APPENDIX 1
Answer Guide

IMPORTANT: Please accomplish and submit one DPS form for **each** data processing system your office uses. Use this file name format – **DPS REGFORM [office] [DPS name]**. There's no need to include these appendices in your submissions.

Now, for the explanation and guide questions for the items/fields in the DPS form.

1. **Name of DPS:** *What process or system does your office use to handle personal data?*

   A "Data Processing System" or "DPS" refers to any process or procedure by which personal data is collected, used, or otherwise processed in an information and communications system, or at least a filing system. It involves the entire lifecycle of personal data within a computer or filing system—from collection or generation, to storage, transfer or disclosure, retention, and disposal.

   EXAMPLES: HR Hiring process, ASMPH student enrollment, LS student admission, AGS grading system

2. **Processing as:** *Is the University, through your office, processing personal data as a Personal Information Controller or as a Service Provider/Personal Information Processor (SP/PIP)?*

   "Personal Information Controller" (PIC) refers to an individual or organization that controls the processing of personal data. It excludes:
   a. a Personal Information Processor (PIP); or
   b. an individual who processes personal data in connection with their personal, family, or household affairs

   "Personal Information Processor" (PIP) refers to an individual, entity, organization, or other entity or body to whom a PIC may outsource or subcontract the processing of personal data. In other words, a PIP processes personal data for or on behalf of the PIC.

   If the University, through your office, is processing personal data for its own purpose, click "Personal Information Controller". If processing is being done on behalf of or under the instructions of another entity/organization, click "Service Provider/Personal Information Processor".

3. **Type of DPS:** *How does your office gather, collect, use, store, or otherwise process personal data?*

   Click "Manual" if personal data is processed through paper-based instruments only.
   Click "Electronic" if personal data is processed only through electronic means such as computers, mobile apps, and online forms.
   Click "Both" if personal data is processed through a combination of manual and electronic means, or through either means.

4. **Is the system, or part of it, outsourced/subcontracted?:** *Is the DPS, or any part of it, managed or provided by a third-party supplier or service provider?* If yes, provide the details required in 4.a.1 – 4.a.3.

   Examples of arrangements considered outsourcing/subcontracting include: engagement of a consultant to maintain the system, use of cloud storage such as Google Drive or Dropbox to store data, and use of a web application software such as Eventbrite for the participant registration.

   4.a.1 **Name of SP/ PIP:** Indicate the service provider's name. If there is more than one, identify at least one and then append "and others", e.g., Google, Inc. and others.

   4.a.2 **Contact No.:** Provide the business contact number of the service provider.

   4.a.3 **Email Add:** Provide the business email address of the service provider.

5. **Personal data processed:** *What personal data do you process through the system?*

5.a. **Personal Information:** "Personal Information" refers to any information, on its own or when taken together with other information, from which an individual's identity is apparent or can be reasonably and directly determined. Personal Information may include data points such as name, email address, sex, and contact details.

5.a.1. **List of Personal Information**: List down the specific personal data points. (e.g., Name, contact details, address, etc.)

5.b. **Sensitive Personal Information**: "Sensitive Personal Information" refers to personal information:

a. about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations;
b. about an individual's health, education (ex. student grades), genetic or sexual life, or to any proceeding for any offense an individual committed or alleged to have been committed (ex. disciplinary/administrative case files), the disposal of such proceedings, or the sentence of any court in such proceedings;
c. issued by government agencies peculiar to an individual (ex. passport number, SSS number, etc.), which includes, but is not limited to, social security numbers, previous or current health records, licenses or their denials, suspension or revocation, and tax returns; and
d. specifically established by an executive order or an act of Congress to be kept classified.

5.b.1. **List of Sensitive Personal Information**: *List down the specific personal data points.* (e.g., Name, birthdate/Age, grades, religion, etc.)

5.c. **When is data collected?:** *Briefly describe the time/moment when data is collected, generated, or received by your office.* (e.g., during registration and upon enrollment)

5.d. **Retention period:** *Briefly describe the period within which you retain the data.* (e.g., within one year from the date of collection, while a contract subsists, etc.)

5.e. **Disposal procedure:** *Briefly describe the method or mode through which you dispose of the data.* (e.g., shredding, incinerating, and sanitizing/wiping the device)

6. **Purpose of processing:** *Why does your office process the personal data?* List down the specific purpose/s for processing the personal data (e.g., for proper documentation and auditing, to process the student's registration for a school activity, to determine if an applicant is qualified to enroll, etc.).

7. **Basis for processing:** *What is your legal basis for processing the personal data collected?*

7.a. **Personal Information:** Refer to Items I. 1-6 of **APPENDIX 2** for possible legal bases for processing personal information. Copy and paste the condition/s that apply to your case.

7.b. **Sensitive Personal Information:** Refer to Items II. 1-7 of **APPENDIX 2** for the possible legal bases for processing sensitive personal information. Copy and paste the condition/s that apply to your case.

8. **Description of the category of the Data Subjects:** *Identify the category/ies of individuals whose personal data you process.* Click all that apply. If the appropriate category is not in the list, click "others" and then identify the category.

9. **Is the data shared with other PIC/s?**: *Does your office share the personal data with individuals, entities, or organizations that are not part of the University, and which process it for their own purpose/s*? Remember, third-party suppliers and service providers are not PICs.

9.a.1. **Name of organization:** If you answered yes, identify the other PIC by name. If there are multiple PICs, identify one and just append "and others".

9.a.2 **with DSA?:** *Is there a contract between the University and the PIC containing specific data privacy provisions that govern the data sharing?* (ex. Data Sharing Agreement, Joint Controllership Agreement, etc.).

10. **Will the personal data be transferred outside the Philippines?:** *Do you share, transfer, or disclose personal data to entities outside the Philippines?* This includes entering into an agreement with third parties, including service providers such as cloud storage providers/developers and web application/portal (e.g., Google Drive, Dropbox), to process the personal data.

11. **Description of Security Measures:** *Do you implement protective measures or security controls (i.e., organizational, physical, and technical) to ensure the safety of the personal data you process?* Examples are listed below. You may choose the ones that are currently implementing.

11.a **Organizational:**

- Privacy Policies: Developing and implementing clear privacy policies that outline how personal data is collected, used, stored, and shared by the organization, providing transparency to individuals.
- Employee Training: Conducting regular data protection and privacy training sessions for employees to raise awareness about data handling best practices, security protocols, and legal requirements.
- Data Retention Policies: Establishing policies and procedures for the retention and disposal of personal data, ensuring that data is stored only for as long as necessary and securely disposed of when no longer needed.
- Third-party Management: Implementing processes to evaluate and select trustworthy service providers who handle personal data responsibly and ensuring appropriate data protection measures are in place in the agreements/contracts.
- Personal Data Inventory: Maintaining an up-to-date inventory of the types of personal data collected, processed, stored, or shared by the office, along with relevant details such as data categories, processing purposes, retention periods, and lawful basis.
- Access Control Policy: Establishing a policy that defines the rules and procedures for granting and revoking access privileges to personal data systems and resources, ensuring that only authorized individuals can access and handle personal data.
- Acceptable Use Policy: Implementing a policy that outlines the acceptable use of organizational systems, networks, and personal data by employees, contractors, and other authorized users, specifying the responsibilities and restrictions to maintain data security and privacy.

11.b **Physical:**

- Access Control Systems: Implementing security measures such as biometric access controls, key cards, or ID-based entry systems to restrict physical access to areas where personal data is stored.
- Video Surveillance: Installing surveillance cameras in data centers, server rooms, and other sensitive areas to monitor physical access and deter unauthorized activities.
- Secure Storage: Storing physical documents containing personal data in locked cabinets, secure rooms, or off-site facilities with restricted access and proper environmental controls (e.g., temperature and humidity).
- Visitor Management: Implementing visitor registration procedures and ID checks to ensure that only authorized individuals have access to areas where personal data is stored.
- Secure Disposal: Employing secure shredding or destruction methods for physical documents or devices that contain personal data to prevent unauthorized retrieval.

11.c **Technical:**

- Encryption: Utilizing strong encryption algorithms and protocols (e.g., AES-256) to protect personal data both in transit (via SSL/TLS) and at rest (stored on servers or databases).
- Firewalls: Deploying firewalls to control network traffic, filter out potential threats, and prevent unauthorized access to systems containing personal data.
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS): Implementing IDS/IPS tools to monitor network traffic for suspicious activities, detect potential breaches, and take proactive measures to prevent them.
- Data Backup and Recovery: Regularly backing up personal data and implementing data recovery mechanisms to ensure data availability and integrity during system failures, natural disasters, or cyberattacks.
- Vulnerability Scanning and Patch Management: Conducting regular vulnerability assessments, scanning systems for known vulnerabilities, and promptly applying security patches and updates to mitigate risks.

12. **Does the system involve the use of online mobile or web-based application?:** *Specify whether the system includes any components that are accessible via the internet, such as mobile apps or web portals.*

13. **Is the system external- and/or internal-facing?:** *Indicate if the system is intended for use only within the University (internal-facing), or if it is accessible by individuals or entities outside the University (external-facing), or both.* (e.g., The HRIS is internal-facing. An online portal for accredited research collaborators, where login is required to access shared data or project updates, is external-facing. An online event registration open to both university members and the general public or invited external guests is both.)

14. **Is the system accessible to the public?:** *Specify whether the general public can access or use the system without requiring special authorization, login credentials, or affiliation with the University.* (e.g., a public website, an open data portal, or an online event registration page, accessible by anyone on the internet)

15. **Do you use the system to make decisions regarding the data subjects?:** *Does your office use the system to generate any decisions/results that may affect the people whose personal data you are processing?*

16. **If yes, indicate the possible decisions that may be made regarding the data subjects?:** *Provide information on the potential decisions, actions, determinations, or conclusions drawn based on the processing of the personal data.* (e.g., Using the system, you get to decide whether to accept or decline a student application, or to determine who is qualified to join a certain program, or to decide who is given access to an online system)

17**. Indicate the factors/criteria used:** *Specify the criteria or factors used in making decisions or drawing conclusions about the affected individuals.* (e.g., age range, civil status, location, financial status, grade range, etc.)

18. **Is the decision-making process automated?** *How does the system generate its decisions? Does it use computer programs or algorithms to make decisions without any form of human intervention?*

19. **What is the lawful basis for processing personal data?** Refer to Items I. 1-6 and Items II. 1-7 of **APPENDIX 2** and indicate the applicable legal basis/es of the processing of the personal data in an automated decision-making context.

20. **If consent is the basis, indicate proof of consent:** *Indicate the medium used to obtain the consent of the affected individuals (e.g., consent form, audio recording, and video recording), and provide the file name of the consent form.*

21. **Do you use the system to profile the data subjects?** *Does your office utilize the system to analyze and categorize (profile) individuals based on their personal data to make predictions, decisions, or assessments about them?*

22. **Indicate the possible decisions made regarding the data subjects:** *Provide information on the potential decisions, actions, determinations, or conclusions drawn based on the processing of the personal data.* (e.g., individuals will be included in a watch list for fraud detection, or they will receive specific marketing campaigns or advertisements based on their demographic information, interests, browsing behavior, or purchase history.)

23. **Indicate the factors/criteria used:** *Specify the data points, characteristics, or attributes used by the system to analyze, categorize, or create profiles of the affected individuals.* (e.g., behavioral data, demographic information, purchase history, online activity, or test scores)

24. **If yes, is the profiling automated?:** *How does the system generate its decisions? Does it make use of computer programs or algorithms to make decisions without any form of human intervention?*

25. **What is the lawful basis for processing personal data?** Refer to Items I. 1-7 and Items II. 1-8 of **APPENDIX 2** and *indicate the applicable legal basis/es of the processing of personal data for profiling purposes.*

26. **If consent is the basis, indicate proof of consent:** *Indicate the medium used to obtain the consent of the affected individuals (e.g., consent form, audio recording, and video recording), and provide the file name of the consent form.*

APPENDIX 2
List of lawful ground for processing personal data

I. Lawful grounds for processing Personal Information

1. The individual gave her **consent** prior to the processing of her personal information, or as soon as practicable and reasonable. She agreed to the collection and processing of her personal information freely, knowing that she can refuse or withdraw it without suffering any negative consequences. She was also informed of the extent of data processing her information will be subjected to.

   Examples:

   A University Press customer expressly agrees to receive new, existing and promotional materials through her registered email address.

   A student allows the Registrar's Office to share her contact details with student organizations during enrollment.

   A former employee gives her consent to have her employee data shared with a prospective employer conducting a background check.

2. Processing the personal information is necessary to fulfill the obligations of the University under a **contract** it entered into with the individual. This also applies if the processing is among the steps necessary for the University to enter into a contract with said individual.

   Examples:

   The University collects from its employees personal information that is necessary in relation to their contract for the purpose of administering their compensation and benefits.

   The Admissions Office shares the economic status of an academic scholar and her household pursuant to her scholarship contract.

   The University processes the personal information of the representatives of service providers it has contracted with.

3. The University needs to process the personal information to comply with a **legal obligation**

   Examples:

   The University discloses personal information if required by a subpoena issued by an appropriate authority.

   The University shares personal information of teachers pursuant to CHED and DepEd regulations.

   The University submits the personal information of foreign students in accordance with Bureau of Immigration rules.

4. The University needs to process the personal information to protect vitally important interests of the individual, including her **life and health.**

   Examples:

   The University discloses to first responders the emergency contact information provided by a student who figured in an accident.

   The University shares with the parents of a victim the CCTV footage of the harassment incident she was involved in.

   The University provides an insurance broker the names and employee numbers of its personnel to ensure they are protected by insurance coverage.

5. The University needs to process the personal information in order to respond to **national emergency** or to comply with the requirements of **public order and safety**. Such requirements must be prescribed by law.

   Examples:

   The University collects personal information for contact tracing purposes pursuant to the national health emergency declared in relation to COVID 19 pandemic.

   The University makes use of an RFID and logbook system to enhance the security of its students.

   The CSMO releases to PNP investigating personnel the names and addresses of attendees in a basketball game held on campus that resulted in a brawl and a number of injured parties.

6. The University needs to process the personal information in order to pursue its **legitimate interests**, or that of a third party to whom the data will be disclosed. This may not be invoked if the fundamental rights and freedoms of the individuals overrides the interests of the University or of the concerned third party.

   Examples:

   The University sends email notifications to its employees' University-issued email address to relay news, developments and policies of the school.

   The University Registrar collects the contact information of attendees to its orientation for the upcoming semester.

   The University may announce an employee's separation from the University to prevent possible occurrences of misrepresentation.

II. Lawful Grounds for the Processing of Sensitive Personal Information and Privileged Information

1. The individual has given her **consent**. In the case of privileged information, though, both of the parties involved in the protected communication must give consent.

   Examples:

   The parent of a minor student gives her consent before the medical records of said student are referred by the University Physician to a Specialist.

   An employee authorizes OHRMOD to share information about her administrative case with a prospective employer.

   An adult student gives her consent before her academic records are transmitted to the school she will be transferring to.

2. The processing about to be conducted by the University is provided for by **existing laws and regulations**. These policies, though, should guarantee the protection of the sensitive personal information involved. Also, if the policies themselves still demand that the consent of the individual be obtained beforehand, then the University must abide by such directive.

   Examples:

   OHRMOD collects the TIN, SSS, Philhealth, and Pag-IBIG information of employees in compliance with relevant government regulations.

   In accordance with DepEd Memorandum Circular 59 (s. 2015), AGS reports the status of bullying or child abuse cases to the agency.

   During the admission process, ASMPH collects the diploma, official transcript of records, and other relevant documents of student applicants pursuant to CHED Memorandum Order No. 18 (s. 2016).

3. The University needs to process the data to protect the **life and health** of the individual or another person. For this to be upheld, however, the individual must be legally or physically unable to express her consent prior to the processing.

   Examples:

   While a student is unconscious, the University Physician discloses her relevant health information to a hospital prior to an emergency medical procedure.

   A guidance counselor shares her psychological assessment to the parent of a student who has been assessed as being capable of inflicting self-harm.

   The BasicEd collects from parents/guardians allergy information on food and medicine of minor students prior to a field trip.

4. The University needs to process the data in order to subject the individual to **medical treatment**. Said treatment, however, must be carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection is given to the data.

   Examples:

   A University Nurse checks the vital signs of a student prior to vaccine administration.

   OHRMOD shares an employee's Philhealth information with her authorized representative as she is about to undergo medical treatment at a hospital.

   The AGS Health Services discloses the health information of a minor student to a Licensed Psychiatrist where the student is undergoing further counseling and psychological treatment.

5. The University needs to process the data to protect its **lawful rights and interests** in court proceedings.

   Examples:

   ULCO utilizes results of administrative cases about an employee in order to defend the University from his claims in a pending labor case.

   In order to establish a claim against an erring service provider, the University offers as a piece of evidence a personal data breach report to the Regional Trial Court.

   The University presents bank deposit and withdrawal slips in court in order to substantiate its allegation of fraud against an erring employee.

6. The University needs to process the data to establish, exercise, or defend its **legal claims**.

   Examples:

   CAO discloses its payment records to the SSS in order to dispel allegations made by an employee regarding its non-remittance of government mandated contributions.

   OAA de gives a student and her parents access to her academic records under its custody after they questioned the revocation of her scholarship grant.

   OHRMOD uses as reference the decision handed down in an administrative case filed against an employee to justify the termination of her employment.

7. The processing involves turning over the data to a government or public authority pursuant to the latter's constitutional or statutory mandate.

   Examples:

   The University provides the Bureau of Immigration with the passport information of students who are foreign nationals.

   The University discloses income tax information about a consultant to the Bureau of Internal Revenue in connection with the latter's ongoing investigation.

   The University reports to the DOH the personal data of employees who have contracted monkeypox.