PRIMER
on Data Protection and Online Learning

Ateneo de Manila University

UNIVERSITY DATA PROTECTION OFFICE
Ateneo de Manila University

The University Data Protection Office (UDPO) is a unit under the Office of the President responsible for ensuring the compliance by the Ateneo de Manila University —including its various offices and personnel—with all applicable privacy and data protection laws and policies.

2021

Published by the University Data Protection Office

Rm 200 Manila Observatory, Katipunan Avenue
Loyola Heights, Quezon City
Philippines 1108
T. +632 84266001 loc. 4801
E. info.udpo@ateneo.edu

Contributors:
Jamael Jacob, Sharifah Aine Datu Tambuyung, Roszano Ayson, Karl John Baquiran, Lianne Bacorro, and Kathleen Grace Benavidez

Contents

Background

This Primer is meant to help Ateneo de Manila University personnel manage and conduct online learning in a manner consistent with applicable privacy and data protection laws, including the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations, and other issuances of the National Privacy Commission (NPC).

It shares practical tips and best practices that enable the safe and secure use of products, tools, and programs ("tools") for online learning, by building on existing guidelines provided by various stakeholders like regulators, other government agencies, and the Data Privacy Council for the Education Sector.

This document, however, is not an exhaustive guide and only covers popular resources the average user is expected to be familiar with. Neither is it intended to be a user manual for any of the tools it features. As newer and more advanced technologies become available, this document may have to be revised or updated.

If you are unfamiliar with some of the terms used in this Primer, kindly refer to the Glossary for guidance.

General Matters

Key Concepts and Principles

If you consider processing personal data necessary or important to online learning, make sure you observe the following important points:

Accountability

The University is accountable for all personal data it collects and processes. This obligation remains even if:

1. it lets others perform the processing for or on its behalf (i.e., when it engages in outsourcing or subcontracting).
2. it has properly obtained the consent of its students (or their parent or legal guardian, in the case of minors).

For this reason, endorsing or recommending specific tools or devices to students or fellow personnel should be exercised responsibly.

Information about Education as Sensitive Personal Information

Any information about education is considered sensitive personal information. Processing it is generally prohibited. It may only be allowed in specific instances (see: Section 13, DPA):

1. when the data subject has given consent;
2. when the processing is provided by law or regulations that afford adequate data protection;
3. when processing is necessary to protect the life or health of the data subject or another person, and the data subject is unable to give consent;
4. when processing is necessary for purposes of medical treatment. However, such treatment must be performed by a medical practitioner or a medical institution, and an adequate level of data protection is ensured;
5. when processing involves information necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings;
6. when processing involves information necessary for the establishment, exercise, or defense of legal claims; or
7. when the information is to be provided to government or a public authority, in line with the latter's constitutional or statutory mandate.

Legitimate Purpose

The processing of personal data must have a declared and specified purpose that is not contrary to law, morals, or public policy (*see*: Section 11.a, DPA). The data subject must be aware or properly informed of such purpose.

Proportionality

The processing of personal data must be adequate, relevant, suitable, necessary, and not excessive in relation to its purpose. It shall only be carried out if its purpose cannot be reasonably fulfilled via another, less intrusive method (*see*: Section 11.d, DPA). Only those information necessary to achieve the declared purpose should be processed. And they should only be kept while such purpose remains unfulfilled—unless there is some other legal basis that justifies a longer retention period.

Legitimate Interest

To make sure the University's legitimate interest is an appropriate basis for a particular data processing activity, a three-part test must be performed. Each part requires answering a particular question:

1. Purpose Test – Does the processing have a legitimate purpose?
2. Necessity Test – Is the processing necessary to achieve such purpose, which means there is no less intrusive way to achieve it?
3. Balancing Test – Is the University's legitimate interest *not* overridden by the data subject's rights and freedoms?

To pass the test, the answer to each question must be in the affirmative.

For additional guidance, refer to the following: (i) NPC Advisory Opinion No. 2018-020; (ii) NPC Advisory Opinion No. 2018-050; (iii) NPC Advisory Opinion No. 2020-006.

Transparency

Apart from purpose, data subjects must also be aware of the nature and extent of the processing of their personal data, including the risks and safeguards involved, the identity of the Personal Information Controller (PIC), their rights as data subjects, and how these rights can be exercised. Any material or communication meant to relay these details must be accessible and easy to understand. Towards this end, the use of a Privacy Notice (also referred to as Privacy Policy) helps a lot.

For additional guidance on Privacy Notices, kindly refer to UDPO Advisory 18-03.
Existing privacy notices of the University found at the UDPO website may be used as reference.

Basic Security Protocols

In an online learning environment, your familiarity with basic security protocols goes a long way towards protecting personal data and the computer devices and equipment you keep them in. It helps minimize the risk of possible data breaches and other types of security incidents.

Choice of Platform

Your choice of application ("app") or platform could make the difference between a safe, enjoyable online learning experience and a horrible one. So make sure you study your options carefully. Read Privacy Notices and Terms and Conditions, and compare. Identify which one actually meets your needs. Watch out for questionable data processing activities. Check news articles and reviews for potential or actual security risks involving the tools you are considering. If in doubt, consult the appropriate Support Office (see: p. 28).

Licensed Software

It is often unavoidable that licensed software will be used for online learning. Subscriptions or purchases may be necessary. The use of bootleg, "cracked", or pirated versions should be avoided. The University prohibits the installation of unlicensed software in University-owned computer devices and the use of unlicensed software in the performance of official University functions. Not only is it illegal, it also increases the chances of you experiencing program malfunction or failure, and getting your device infected with malware. You are also unable to obtain valid updates or upgrades from the developer, or enjoy warranty against product defects.

Unique IDs

Users of University information technology (IT) resources are given unique credentials that must be used only for study or work in the University. If those unaffiliated with the University wish to access or use such resources, they may request for guest accounts, subject to the approval of the University. Access requests should be sent to the Information Technology Resource Management Office (ITRMO) or, in the case of specific systems or platforms, the unit or office that manages them.

Strong passwords

When asked to create passwords, always use strong ones. Better yet, use passphrases instead. If possible, use a combination of alphanumeric and special characters (EXAMPLE: Th1s1s@p@ssphr@s3). Make it a habit to change them regularly, too. If you can afford to purchase or subscribe to password manager services, do so.

Encryption

Those familiar with the technology should use encryption to secure data both while sending it out and while keeping it in storage. This is ideal for those handling classified or sensitive personal information. There are many programs out there that can be used for this purpose. OpenPGP, for instance, can be used to encrypt emails, while programs like FileVault can be used to encrypt information on Mac computers.

Access restrictions

In relation to specific systems or offices, it is ideal to have a written policy that helps manage who gets to have access to the stored information. Apart from enhancing security, it also fosters accountability.

Regular Updates

Make it a habit to update your computer device's operating system and the applications running on it. Check regularly if you have the latest versions of your software. Updates introduce new features and address known vulnerabilities.

Backup

Back up your data often. If you can afford to, always maintain multiple copies and keep them in separate locations. Of course, such locations must, in themselves, also be safe and secure.

Data storage and disposal

Personal data should always be stored and disposed of in a safe and secure manner. This may mean:

1. storing them only in University-owned devices and/or systems
2. developing a Record Management Policy that contains the retention schedule and disposal procedure for specific categories of personal data. It should be consistent with any retention periods prescribed by existing laws, government regulations, or University policies.
3. when deleting or disposing of records, making sure the data they contain becomes irretrievable or inaccessible after such process.

Incident management

Report any actual or suspected data breach or security incident to the University Data Protection Office (UDPO). You could be committing a crime if you conceal or fail to report certain types of data breaches. For more information about the reporting process, refer to the University's Security Incident Management Policy.

Capacity building

The University, through its various units, often organizes instructional workshops and produces information materials that deal with security in online spaces. The ITRMO, for instance, has a specific web portal dedicated to various security reminders. Make an effort to attend such activities and go over said materials.

Key Areas of Concern

Emails

In today's modern society, emails account for a large chunk of the communication that goes on between individuals and organizations. They include those exchanged between University personnel and students, as well as between their respective peers.

- Use your official email account (i.e., @ateneo.edu) for school-related communications.
- Avoid or at least minimize the use of your official email account in your personal or household affairs (e.g., signing up for a raffle, opening an account in a social media platform, etc.).
- Be careful when opening or receiving emails, especially from unknown or unfamiliar sources.
- Do not draft emails while distracted. Many data breaches are caused by individuals performing two or more tasks simultaneously. They end up sending unfinished messages, attaching wrong files, or indicating the wrong recipients.
- Avoid discussing confidential or sensitive personal information via email threads. Keep any discussion regarding personal data to a minimum.
- When preparing an email, draft your subject line properly. If possible, refrain from including personal details (e.g., "re: exam results of Juan dela Cruz").
- If attaching a file to an email, make sure you have the correct one. Check if all pages of an attached document actually need to be shared. One or more items in the document may have to be redacted, covered, or removed.

- Whenever appropriate, make sure your attachment is password-protected. This is ideal for files containing confidential or sensitive personal information.

- Add the email address of your recipient last. This helps avoid sending an incomplete or unfinished email.

- Use the CC and BCC features responsibly and sparingly. Unless all recipients of a single email belong to the same group and have similar access privileges, use the BCC feature, instead of the CC one. The BCC function gets the job done without unnecessarily disclosing the identities of the other recipients and their respective email addresses.

- When sending out education-related information (e.g., grades, feedback, assessment, etc.) about specific students, do so on an individual basis, preferably through an encrypted or at least password-protected file.

- Check carefully if you are sending your message to the correct or intended recipient. Make sure there are no typographical or spelling errors. Be extra careful if the email platform has an auto-complete feature, since a common name could lead to two or more different email addresses.

- When replying to an email that has multiple recipients, use the “Reply all” function properly. Ask yourself the following questions: Do all of the recipients need to be informed of my response? Would replying to the sender alone suffice? If not, would removing certain people as recipients be appropriate?

- When an email is sent to you by mistake, inform the sender as soon as possible and delete it permanently. If personal data under the control or custody of the University was unnecessarily disclosed, report the incident to the UDPO.

For a more extensive discussion of these points, kindly refer to UDPO Advisory 18-01.

Video Conferencing Platforms

Video conferencing platforms are essentially software that lets people conduct face-to-face meetings without having to meet in person. They are particularly useful for classes or events where the participants are situated in different, remote locations.

- When you will be recording an online class or event, inform everyone before commencing. A short Privacy Notice may be displayed prior to recording. An advance copy of the document may be included in the schedule or invitation you send out. You can also verbally relay the information that would otherwise be featured in a Privacy Notice.

  If you wish to adopt the best practice of obtaining the prior consent of the students or participants, note that consent must be in a written, recorded, or electronic format. Fortunately, some platforms already have built-in consent mechanisms. To avoid delay, it may be ideal to secure consent well in advance.

- If you want all students or participants to have their webcams turned on for the duration of a class or event or, at least, during specified times, establish a clear webcam policy governing the use of such devices. The purpose for the use of the webcam should be clearly identified and ought to take into account not only the University's legitimate interests, but also individual privacy rights.

  The policy may also consider: (1) the optional use of webcams; (3) the occasional use of webcams, such as during attendance checks, graded oral recitations, or any time the participant is speaking; and/or (2) the use of backgrounds and filters.

- Make use of PINs or passcodes to protect online sessions against uninvited guests. Most video conferencing platforms have these features.

- To avoid interference or disruptions caused by intruders or uninvited guests, exercise care when sharing the link (and other meeting credentials or details) to an online class or event. Unless the class or event is open to everyone, such information should be kept private. The use of a registration form through which all relevant information can be shared is a good option.

- Set appropriate meeting room configurations, such as:

    1. Only authenticated attendees are allowed to join.
    2. The request of each attendee to join is evaluated individually. Attendees are unable to join if the host has not yet logged in.
    3. A waiting room is enabled.
    4. A standard naming format (i.e., how each attendee should identify himself or herself) is provided. Attendees may be prohibited from renaming themselves once a meeting has started.
    5. Meetings always begin with the participants' webcams and/or microphones automatically turned off. Depending on the nature of the meeting, this may be maintained for the entire duration of the class or event.
    6. A password is required prior to entry.
    7. Desktop or screen sharing is disabled, except for those who are expected to speak, present, or report. Access to other meeting room features such as chat, private messages, file transfer, in-app recording, and annotation tools may also be restricted.
    8. Use of wireless earphones or microphones (e.g., via Bluetooth connection) is discouraged, especially for assigned speakers. They tend to have more connection issues compared to their wired counterparts.

- By default, students or participants should not be allowed to record (and then share) an online class or event without the approval of the University and other affected data subjects.

  While this rule is nearly impossible to enforce real-time given the range of recording tools available to attendees, it is still worth establishing before a class or event begins. Everyone should be aware that its violation may be considered an infraction (as per University policy), a crime, or an appropriate basis for a legal claim by an aggrieved individual.

Chat or Messaging Apps

Relaying school-related communications online should be carried out through official channels (e.g., email). This makes the use of chat or messaging apps not ideal, unless all the parties are using verified accounts. However, if resorting to such programs cannot be avoided, some points are worth considering.

- Always verify the identity of the individual you are communicating with via other channels (e.g., email, phone call, etc.).

- If you can, limit communications to urgent concerns or at least those that do not involve confidential or sensitive personal information. You should also avoid sending (or asking the other party to send) any information that may be used to commit identity fraud (e.g., scanned copy of IDs, log-in credentials, etc.).

- Familiarize yourself with the privacy and security settings of the app. Enable encryption and other available security features. Some programs allow messages to be deleted automatically after a certain period of time. If that function is unavailable, manually dispose of any shared personal data on a regular basis.

- When creating (or joining) a group chat:
    1. Make sure all members actually need to be part of the group, or are at least qualified to be one. Remove those who do not meet such criteria. If you are not the creator or owner of the group, have them remove said individual.
    2. Seek permission before adding a person to a group. If an “invite” function is available, invite people to join instead.
    3. Set and enforce appropriate rules. Make sure all members are familiar with them.
    4. Delete groups that are no longer in use.

- Provide alternative communication channels. Some students (and parents) may not have access to chat or messaging apps or prefer not to use the same.

Social Media Apps and Platforms

Social media is, by default, a public space. The medium is inherently meant for sharing materials—if not to the public, at least to certain groups of people. Even uploaded materials you choose to be visible only to you are still accessible to the developers of the app or platform. Keep this in mind when considering this medium for online learning purposes.

- Limit the use of social media to the posting of materials or communications that are not deemed confidential or sensitive personal information, or any information that may be used, under certain circumstances, to commit identity fraud. Urgent or general announcements, notices, or statements are ordinarily safe for publication.

- Familiarize yourself with the privacy and security settings of the app or platform. Enable security features like two-factor authentication and account recovery options.

- Be aware of the rules that govern the use of the app or platform. Unlawful disclosure of personal data and other types of unwarranted privacy intrusions are often legitimate grounds for the suspension or deletion of social media accounts.

- When creating (or joining) a group:

    1. Some platforms allow groups to remain private. They are visible only to members and those invited to become members. Use this feature to enhance the security and privacy of the group.
    2. Make sure all members actually need to be part of the group, or are at least qualified to be one. Remove those who does not meet such criteria. If you are not the creator or owner of the group, have him or her remove said individual.
    3. Set and enforce appropriate rules. Make sure all members are familiar with them.
    4. Delete groups that are no longer in use.

- When creating an account for or on behalf of a particular unit or office of the University, coordinate with the University Marketing and Communications Office (UMCO). It needs to be aware of all instances a person or office presents itself as an authorized representative of the University.

- Provide alternative communication channels. Some students (and parents) may not have a social media account or prefer not to create one.

For additional guidance, kindly refer to the University's Social Media Guide and NPC Advisory Opinion 2020-046.

Learning Management Systems

Learning management systems (LMS) are designed for online training programs and information sharing. They have many useful features such as the recording of learning sessions and the creation of training progress reports. Common LMS include Canvas, Moodle, and Google Classroom.

- Use LMS authorized and officially recognized by the University. They have been vetted by the concerned offices and are expected to have the minimum safeguards necessary to protect users and their personal data. Guidelines on the proper use of these systems and platforms are often given during orientations provided by ITRMO.

- All users, whether they be teachers or students, should be familiar with the security features that come with an LMS. Those features should be enabled at all times. For instance, if an LMS permits 2-factor authentication, turn it on as an additional layer of protection. Administrators should assign user permissions carefully.

- Exercise caution when integrating third-party applications, supporting tools, and other services with an LMS. They may have vulnerabilities that could compromise the system itself and the information it contains.

- When making public announcements via an LMS make sure no confidential or sensitive personal information—like grades or test results—are involved. Those kinds of information must only be communicated to their intended recipients.

- Unless their assignments, projects, or submissions are inherently public by nature, students should be instructed to submit their outputs directly to their teacher. If the LMS does not allow this, the students should use their University-issued email accounts instead.

Registration Forms

You may occasionally find the need to organize or host activities that involve a registration system. When you do so, you collect personal data through registration forms, sign-up sheets, attendance logs, and other similar documents ("registration forms"). You then use the collected information to identify participants, relay important event-related communication, and other compatible purposes.

- It should be clear to you why you need to use a registration system. The purpose/s of your data collection will determine the type and amount of personal data you need to gather from attendees or participants.

- Before using a registration system, including any online registration form or platform, a risk assessment is highly recommended. This is particularly true if you, as organizer: (a) are unfamiliar with the system or platform you intend to use; (b) have previously encountered issues while using said system or platform; or (c) will be securing the services of a third party in managing the registration system.

  Consultation with the ITRMO is recommended for any technology-related inquiries or clarifications. If your unit has its own IT office or personnel, refer your inquiries or concerns through them.

- During registration proper, remember the following:

  Limited access to registration data. The names and other personal details of attendees or participants should not be visible or accessible to unauthorized personnel, including other attendees or participants. See to this when adjusting the settings of the online registration platform.

Transparency and consent. The registration system should be covered by an appropriate Privacy Notice that is visible or at least accessible to attendees or participants before they provide their personal data. If consent of the attendee or participant is necessary, the organizer should ensure that it has obtained the same prior to the collection of personal data. Learn more about the preparation of consent forms by reading UDPO Advisory 18-05.

Third-Party platforms. If you intend to use an online registration platform, read its Privacy Notice and its Terms and Conditions. Find out how it will be processing the personal data of attendees or participants. Pay close attention to its data sharing and data retention practices, if these are indicated in the documents. For optimal assistance from the University, use platforms currently supported by the ITRMO (i.e., Google- or Microsoft Office 365-based systems).

Registration via email. When processing registration via email, especially when sensitive personal information are involved, the use of encryption should be explored, as regular emails may be incapable of providing adequate security.

Just-in-time notices. If a mobile app will be used as an online registration platform, those that provide just-in-time notices are preferred.

Security features. In order to enhance the security of the registration system, appropriate technical measures may be implemented, such as SSL Certificates, QR Codes, Captcha, field validation, or other similar measures. A higher level of security is necessary when confidential or sensitive personal information will be collected or when registration will involve payment or the collection of fees.

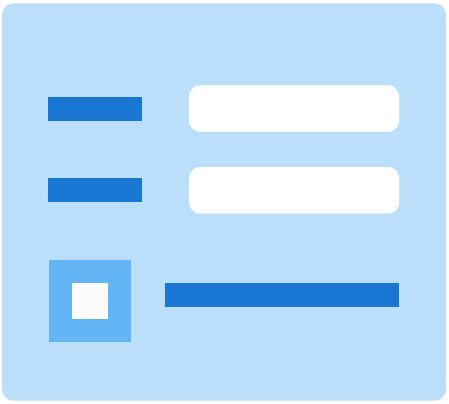
Pre-launch inspection or dry run. Before launching your registration system, perform a dry run to ensure that all security features are functioning properly. Document all technical tests that you carry out.

Payments. If the registration system involves payment or the collection of fees, it must adhere to all applicable regulations and standards, such as the Payment Card Industry Data Security Standards (PCI DSS). There must be substantial coordination with the Bursar (under the Office of the Vice President for Finance and Treasurer) and the ITRMO in order to obtain the necessary approvals and to ensure seamless integration with existing online payment systems of the University.

- If the collected personal data will be shared, disclosed, or transferred to third parties:

    1. the data sharing must be justified by at least one of the criteria listed in Item No. 2 under “Key Concepts and Principles”;
    2. the data sharing must be featured in the Privacy Notice that applies to the event or activity;
    3. the organizer must enter into a Data Sharing Agreement (DSA) with the third party, unless there is sufficient justification for its non-use; and
    4. the DSA must contain the provisions featured in Section 9, of NPC Circular 2020-03.

  This also applies to events or activities where third parties are involved as co-organizers.



Online Surveys or Polls

You may also have to send out short online survey forms or questionnaires to other University personnel and students (or their parents) in order to obtain valuable information or insights in relation to a class, event, or some other facet of online learning.

- Communicate properly the nature of your survey and state your objective/s in plain and clear terms. Respondents should be able to understand why and how you intend to conduct it. The propriety of the questions and the information you will collect will be evaluated against your objective/s. Also, if the survey or part of it is optional, this should be clearly indicated.

- Keep in mind that the survey or poll must be related to your work or your office's. If it is meant to further you personal interests (e.g., in relation to your business or study), you must first secure authorization from your office or unit. Coordination with the UMCO is also necessary if you want to disseminate the survey via the University's official communication channels.

- Assess if you can successfully conduct the survey using only anonymized data. If you can, you should pursue that route.

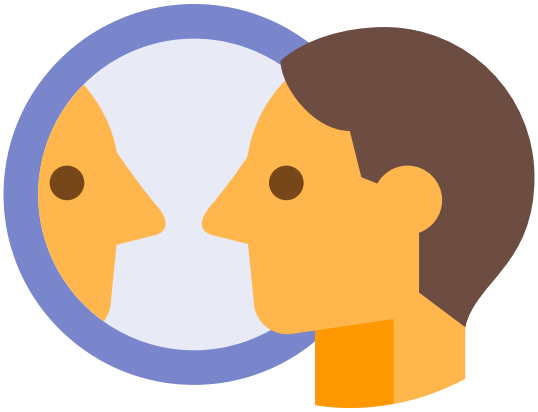
- Refer to the appropriate Privacy Notice of the University that applies to your survey. If none of the existing policies fully captures the parameters of your survey, craft a separate one.

  There may be instances when you need to obtain the express consent of the respondents. This is usually the case when you opt to collect sensitive personal information. Remember that a consent form is different from a privacy notice.

- If you will send out survey forms (or a link thereto), make sure to use the BCC function in order to avoid disclosing the email addresses of other would-be respondents. Directing it to a mailing list is acceptable if all its members are potential respondents.

  If you will commission a third party to conduct the survey, make sure it is covered by an appropriate Data Processing Outsourcing Agreement (DPOA). Consult the UDPO regarding this matter.

For additional guidance, kindly refer to NPC Advisory Opinion No. 2019-018.



Online Proctoring

Online or remote proctoring is the supervision of examinations in an online setup with the use of technologies or tools. It allows students to take their exams in a remote location while maintaining the integrity of the test, by preventing cheating or any irregular student behavior. The technologies used for this purpose usually allow the teacher or proctor to monitor the examinee's computer device, including its webcam and microphone.

- The University does not mandate or prescribe the use of proctoring software, let alone a specific brand or product. You should consult your department or unit if you consider its use necessary for your class. Coordination with the ITRMO is also important.

- Online proctoring may entail any or all of the following:

    1. installation of the proctoring software in the examinees' computer
    2. verification of the examinee's identity through the collection of their personal data
    3. access to the screen or monitor of the examinees
    4. scanning of the examinees' computer for other programs or software that may be running, and for other monitors connected to the computer;
    5. scanning (via webcam) of the desk and room where examinees will be taking the exam
    6. monitoring and recording of the exam, using the examinees' computer
    7. implementation of automated processing techniques

- Proctoring software may differ in their features and capabilities. This may result in the collection and use of different types and amounts of personal data. Familiarize yourself with the features of the software you will be using. Make sure you only collect those information necessary to facilitate an honest and orderly online exam. Unless there exists sufficient justification, extra or additional features should be turned off.

- Recorded or collected data should be treated as confidential, by default. Using and sharing them should be limited only to the declared purpose/s, as relayed to the student prior to the exam.

- Since online proctoring is still new to most students and parents, be prepared to explain to them how it works, including the software that will be used. If necessary, walk them through the entire process. Communicate any attendant risks and suggest possible ways to address them. A Frequently-Asked-Questions document would be useful for this purpose.

Other Tools for Online Learning

The requirements of a particular course or class usually determine if you will need additional tools. This explains why it is typically the teachers who are expected to make the appropriate decision on this matter, after they perform an adequate assessment of the situation.

- If you believe that your class requires additional digital tools, raise the matter to your department or unit, and the ITRMO, as soon as possible. If there are data protection, intellectual property, or general legal concerns, the UDPO, the Ateneo Intellectual Property Office (AIPO), and the University Legal and Compliance Office (ULCO) may be consulted, in that order.

- If the tool is available locally or the developer/vendor has an authorized local agent, the purchase of or subscription to said tool should be covered by a written contract that affords adequate protection to any personal data that may be processed while the tool is in operation. The UDPO has available contract templates ready for use. If the developer/vendor has its own template and prefers to use the same, refer the document to UDPO, AIPO, and/or ULCO for review, as necessary. Technical matters, like compatibility issues, should be promptly referred to the ITRMO.

Support

When addressing the challenges posed by online learning, University personnel may consult or seek the assistance of the following offices:

University Data Protection Office
info.udpo@ateneo.edu (queries)
alert.udpo@ateneo.edu (security incidents)

Information Technology Resource Management Office
itrmo@ateneo.edu

University Legal and Compliance Office
legal@ateneo.edu

University Marketing and Communications Office
umco@ateneo.edu

Ateneo Intellectual Property Office
aipo@ateneo.edu

Glossary

When used in this Primer, the following terms shall have their corresponding meanings as provided below:

- “Chat or messaging app” refers to any online platform that enables instant messaging, either as a standalone direct messaging app or an adjunct of a separate platform or program. Examples include Facebook Messenger, Google Hangouts, Signal, Telegram, Viber, WhatsApp, and Wire.

- “Consent” refers to any freely given, specific, informed indication of will, whereby a person agrees to the collection and processing of his or her personal data. It must be evidenced by written, electronic or recorded means. It may be given by a lawful or authorized representative.

- “Data Processing Outsourcing Agreement” refers to a contract governing an engagement or transaction between a Personal Information Controller and a Personal Information Processor. It affords protection to any or all personal data that is processed in relation to such contract.

- “Data Sharing” refers the sharing, transfer, or disclosure to a third party of personal data under the custody of the University, as a personal information controller. “Third party” does not include service providers of the school.

- “Data Sharing Agreement” refers to a contract governing a data sharing arrangement between two or more Personal Information Controllers. It affords protection to any or all personal data that are processed in relation to such contract.

- “Data Subject” refers to an individual whose personal data is processed.

- “Encryption” refers to the process of scrambling or transforming data into a code, such that it can only be read by a person who has the so-called decryption key.

- “Just-in-time notices” refers to relevant and focused privacy-related information that pop up when a user interacts with a particular data field. They help explain what information must be provided in the said field, including the purpose of its collection.

- “Learning Management System (LMS)” refers to a software application for the administration, documentation, tracking, reporting, automation and delivery of educational courses, training programs, or learning and development programs.

- “Personal Data” is the collective term used when referring to personal information, sensitive personal information, and to the extent applicable, privileged information.

- “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.

- “Personal Information Controller” refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes: (a) a person or organization who performs such functions as instructed by another person or organization; and (b) an individual who collects, holds, processes or uses personal data in connection with his or her personal, family or household affairs.

- “Personal Information Processor” refers to any a person or organization to whom a personal information controller outsources the processing of personal data.

- “Privileged Information” refers to information considered by the Rules of Court and other laws as privileged communication.

- “Processing” refers to any operation performed on personal data including, but not limited to, collection, storage, updating, retrieval, use, consolidation, blocking, or destruction of data.

- “Public authority” refer to any government entity with law enforcement or regulatory authority or function, as vested by law or the Constitution.

- “Sensitive Personal Information” refers to personal information:

    1. about an individual, race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
    2. about an individual, health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
    3. issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
    4. specifically established by an executive order or an act of Congress to be kept classified.

- “Social Media Account” refers to an individual’s personalized access to a social media platform, typically using a username and password combination. It allows its owner to interact with other account owners on the same social media platform.

- “Social Media Apps and Platforms” refers to networking sites or applications that enable their users to create and share content and information to and promote discussion among all of an individual account owner’s contacts or to/among the public in general. They then allow users to participate in social networking. It includes, but is not limited to, Facebook, Instagram, YouTube, Twitter, LinkedIn, and other similar platforms.

- “University information technology (IT) resources” refers to computers, hardware, software, subscriptions, services, networks, databases, files, electronic files, personal data and other information, software licenses, network bandwidth, username, passwords, documentation, electronic communication, computer laboratories and similar technologies that are owned, managed, or maintained by any office or unit of the University.

University Data Protection Office
ATENEO DE MANILA UNIVERSITY