

PRIVACY POLICY AND TERMS OF AGREEMENT

At the University of Mindanao, our commitment to becoming a globally recognized institution offering quality, affordable, and open education goes hand in hand with our dedication to safeguarding the privacy of our stakeholders. In line with this commitment, we diligently adhere to privacy practices and comply with the provisions of the Data Privacy Act of 2012 and its Implementing Rules and Regulations, which are applicable to all information processing activities conducted by our institution.

The University of Mindanao (*UM*) respect your right to privacy and the confidentiality of your personal data.

The Privacy Policy explains the following:

- what are the personal data we collect, and why do we collect it;
- who will use the personal data collected, and how will it be used;
- to whom we share the personal data collected;
- how long we store and retain your personal data;
- how will the University of Mindanao handle data breaches; and
- what are the rights of the data subject with respect to their personal information collected?

The Terms of Agreement constitute our contract with you. Please review the Terms carefully before **you sign in**. By signing in, you acknowledge that you have accepted these Agreements and agree to be bound by them.

Other policies of the University of Mindanao (*the University*) which are not inconsistent with the Policy and the Terms, will remain valid. If any terms or provision of the Policy or the Terms shall be held invalid, illegal, or unenforceable, the remainder of the terms or provisions shall remain in full force and shall not be affected, impaired or invalidated.

DEFINITION OF TERMS

As stated in **RA 10173** (<https://privacy.gov.ph/data-privacy-act>), this agreement defines and uses the following terms.

Data subject – refers to an individual whose personal, sensitive personal or privileged information is processed by the organization.

Personal information - refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information or, when put together with other information, would directly and certainly identify an individual.

Sensitive personal information - refers to personal information:

- i. about an individual's age, color, race, ethnic origin, marital status, and religious, philosophical or political affiliations;
- ii. an individual's health, education, the sexual life or genetic of a person, or any offense committed by such person, the disposal of such actions, or the sentence of any court in such circumstances;
- iii. any issued documents by the government agencies peculiar to an individual, which includes, but is not limited to, social security numbers, previous or current health records, licenses, suspension or revocation, and tax returns; and
- iv. specifically established by an act of Congress or executive order to be kept classified.

PRIVACY POLICY

The University is committed to complying with the Data Privacy Act of 2012 and to cooperating fully with the National Privacy Commission (NPC). In this endeavor, UM is committed to ensuring the free flow of information and protecting and respecting the confidentiality of your personal information.

We have provided the following examples to clarify our Policy using simple and easily understandable language. These examples only encompass some types of personal data we process, and they only cover some of the methods and reasons for processing such data. Our commitment to data privacy and transparency extends beyond these illustrations, and we strive to handle all personal information with the utmost care and responsibility.

The Information We Collect, Acquire or Generate

We collect, acquire, or generate your personal information in forms, but not limited to written, photographic and filmed pictures, digital or biometric records. Personal data collected may include information upon employment, the information we acquire, attain or generate during your stay with us, and unsolicited information, particularly;

1. The information you provide us with your application for admission/employment/ accreditation/visit

Upon application for admission/employment/accreditation/visit, we collect information circumstances and directory information such as but not limited to:

Students - name, birth date, birthplace, age, sex, religion, home address, contact information, your email address, family history, previous schools attended, academic performance, disciplinary record, medical record, etc.

Employees - name, complete mailing address, email address, contact number/s, age, sex, place of birth, date of birth, gender, civil status, religion, citizenship, blood type and any other health information, education, photos, and documents issued by government agencies peculiar to an individual.

Suppliers/Vendors - name, complete mailing address, email address, contact number/s, website, names of corporate officers/partners/major owners, and any other documents issued by government agencies peculiar to an individual.

Guests/Visitors - time-in and time-out, name of visitor, address and company connected, contact number, personal identification card, the purpose of the visit, signature, vehicle plate number, if applicable.

2.The Information we acquire or generate

During your stay/employment/accreditation/visit with us, we will collect the following information:

Students - your academic or curricular undertakings, the classes you enroll in, academic performance, attendance record, medical record, etc. We will also obtain information concerning co-curricular matters, such as outreach activities, study tours, and extracurricular activities, such as membership in student organizations, leadership positions, and participation and attendance in seminars, competitions, and programs. We will also collect information in connection with any disciplinary incident/s, including associated sanctions you may be involved in.

Employees - your education, marital status, attendance record, medical record, consent letter signed upon work for an employee, identification card, and other information gained from reference checking and background investigation. We will also obtain information for and in relation to co-curricular matters, such as outreach activities and study tours, as well as extracurricular activities, including membership in labor organizations and participation in competitions, seminars, and platforms. Alongside this, we will also collect information in connection with any disciplinary incidents, including associated sanctions that may be involved in.

Suppliers/Visitors - your company profile, price list/quotation, product sample/brochure, DTI Registration, Customer References, Annual Business Permit, and BIR Certification.

Guests/Visitors - your visitor's record, and we will also collect information in connection with any incidents during your appointment or official visit, including associated sanctions that you may be involved in.

There will be various occasions when we acquire other forms of data (e.g., pictures or videos of activities you participated in, recordings from closed-circuit television cameras installed in the UM

premises for security purposes, etc.) or generate statistical information such as institutional ranking and performance evaluation.

3. Unsolicited Information

In some instances, some personal information is sent to or received by us even without prior request. In such cases, the University of Mindanao determines whether such information should be kept or disposed of. If it is related to our institutional interests, such information shall be treated with confidentiality, and we will immediately cause the disposal of such data in such a way that will protect your privacy.

Rights of the Data Subjects

The following are the rights written in the Implementing Rules and Regulations of Republic Act 10173, otherwise known as the Data Privacy Act of 2012:

Section 34. Rights of the Data Subject. The data subject is entitled to the following rights:

A. Right to be informed

1. The data subject has a right to be informed whether personal data pertaining to him/her shall be, are being, or have been processed, including the existence of automated decision-making and profiling.
2. The data subject shall be notified and furnished with the information indicated hereunder before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity:
 - Description of the personal data to be entered into the system;
 - Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;
 - Basis of processing, when processing is not based on the consent of the data subject;
 - Scope and method of personal data processing;
 - The recipients or classes of recipients to whom the personal data are or may be disclosed;
 - Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
 - The identity and contact details of the personal data controller or its representative;
 - The period for which the information will be stored; and
 - The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the Commission.

B. Right to object. The data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing, or profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject in the preceding paragraph. When a data subject objects or withholds consent, the personal information controller shall no longer process the personal data, unless:

1. The personal data is needed pursuant to a subpoena;
2. The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject; or
3. The information is being collected and processed as a result of a legal obligation.

C. Right to Access. The data subject has the right to reasonable access to, upon demand, the following:

- a. Contents of his or her personal data that were processed;
- b. Sources from which personal data were obtained;
- c. Names and addresses of recipients of the personal data;
- d. The manner by which such data were processed;
- e. Reasons for the disclosure of the personal data to recipients, if any;
- f. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;
- g. Date when his or her personal data concerning the data subject were last accessed and modified; and
- h. The designation, name or identity, and address of the personal information controller.

D. Right to rectification. The data subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof: Provided, That recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject.

E. Right to Erasure or Blocking. The data subject shall have the right to suspend, withdraw, or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system.

1. This right may be exercised upon discovery and substantial proof of any of the following:
 - The personal data is incomplete, outdated, false, or unlawfully obtained;
 - The personal data is being used for a purpose not authorized by the data subject;
 - The personal data is no longer necessary for the purposes for which they were collected;
 - The data subject withdraws consent or objects to the processing, and there is no other legal
 - ground or overriding legitimate interest for the processing;
 - The personal data concerns private information that is prejudicial to the data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
 - The processing is unlawful;
 - The personal information controller or personal information processor violated the rights of the data subject.

2. The personal information controller may notify third parties who have previously received such processed personal information.

F. Right to damages. The data subject shall be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of his or her rights and freedoms as the data subject.

Section 35. *Transmissibility of Rights of the Data Subject.* The lawful heirs and assigns of the data subject may invoke the rights of the data subject to which he or she is an heir or an assignee, at any time after the death of the data subject, or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

Section 36. *Right to Data Portability.* Where his or her personal data is processed by electronic means and in a structured and commonly used format, the data subject shall have the right to obtain from the personal information controller a copy of such data in an electronic or structured format that is commonly used and allows for further use by the data subject. The exercise of this right shall primarily take into account the right of data subject to have control over his or her personal data being processed based on consent or contract, for commercial purpose, or through automated means. The Commission may specify the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

Section 37. *Limitation on Rights.* The immediately preceding sections shall not be applicable if the processed personal data are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out, and no decisions are taken regarding the data subject: Provided, that the personal data shall be held under strict confidentiality and

shall be used only for the declared purpose. The said sections are also not applicable to the processing of personal data gathered for the purpose of investigations in relation to any criminal, administrative, or tax liabilities of a data subject. Any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research or investigation.

FREQUENTLY ASKED QUESTIONS:

Who uses the data subject's Personal Information?

The personal information is accessed and used by the University of Mindanao personnel with a legitimate interest in it to carry out their contractual duties.

How do we use your Personal Information?

We use your information within the bounds of the law as we carry out our responsibilities as an educational institution. This information shall be used for academic, administrative, historical, and statistical purposes.

We may utilize your information for the following purpose/s:

- To ensure adherence to legal and regulatory requirements;
- To authenticate the identities of students, employees, vendors, and visitors;
- To derive valuable statistical insights and analytics to aid in administrative decision-making;
- To strengthen security measures and streamline investigations of reported violations;
- To readily generate essential statutory reports;
- For the effective management of employees and human resources, as mandated by applicable laws;
- For the advancement of research efforts, contributing to the collective knowledge;
- To establish, exercise, or defend legal claims as necessary.

Suppose we are to use your personal information other than our legitimate interests as an academic institution/employer/vendee. In that case, we will obtain your written consent for that specific purpose unless you request us to use or share your personal information for such purpose or processing without your permission is allowed under the Act or other applicable laws.

Who shall we share your Personal Information with?

The University is committed to safeguarding and meticulously handling personal information. Confidential data will never be shared or disclosed to any third parties without obtaining explicit consent from the involved data subjects. Should any situations arise where data disclosure becomes necessary and permitted, the University thoroughly evaluates the privacy and security practices of authorized third-party service providers. However, there may be situations where

disclosure is required by law or regulations. Data privacy and regulatory compliance are diligently ensured in all processes.

The University has established a standardized data request procedure for the internal sharing of Personal Information between different units. This formal process ensures that data is transmitted exclusively through official channels and is only shared for legitimate and authorized purposes. By adhering to this protocol, the University upholds strict data security and confidentiality standards, promoting a safe and trustworthy environment for handling sensitive information.

How long shall we retain your Personal Information?

Unless otherwise provided in the appropriate University procedures, we will keep your personal information indefinitely for historical and statistical purposes. A retention period is provided, and all records will be disposed of after that period.

How shall we store your Personal Information?

The University of Mindanao clientele's personal data, either paper-based or electronic/digital form, shall be stored in a data room that is practicable, functional, and secured against natural disasters, power disturbances, external access, and other similar threats.

How shall we dispose your Personal Information?

Personal data shall be disposed of or discarded securely to prevent further processing, unauthorized access, or disclosure to any other party or the public or prejudice the interests of the data subjects.

Procedures for disposal of personal data:

- a. disposal of files that contain personal data, whether such files are stored on paper, film, optical, or magnetic media;
- b. secure disposal of computer equipment, such as disk servers, desktop computers, and mobile phones at end-of-life, especially storage media: Provided that the procedure shall include the use of degaussers, erasers, and physical destruction devices, and
- c. disposal of personal data stored offsite.

How will we handle data breaches?

Any suspected attempts or actual breaches reported to the University will be dealt with in accordance with the law. The University of Mindanao will take all necessary steps to solve such a breach and mitigate the consequences thereof. All data subjects affected by such incidents will be promptly notified accordingly.

