

UNIVERSITY OF THE PHILIPPINES (UP) PRIVACY NOTICE FOR STUDENTS (REVISED AS OF THE 1st SEMESTER/TRIMESTER 2024-2025)

POLICY

To exercise and safeguard academic freedom and uphold your right to quality education, the University of the Philippines (UP) needs to process your personal and sensitive personal information (personal data) - that is, information that identifies you as an individual.

UP is committed to comply with the Philippine Data Privacy Act of 2012 (DPA) <https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/> in order to protect your right to data privacy.

This privacy notice explains in general terms:

- (1) the nature, purpose/(s) and extent of the processing of your personal data;
- (2) the legal basis/(es) for such processing;
- (3) the risks associated with such processing and the measures that UP has put in place to protect your data privacy; and
- (4) your data privacy rights and how you may exercise the same.

Please note that there are specific privacy notices for UP portals i.e. SLAS Online [SLAS Online \(up.edu.ph\)](https://slas.up.edu.ph), UP data processing systems e.g. privacy notice for pre enrollment health assessment (PEHA), the registration system that you used or are using in order to pre enlist and enroll, the learning management system (LMS), etc. of your campus that may also apply to the processing of your personal data. Systemwide privacy notices are available at [UP PRIVACY POLICIES - HOMEPAGE](#). Please visit the website of your campus for the privacy notices of campus based portals and data processing systems.

The term *UP/University/us* refers to the University of the Philippines System and its Constituent Universities (CU), any of its offices, or any of its officials or authorized personnel.

The term *you/your* refers to all students of the UP System, as well as those qualified to enroll in UP who seek to be admitted to the University and, where the context so indicates, in the case of students and admission applicants who are below eighteen (18) years of age, their parents or guardians who also sign registration related forms.

PERSONAL DATA COLLECTED FROM STUDENTS, AND THE PURPOSE/S AND LEGAL BASIS/ES FOR PROCESSING SUCH INFORMATION

Various UP offices collect your personal data through paper based and online processing systems. UP may likewise collect publicly available information about you as allowed by the DPA. Some application forms require you to provide a photograph. In some instances, your image is captured by UP's closed-circuit television (CCTV) cameras, or when UP documents, records, broadcasts (including live streaming), or publishes University activities or events.

When you applied for admission to UP you provided us, through the forms you submitted and signed (and in the case of minors– that your parents/guardians also signed), among others, your name, sex assigned at birth, date and place of birth, citizenship, your photograph, information about your family (names of your parents, their citizenship, civil status), if applicable, your access credentials for the portal you used in order to file your application for admission, signature and other personal information that we use, along with other documents you provide us (e.g. information contained in educational records and your PSA birth certificate and or marriage certificate) to be able to verify your identity in the course of determining your eligibility to enroll in UP. We required you to attest that the information that you provided us is true and correct as we also use the information in order to prevent the commission of fraud. Such processing is necessary for compliance with our legal obligation as a publicly funded University and to uphold our legitimate interest as an educational institution as well as that of taxpayers. When you provide UP with the personal data of third parties i.e. your parents and or your legal guardian or other person you have identified as your person to contact in case of emergency you warrant that you have obtained their consent for UP to process their personal data and will hold UP free and harmless from all liabilities for the processing of their personal data that you have provided to the University pursuant to its policies, rules and regulations.

In the case of students who were admitted through the UPCAT, you also provided the highest educational attainment and occupation of your parents as well as your family's annual household income and information regarding whether you are a member of an indigenous people's group. UP processed that information along with your permanent address and other information (e.g. grades) as the selection of campus qualifiers also considers socioeconomic and geographic factors as explained in the UPCAT Bulletin. Such processing is pursuant to Section 9 of RA 9500 which requires UP to take affirmative steps to enhance the access of disadvantaged students to the University's programs and services.

Non-Filipino citizens seeking admission to the University are required to provide personal data in order for UP to ascertain that their admission and enrollment is

allowed under applicable Philippine laws, rules and regulations, and University rules and procedures.

Upon your initial enrollment as well as in the case of your re-admission (if applicable), as a precondition for the issuance of your UP admission slip, you were required pursuant to Article 329 of the Revised UP Code to sign and submit the UP student pledge to your University Registrar which states:

In consideration of my admission to the University of the Philippines System and of the privileges of a student in this institution, I hereby promise and pledge to abide by and comply with all the rules and regulations laid down by competent authority in the University System and in the College or School in which I am enrolled.

By signing and submitting such student pledge you entered into a contract with UP. Your personal information e.g. your name, photograph, signature, sex assigned at birth, address, contact information, the name of your parents, etc. will be processed by UP (for recently admitted students) or, in the case of continuing students, was processed pursuant to such contract under 12b of the DPA.

As for your sensitive personal information, such as information related to your education; your exact birthdate and age; health information processed by UP offices in connection with your admission, such health information you submit for excusing your absence(s), the filing of leave of absence, readmission from absence without leave, appeals and the like; and, if applicable, information about your religious affiliation; information that you are a member of an Indigenous Peoples group; your civil status (in the event you are a married woman who opts to use the surname of your spouse); information regarding any offense that you have committed or alleged to have committed for which disciplinary proceedings may be conducted by UP, your UP student number and other government issued identification card information or document e.g. PSA birth certificate or marriage certificate that you submit to UP (in the case of a married woman who opts to use the surname of her spouse), it is understood that by entering into such contract with UP through the signing of the student pledge, you necessarily grant UP your consent for the processing of your sensitive personal information pursuant to the abovementioned applicable rules and regulations that UP adopted in order for the University to provide you with quality education such that there is no further need for us to obtain your consent for such processing done in the exercise of UPs academic freedom.

The personal data of students who continue to avail of the services of UP i.e. continuing students and those applying for certifications, clearances, true copy of grades, transcripts and other UP official documents shall continue to be processed pursuant to contract under 12b (contract) and 13 a (consent) of the DPA.

Note that National Privacy Commission (NPC) the body tasked with implementing the DPA, issued Advisory Opinion 2022-14

<https://privacy.gov.ph/wp-content/uploads/2022/08/Advisory-Opinion-No.-2022-014-Redacted.pdf> which states:

Although the “fulfillment of a contract” requirement is not included in the enumeration in Section 13, the NPC anchors the processing of sensitive personal information within the school’s educational framework upon consent based on jurisprudence defining the contractual nature of the relationship between the school and the student. Hence, upon enrollment, the student and the school are deemed to have executed a contract imbued with public interest that necessarily carries with it the consent of both parties. A different interpretation would otherwise create an absurd situation where schools may not process or use their student’s educational information for his or her own education and benefit.

Processing of personal data within the educational framework in relation to academic freedom.

At this juncture, the NPC would like to clarify that educational institutions may process personal data to achieve the purposes within its educational framework without the need for consent of the data subject. The data subject in an educational setting includes students, faculty and staff. It is then of utmost importance that the school delineates all processing operations, carefully identifying those that are core to the educational framework and those outside of it (e.g. marketing or public relations purposes)

x x x

Connected to this, the Supreme Court reiterated in the Isabelo, Jr. case, the doctrine in Ateneo de Manila University vs. Capulong that : “...this Court cited with approval the formulation made by Justice Felix Frankfurter of the essential freedoms subsumed in the term ‘academic freedom’ encompassing not only ‘the freedom to determine . . . on academic grounds who may teach, what may be taught (and) how it shall be taught’ but likewise ‘who may be admitted to study.’”

In the same vein, the NPC respects the same doctrine of Academic Freedom for the processing of personal data within the educational framework, if it is in accordance with the provisions of the DPA and other existing laws, rules and regulations. The NPC will remain neutral on the chosen methods and technology by the educational institution as long as it is within the bounds of the law (footnotes omitted,underscoring supplied).

You may wish to refer to the case of Garcia vs. Faculty Admissions Committee Loyola School of Theology G.R. No. L-40779 November 28, 1975 68 SCRA 277 (1975) cited in University of the Philippines vs. Arokiaswamy G.R. No. 134625. August 31, 1999 <https://elibrary.judiciary.gov.ph/thebookshelf/showdocs/1/3688> which states that:

Wide indeed is the sphere of autonomy granted to institutions of higher learning, for the constitutional grant of academic freedom, to quote again from *Garcia v. Faculty Admission Committee, Loyola School of Theology*, "is not to be construed in a niggardly manner or in a grudging fashion (footnotes omitted,underscoring supplied)."

UP processes your personal data , in the course of fulfilling its obligation, to provide you quality education by exercising its right to academic freedom, and upholding academic standards, when the University's duly authorized personnel process your enrollment; evaluate the work that you submit in fulfillment of your academic requirements and give you grades; act on your applications for change of matriculation, dropping, leave of absence and the like; determine your academic progress and compliance with the University's retention and other rules; evaluate and recommend you for graduation; act on appeals on such matters; and, in the event you are qualified under the rules, recommend that you be awarded honors upon your graduation.

Aside from sensitive personal information in the form of grades, you also provide UP with health information as part of the admission and registration processes so that the University may determine your physical fitness to enroll; and be able to provide you with the proper care when you avail of UP's health services; or in case of an emergency; or in compliance with University rules that are meant to uphold academic standards (e.g., submission of medical certificates in order for your absences to be excused, for you to drop a subject, go on leave of absence, or justify underloading in an appeal to graduate with honors, etc.).

UP processes information regarding your religious affiliation in the course of verifying your identity (e.g. offices match information in your birth certificate and school records provided to us etc.) to conduct research to see to it that we uphold the principle of democratic access; and that, as a non-sectarian institution, we do not discriminate on the basis of religious creed; and to uphold your right to freedom of religion (e.g. by providing you with services that are consistent with your beliefs in relation to your health needs and food preparation, etc.).

Contact information is processed by UP in order to be able to communicate effectively with you, and to enable us to contact your family or other people you identify, in the case of an emergency. For example, UP offices or your teachers may use the

information generated by the applicable registration system in order to contact you via email or via a messaging system for class related and other academic matters, as well as UP related activities and information. UP may also contact you in order to solicit your consent to participate in academic or non-commercial research.

UP processes personal data, and, in particular, financial information related to your studies, in order to administer State-funded and privately financed scholarships, as well as grants or other forms of assistance, pursuant to its contractual or legal obligations as part of the University's legitimate interests and that of taxpayers, as well as relevant third parties, such as donors or sponsors.

Your personal data may also be processed in order for UP to provide you with services, such as the issuance of your ID card, stickers or gate passes, library, dormitory, health, counseling and guidance services and the like; facilitate the processing of applications for insurance and insurance claims; determine whether the student organization or association to which you belong may be recognized and given access to University services, etc., to enable your participation in student elections, exchange programs, internships, training programs, conferences, etc.; administer scholarships, grants and other forms of assistance, pursuant to UP's contractual or legal obligations; or to protect your vitally important interests.

CCTVs and other security measures which may involve the processing of your personal data are intended to protect your vitally important interests, for public order and safety, and are processed pursuant to the University's and the public's legitimate interests. UP processes personal data in order to comply with its duty as an academic institution to exercise due diligence to prevent harm or injury to you or others.

You may also be required to present your UP ID, or if such is not yet available, your government issued identification card when you avail of University services, or when you request documents containing your personal data. If you request such information through a representative, UP will require that you provide a letter of authorization specifying the information or document requested, the purpose(s) for which the same will be used, and the presentation of your UP ID or other valid government-issued identification card (GIID), as well the GIID of your duly authorized representative, in order for UP to see to it that fraud is prevented, and your right to data privacy is upheld.

UP will process your name, student number and photograph in order to issue your UP radio-frequency enabled identification (RFID). A unique, randomly generated number, as well as your student number, will be encoded in the RFID tag or chip of your UP ID such that these will be the only information that can be read by a compatible RFID reader.

UP, using its RFID readers, will process the abovementioned information when you tap or wave your UP ID card in close proximity to such readers in order to:

1. regulate access to libraries and other University buildings in order to supplement other existing security measures in place;
2. provide you with RFID enabled services in UP offices where these are applicable or available; and
3. provide benefits to qualified students pursuant to the UP Charter and relevant internal rules.

UP has a legitimate interest in securing the UP community, its buildings and other assets and adopting means in order to provide services in a more efficient manner. UP is also required under its Charter to adopt measures in order to provide democratic access to its services. Rest assured that the University will process the above UP RFID information only for legitimate purposes, and for such periods allowed by the DPA and other applicable laws. UP has adopted appropriate measures to safeguard your right to data privacy over your abovementioned information.

The University provides for the secure processing and, when applicable, secure archival of the educational record and other relevant personal information of its students that are needed to verify their identity so that UP will be able to provide the proper transcripts, certifications, and other documents that current or former students or alumni may request as required by the Education Act of 1982, and comply with obligations to the UP Alumni Association under the UP Charter and University rules, as well as for historical and research purposes as permitted by law.

The relevant application forms and supporting documents submitted by those who are not qualified to enroll in UP, including those who are not accepted as shiftees or transferees, as well as qualified applicants who do not thereafter enroll in UP are securely disposed of within a reasonable period of time as determined by the University pursuant to applicable laws and regulations.

We also securely store and further process your educational record in order to comply with legal obligations such as providing information required by public authorities like the UNIFAST, CHED, Commission on Audit; to establish or defend legal claims; and to carry out other activities allowed or required by the DPA as well as other applicable laws and issuances.

UP likewise stores your personal data pursuant to Sec. 11 (f) of the DPA which states *Provided*, That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: *Provided, further*, That adequate safeguards are guaranteed by said laws authorizing their processing.

UP conducts research on stored, previously processed, de-identified data in order to comply with its legal obligations including its right and responsibility to exercise academic freedom under the 1987 Constitution and the UP Charter. UP as a research university must conduct scientific research in order to produce general demographic information and statistics regarding UP students across various time periods. Such research enables the University to assess whether its policies, programs, as well as procedures and revisions to the same in different years, enable the University, among others, to enhance the access of disadvantaged students to UP's programs and services (Sec. 9 of RA 9500 or the UP Charter), comply with the spirit of other applicable laws such as RA 10687 or the Unified Student Financial Assistance System for Tertiary Education (UniFAST) Act, and RA 10931 or the Universal Access to Quality Tertiary Education Act and to allow us to provide advice and technical assistance to public authorities such as Congress, the Commission on Higher Education, the UniFAST Board, etc. in accordance with Sec. 7 of the UP Charter.

Before any research is conducted by UP, so that we will be able to comply with our ethical obligations and uphold your right to privacy, duly authorized UP personnel will remove identifiers from the applicable dataset such that UP's researcher or research teams who will perform operations on such dataset will not be able to associate your data with you. The research results will only include aggregate or statistical data and general demographic information that does not identify you and any other data subjects.

Kindly note that Sec. 16.C.2 of Memorandum Circular 2023-4 issued by the National Privacy Commission provides that:

The conduct of research where the end results will be anonymized and will only disclose the general demographic of the research subjects does not require the consent of the data subject.

On the other hand, if research will make use of identifiable personal data, when so required by applicable laws, rules and or ethical guidelines such as the guidelines issued by the Philippine Health Research Ethics Board pursuant to the Philippine National Health Research System Act, we will first obtain the proper ethics clearance as well as your informed consent prior to the conduct of such research.

INSTANCES WHEN YOUR RELEVANT PERSONAL DATA MAY BE DISCLOSED BY UP TO THIRD PARTIES AND THE PURPOSE/S AND LEGAL BASIS FOR SUCH DISCLOSURES

The University will disclose or share your relevant personal and/or sensitive personal information to third parties in order to carry out its mandate as an academic institution, comply with legal obligations, perform its contractual obligations to you, promote and protect your interests, and in order to pursue its legitimate interests or that of a third party. UP discloses such information when required or allowed by law, or with your consent. Examples of these include:

1. posting the list of students qualified to enroll in UP as well as waitlisted applicants on bulletin boards pursuant to its functions under its Charter, and for transparency in the admissions process as allowed by NPC Advisory Opinion 2018-20
<https://privacy.gov.ph/wp-content/uploads/2022/01/AdOpNo.2018-020.pdf>
2. submission of information required by the UNIFAST Board and the Commission on Higher Education in order to implement the Universal Access to Quality Tertiary Education Act of 2017 (RA 10931) and the UNIFAST Act (RA 10687) pursuant to 4d of the DPA;
3. disclosure of information to the proper bodies to enable you to take licensure, board, bar examinations and the like;
4. disclosure of your personal data to relevant third parties in order for UP to respond to an emergency and comply with its duty to exercise due diligence to prevent harm or injury to you and/or others;
5. disclosure of your personal data in compliance with University policies, rules and processes adopted pursuant to the UP Charter in order to uphold or promote your interest and/or the principle of transparency in the conduct of student elections (e.g. posting of list of candidates and results); disclosures contained in the minutes of University bodies such as the Board of Regents in connection with graduation, student discipline, and other processes involving UPs exercise of academic freedom ;
6. providing information pursuant to the provisions of the DPA or other applicable laws, and lawful orders or processes issued by government agencies, courts, and law enforcement agencies.
7. disclosures to enable UP to participate in university ranking exercises and other similar activities pursuant to its right to academic freedom;
8. sharing personal data with your parent(s)/ guardian/spouse, or other next of kin, in order to promote your best interests as required by law, or when necessary in order for the University to respond to an emergency, uphold your vitally important interests, or to prevent harm to you and/or others, or with your consent, when consent is the proper basis for processing;
9. disclosures for your benefit, or in support of your interests, such as those intended to enable you to participate in exchange programs, conferences, trainings and the like, academic, athletic and other similar competitions or events; to apply for, receive and comply with terms and conditions of scholarships, grants and other forms of assistance; to be granted Civil Service

eligibility based on Latin honors under PD 907 or in relation to internship, employment or other career opportunities pursuant to UPs exercise of academic freedom or, when applicable, with your consent;

10. disclosures to recognize your achievements such as through the publication and distribution of the commencement program, and other materials containing the names of graduates, their respective courses/certificates and honors received, or sharing of relevant information with honor societies or entities that confer awards with your consent;
11. in the exercise of the sound discretion of UP pursuant to its mandate as a research university we may share your name, email, and other relevant personal information, with your consent, with researchers conducting academic or non-commercial research who have put in place applicable measures required by ethical guidelines and the DPA to uphold your privacy so that they can solicit your consent to participate in research;
12. news or feature articles about your achievements, awards received, research and public service activities and the like in University publications, websites or social media posts, disclosures that the University may make in the exercise of its sound discretion in response to inquiries from the press, or press releases and other similar disclosures for journalistic purposes, as allowed by the DPA, or when applicable, with your consent;
13. publishing, broadcasting or live streaming of University activities or events pursuant to the legitimate interests of the University and third parties or for journalistic purposes, as allowed by the DPA;
14. other instances analogous to the foregoing.

UP will take reasonable steps to require third parties who receive your information to uphold your right to data privacy.

DATA PRIVACY RISKS AND HOW UP PROTECTS YOUR PERSONAL DATA

The processing by UP of your personal data in order to carry out its contractual obligations to you and to exercise its academic freedom carries risks that may involve the confidentiality, integrity, and availability of personal data or the risk that processing will violate the privacy principles and rights of data subjects. UP has put in place reasonable physical (e.g. access control measures such as locks, security personnel, etc.) organizational (e.g. only authorised personnel who have signed the required non-disclosure undertaking and need such personal data to perform their functions are allowed to process such personal data, periodic privacy impact assessments etc.) and technical measures (e.g. use of CDN, encryption, multi factor authentication for UP mail and portals, the conduct of vulnerability and penetration testing and other similar measures) to prevent or mitigate such risks. Kindly note that these measures do not guarantee absolute protection against such risks as when systems are subject to targeted cyberattacks, malware, ransomware, computer viruses, etc. However, UP has

also adopted measures in order to deal with security incidents or personal data breaches in compliance with the DPA and National Privacy Commission (NPC) issuances. See the Board of Regents approved UP Data Privacy Manual https://privacy.up.edu.ph/instructions-and-guides/CERTIFIED%20TRUE%20COPY_DATA%20PRIVACY%20MANUAL%202023%20EDITION.pdf which includes security incident and breach response procedures (Part 7, page) and the following forms:

Form 1 Security Incident or Data Breach Report Form

<https://privacy.up.edu.ph/downloadable-forms/UNIVERSITY%20OF%20THE%20PHILIPPINES%20SYSTEM%20ADMINISTRATION%20INCIDENT%20OR%20BREACH%20REPORT%20FORM.docx.pdf>;

Form 2 Preliminary Assessment Form

<https://privacy.up.edu.ph/downloadable-forms/PRELIMINARY%20ASSESSMENT%20FORM%20FOR%20SECURITY%20INCIDENTS%20OR%20PERSONAL%20DATA%20BREACHES.pdf>;

Form 3 Mandatory Personal Data Breach Notification to the National Privacy Commission

<https://privacy.up.edu.ph/downloadable-forms/Mandatory%20Notification%20to%20NPC.pdf>

Form 4 Mandatory Personal Data Breach Notification for Data Subjects

<https://privacy.up.edu.ph/downloadable-forms/Mandatory%20Personal%20Data%20Breach%20Notification%20for%20Data%20Subjects.docx.pdf>

Form 5 Security Incident or Personal Data Breach Report Form

<https://privacy.up.edu.ph/downloadable-forms/SECURITY%20INCIDENT%20OR%20PERSONAL%20DATA%20BREACH%20REPORT.pdf>

We remind you in our various portals and privacy notices to keep your personal data secure by double checking that the email account you will be using or are using for UP portals has not been compromised by using [Have I Been Pwned](#), using a strong password for such account

<https://itdc.up.edu.ph/about/advisories/2023%2012%2004%20REMINDER%20-%20Use%20Strong%20Passwords%20for%20UP%20Mail%20Accounts.pdf>, when possible activating two factor authentication for your personal email accounts if you have yet to be issued a UP email account, using your UP email account for UP portals and communications with UP as required by UP memos [\[MEMO TJH 2021-10\] Reminder](#)

that faculty and students must use UP Mail for official correspondence and data privacy and security measures required for sending attachments and sharing G.pdf not using public, unsecured networks for submitting personal data or at least using VPN if use of such unsecured networks is unavoidable and keeping all UP account credentials, including your student number, confidential.

ACCESS TO AND CORRECTION OF YOUR PERSONAL DATA AND YOUR RIGHTS UNDER THE DPA

You have the right to access personal data being processed by UP about you. You may access your personal data, for instance, through UP's information systems such as the system you use for enrollment, your online classes, for applying for financial and other assistance [SLAS Online \(up.edu.ph\)](http://SLAS Online (up.edu.ph)) or request documents from relevant offices (e.g. the University Registrar or your College Secretary). In order for UP to see to it that your personal data are disclosed only to you, these offices will require the presentation of your UP ID or other documents that will enable UP to verify your identity. In case you process or request documents through a representative, in order to protect your privacy, UP requires you to provide a letter of authorization specifying the purpose for the request of documents or the processing of information, and your UP ID or other valid government-issued ID (GIID), as well as the valid GIID of your representative.

As mentioned above, UP requires you to provide correct information. In the event that your information needs to be updated please follow the instructions found in the relevant portal or website, or kindly get in touch with the proper University office(s). Please note that the correction of grades is subject to University rules and procedures. Aside from the right to access and correct your personal data, you have the following rights subject to the conditions and limitations provided under the DPA and other applicable laws and regulations:

1. The right to be informed about the processing of your personal data through this and other applicable privacy notices.
2. The right to object to the processing of your personal data, to suspend, withdraw or order the blocking, removal or destruction thereof from our filing system. Kindly note however that, as mentioned above, there are various instances when the processing of personal data you have provided is necessary for us to comply with UP's mandate, statutory and regulatory requirements, or is processed using a lawful basis other than consent. In the case of your UP ID it is your duty to immediately report the loss of such card to your University Registrar and the UP ITDC so that UP can prevent the unauthorized use of the same.
3. The right to receive, pursuant to a valid decision, damages due to the inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of

personal data, taking into account any violation of your rights and freedoms as a data subject and

4. The right to lodge a complaint before the National Privacy Commission provided that you first exhaust administrative remedies by filing a request with the proper offices or a complaint with the proper DPO through the email address indicated below regarding the processing of your information, or the handling of your requests for access, correction, blocking of the processing of your personal data and the like.

HOW WE OBTAIN YOUR CONSENT AND HOW YOU CAN WITHDRAW CONSENT

When consent is UPs lawful basis for processing under 12 a and or 13 a of the DPA, UP will obtain your consent by asking you to execute the proper online e.g. [SLAS Online \(up.edu.ph\)](https://slas.up.edu.ph) or paper based form. If you are below eighteen years of age, we will require your parent or guardian to execute or sign and submit the proper consent form or withdrawal of consent letter. If you wish to withdraw consent, kindly write or send an email to the proper UP office and identify the processing activity for which you are withdrawing consent. Please attach a copy of your UP ID so that the proper UP office will be able to verify your identity. Note that consent may be withdrawn only for a processing activity/ies for which consent is the only applicable lawful ground for such processing. Kindly await such UP office's action regarding your request. Rest assured that once such office confirms that you have validly withdrawn consent for a processing activity/ies the same shall be effective.

REVISIONS TO THE PRIVACY NOTICE AND QUERIES REGARDING DATA PRIVACY

The previous privacy notices issued for the 1st and 2nd semesters/trimester 2018-19 and the notice issued on 27 August 2019 have been revised. This amended notice will be effective for starting the 1st semester 2024-2025.

We encourage you to visit this site [UP PRIVACY POLICIES - HOMEPAGE](#) and your campus website from time to time to see any further updates regarding this and other privacy notices that may apply to you. Changes to UP privacy notices can be seen through this site.

If you have any Data Privacy queries or concerns as it relates to your student records, you may contact your CU's UP Data Protection Officer through the following:

1. Via post
2. Through the following landlines
3. Through email

Post: Lower Ground Floor, PHIVOLCS Building.
C.P. Garcia Avenue
Diliman, Quezon City 1101
Landline: 8255-3561
Email: dpo.updiliman@up.edu.ph

UP Los Baños

Post: Office of the University Registrar, G/F CAS Annex I Building, UP Los Baños,
College 4031, Laguna, Philippines
Landlines: (049) 536-2553 / (049) 536-2426
Email: dpo.uplb@up.edu.ph

UP Manila

Post: 3/F Information Technology Center, Joaquin Gonzales Compound,
University of the Philippines Manila, Padre Faura St., Ermita, Manila
Landline: +63 (2) 509-1003; (PGH) 554-8400
Email: dpo.upmanila@up.edu.ph

UP Visayas

Post: c/o Office of the University Registrar, New Administration Building,
University of the Philippines Visayas, 5023 Miag-ao, Iloilo
Landline: (033) 315-9631 or 315-9632 and local numbers 191-192
Email: dpo.upvisayas@up.edu.ph

UP Open University

Post: 2/F UP Open University Main Building
UP Open University Los Banos 4031 Laguna
Landlines: (049) 536-6001 to 006 local 299
Email: dpo.upou@up.edu.ph

UP Mindanao

Post: c/o Office of the Chancellor
University of the Philippines Mindanao
Barangay Mintal, Davao City 8022

Landline: (082) 293-0310

Email: dataprotection.upmindanao@up.edu.ph

UP Baguio

Post: Office of the University Registrar, UP Baguio, Gov. Pack Road, Baguio City
2600

Landline: +63 (74) 442-5592

Email: dpo.upbaguio@up.edu.ph

UP Cebu

Post: Room 242, Arts and Science building, UP Cebu Lahug Campus

Landline: +63 (32) 233-8203 loc 202

Email: dpo.upcebu@up.edu.ph

For queries, comments or suggestions regarding this System-wide privacy notice, please contact the University of the Philippines System Data Protection Officer through the following:

1. Via post
c/o the Office of the President 2F North Wing Quezon Hall (Admin Building)
University Avenue, UP Diliman, Quezon City 1101 Philippines
2. Through the following landlines
(632)89280110
(632)89818500 loc. 2521
3. Through email
dpo@up.edu.ph