information on the privacy practices of AdRoll, please visit the NextRoll, Inc. Privacy Policy web page: https://www.nextroll.com/privacy.

Facebook Fan Page

Data Controller for the Facebook Fan Page

Mount Union is the data controller of your personal data collected while using the service as operator of the Facebook Fan Page: https://www.facebook.com/UniversityofMountunion. Mount Union and the operator of the social network Facebook are joint controllers.

Mount Union has entered into agreements with Facebook that define the terms for use of the Facebook Fan Page, among other things. These terms are mostly based on the Facebook terms of service: https://www.facebook.com/terms.php.

For more information, visit the Facebook privacy policy at https://www.facebook.com/policy.php or contact Facebook online, or by mail: Facebook, Inc. ATTN, Privacy Operations, 1601 Willow Road, Menlo Park, CA 94025, United States.

Facebook Insights

Mount Union use the Facebook Insights function in connection with the operation of the Facebook Fan Page and on the basis of the GDPR, in order to obtain anonymized statistical data about our users. For this purpose, Facebook places a Cookie on the device of the user visiting Mount Union Facebook Fan Page. Each Cookie contains a unique identifier code and remains active for a period of two years, except when it is deleted before the end of this period. Facebook receives, records, and processes the information stored in the Cookie, especially when the user visits the Facebook services, services that are provided by other members of the Facebook Fan page and services by other companies that use Facebook services.

For more information on the privacy practices of Facebook, please visit Facebook privacy policy at https://www.facebook.com/full_data_use_policy.

Children's Privacy

Mount Union's services does not address anyone under the age of 13. We do not knowingly collect personally identifiable information from anyone under the age of 13. If you are a parent or guardian and you are aware that your child has provided Mount Union with personal data, please contact us. If we become aware that we have collected personal data from anyone under the age of 13 without verification of parental consent, we take steps to remove that information from our servers.

If we need to rely on consent as a legal basis for processing your information and your country requires consent from a parent, we may require your parent's consent before we collect and use that information.

Links to Other Websites

Mount Union website(s)/services may contain links to other websites that are not operated by Mount Union. If you click on a third-party link, you will be directed to that third-party's site. We strongly advise you to review the Privacy Policy of every site you visit. We have no control over and assume no responsibility for the content, privacy policies or practices of any third-party sites or services.

IV. GDPR Privacy

Legal basis for processing personal data under GDPR

We may process personal data under the following conditions:

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

- **Consent:** You have given your consent for processing personal data for one or more specific purposes.
- **Performance of a contract:** Provision of personal data is necessary for the performance of an agreement with you and/or for any pre-contractual obligations thereof.
- **Legal obligations:** Processing personal data is necessary for compliance with a legal obligation to which Mount Union is subject.
- **Vital Interests:** Processing Personal Data is necessary in order to protect your vital interests or of another natural person.
- **Public Interests:** Processing personal data is related to a task that is carried out in the public interest or in the exercise of official authority vested in Mount Union.
- **Legitimate Interests:** Processing personal data is necessary for the purposes of the legitimate interests pursued by Mount Union.

In any case, Mount Union will help to clarify the specific legal basis that applies to the processing, and in particular whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract.

Your Rights under the GDPR
Mount Union undertakes to respect the confidentiality of your personal data and to guarantee you can exercise your rights.

You have the right under this privacy policy and by law if you are within the EU to:

- **Request access to your personal data:** The right to access, update or delete the information we have on you. Whenever made possible, you can access, update, or request deletion of your personal data.
- **Request correction of the personal data that we hold about you:** This right exists where we are relying on a legitimate interest as the legal basis for our processing and there is something about our particular situation, which makes you want to object to our processing of your personal data on this ground. You also have the right to object where we are processing your personal data for direct marketing purposes.
- **Request erasure of your personal data:** You have the right to ask us to delete or remove personal data when there is no good reason for us to continue processing it.
- **Request the transfer of your personal data:** Mount Union will provide to you, specific information, dependent on the office, your personal data upon request. Please note that this right only applies to automated information which you initially provided consent for Mount Union to use.
- **Withdraw Your consent.** You have the right to withdraw Your consent on using your Personal Data. If You withdraw Your consent, we may not be able to provide You with access to certain specific functionalities or service.

PROCEDURE

- Annual Notice to Students
  - 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 along with catalog.

- Conspicuous Notice to Customers
  - The University will maintain and provide necessary and proper notices and disclosures to Customers.

- Customer Inspection and Review of Records
  - Request to review records must be made separately, in writing, to each office maintain 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.

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

  - Information contained in records will be fully explained to the customer by university staff or employees having control of the record.

  - 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.

- Challenge of Record
  - 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.

  - Customers will be afforded a full and fair opportunity to present evidence relevant to the reasons for the challenge. 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.

- Complaints, Concerns or Suggestions
  - Any customer who has reason to believe that the university is not complying with applicable laws or this policy should inform the University Registrar, Business Office, Human Resources, Office of Alumni, CIO or the Director of IT for Security.

  - 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.

- Maintaining and Disposing of Customer Records
  - Records must be maintained, stored, retained and destroyed according to the University Records Retention and Document Destruction Policy

- Contact Us
  - If you have questions about this policy email the Office of Information Technology at IT@mountunion.edu.
  - If you are a student and have questions about your data email Mount Union's University Registrar at registrar@mountunion.ed.
  - If you have questions about Mount Union's websites or social media pages email the Mount Union's Office of Marketing at marketing@mountunion.edu
  - If you are an employee and have questions about your employee record, contact hr@mountunion.edu.
  - If you have questions on vendor records, contact the business office at businessoffice@mountunion.edu

- Changes to this Privacy Policy
  - We may update our Privacy Policy from time to time. You are advised to review this Privacy Policy
  - Periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page and updated with the "Last updated date at the top of this Privacy Policy.

Responsibilities

Position or Office	Responsibilities
Office of Information Technology	Oversee changes to this policy
Office of University Registrar	Oversee student records
Office of Human Resources	Oversee employee records

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

Position or Office	Responsibilities
Office of Business Affairs	Oversee vendor records
Office of Financial Aid	Oversee student financial aid records
Office of Student Affairs	Oversee student housing records
Office of Marketing	Oversee website(s) & Mount Union's social media pages

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: 09/10/2018

Last Revised: 12/01/2021

Reviewed: 12/01/2021