PRIVACY IMPACT ASSESSMENT

The Privacy Impact Assessment is an analysis of how personally identifiable information is collected, used, shared, and maintained. It is an important component of the school's protection of privacy and is to be implemented as part of the La Consolacion College Manila's privacy by design requirement under the National Privacy Commission Advisory No. 2017-03.

The objectives of the assessment are the following:

(a) to assess how the La Consolacion College Manila processes Personal Data;
(b) to maintain its privacy management program; and
(c) to properly manage privacy risks.

This Privacy Impact Assessment records the document of the Privacy Assessment results of privacy analysis and describes the privacy risk and/or security of La Consolacion College Manila. This serves, then, as a basis for implementing privacy changes.

In observance of the Data Privacy Act (Rule IV), the following are the sections (Sections 17-19) of the Data Privacy Principles:

Section 17. General Data Privacy Principles. The processing of personal data shall be allowed, subject to compliance with the requirements of the Act and other laws allowing disclosure of information to the public, and adherence to the principles of transparency, legitimate purpose, and proportionality.

Section 18. Principles of Transparency, Legitimate Purpose and Proportionality. The processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and proportionality.

a. Transparency. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.
b. Legitimate purpose. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.
c. Proportionality. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal

data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

Section 19. General principles in collection, processing and retention. The processing of personal data shall adhere to the following general principles in the collection, processing, and retention of personal data:

a. Collection must be for a declared, specified, and legitimate purpose.

1. Consent is required prior to the collection and processing of personal data, subject to exemptions provided by the Act and other applicable laws and regulations. When consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn.
2. The data subject must be provided specific information regarding the purpose and extent of processing, including, where applicable, the automated processing of his or her personal data for profiling, or processing for direct marketing, and data sharing.
3. Purpose should be determined and declared before, or as soon as reasonably practicable, after collection.
4. Only personal data that is necessary and compatible with declared, specified, and legitimate purpose shall be collected.

b. Personal data shall be processed fairly and lawfully.

1. Processing shall uphold the rights of the data subject, including the right to refuse, withdraw consent, or object. It shall likewise be transparent, and allow the data subject sufficient information to know the nature and extent of processing.
2. Information provided to a data subject must always be in clear and plain language to ensure that they are easy to understand and access.
3. Processing must be in a manner compatible with declared, specified, and legitimate purpose.
4. Processed personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
5. Processing shall be undertaken in a manner that ensures appropriate privacy and security safeguards.

c. Processing should ensure data quality.

1. Personal data should be accurate and where necessary for declared, specified and legitimate purpose, kept up to date.
2. Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.

d. Personal Data shall not be retained longer than necessary.

1. Retention of personal data shall only for as long as necessary:

(a) for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;

(b) for the establishment, exercise or defense of legal claims; or

(c) for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.

2. Retention of personal data shall be allowed in cases provided by law.

3. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects.

e. Any authorized further processing shall have adequate safeguards.

1. Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes, and, in cases laid down in law, may be stored for longer periods, subject to implementation of the appropriate organizational, physical, and technical security measures required by the Act in order to safeguard the rights and freedoms of the data subject.
2. Personal data which is aggregated or kept in a form which does not permit identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose.
3. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

Physical and Technical Security Measures

It is the duty of La Consolacion College Manila to implement reasonable and appropriate physical and technical security measures for the protection of personal data.

Physical Security

- Secured storage type and location
- Authorized personnel to access the data storage facility
- Monitoring and limitation of access to data storage facility
- Implementation of Clean Desk Policy

Technical Security

- Implementation of Password policy
- Identification using multi-level authentication

How do I accomplish the “Documents” spreadsheet?
1. List down all Documents managed by your UPD unit.

“Documents” are form, template, record, list, table, report, issuance, invoice, receipt or other documents that contain personal information of individuals. Examples are enrollment forms, class lists, request forms, approval forms, vouchers, etc.

2. For each document, identify information on the processing of the concerned document (inbound, outbound, storage, final status).

3. For each document, identify data privacy information in the concerned document (personal information, sensitive information, disclosures, excessiveness).

a. Personal information are any information that can be used to ascertain the identity of an individual. Examples are name, student number, age, contact information, etc.

b. Sensitive information are those information which may cause material damage if misused. Examples are educational information, health information, financial information, etc.

4. Still in the Documents spreadsheet, tell us if you need data privacy help by identifying problems in the concerned document (security, useless steps in processing, risks in processing, etc.).

a. Processing refers to any act done in the document, including accomplishing, receiving, storing, transferring using, disclosing, sharing or destroying the information in the document or the document itself.

5. Tell us your suggestions, if any, on how to improve the concerned document.

Do not hesitate to consult relevant people in your unit to identify and understand the documents used by your unit.

How do I accomplish the “Policies” spreadsheet?

1. In the Policies spreadsheet, list down the title of all the Policies in your UPD units which relates to data governance, data privacy or information security.

   For this purpose, policies includes approved rules, regulations, procedures, guidelines, manual, memo, circular or order in your UPD unit.

2. For each policy, write down the involved UPD units whom are required to follow and those having jurisdiction or authority in cases of violation.
3. Still in the Policies spreadsheet, tell us if you need data privacy help by identifying matters or items that need to be included or revised to improve data privacy.

4. Tell us your suggestions, if any, on what other policies we should create.

How do I accomplish the "Data Processing Systems" Spreadsheet?

1. In the Data Processing Systems spreadsheet, list down the name of the Data Processing Systems your unit or sub-unit use.

   Data Processing Systems refers to either computerized system or physical records which stores, processes or transmits personal information or sensitive personal information owned or managed by your UP Diliman unit or office

   Note: Do not include systems or records managed by another unit or office.

2. For each Data Processing System, identify what classes of UP people's information are being processed.

   UP People refers to students, parents, guardians, faculty, visiting faculty, staff, Research, Extension and Professional Staff (REPS), UP contractual personnel, Non-UP contractual personnel, retirees, applicant students, applicant faculty, applicant staff, researchers, research subjects, patients, clients, customers, alumni, donors, donees, contract counterparties, partners, subcontractors, outsourcees, licensors, licensees and other persons with a juridical link with UP Diliman.

3. For each Data Processing System, what other UP units or Non-UP offices that can access the personal information or sensitive personal information.

4. For each Data Processing System, list down the type of access that other UP units or Non-UP Offices they have (admin/ edit/ view) in the system.

5. Still in the Data Processing Systems spreadsheet, write down the office/s or person/s that receive report with personal information from the system or record.

6. List down the data privacy or information security measures that are currently used to protect data, that are missing or features that are unnecessary.

7. Still in the Data Processing Systems spreadsheet, tell us if you need data privacy help by identifying vulnerabilities, threats or risks to the system or record that should be addressed.

8. Tell us your suggestions on what other improvements, if any, that we can make to the system or record.

What are examples of Personal Information?

Personal information refers to information that can reasonably and directly ascertains an individual or when put together with other information would directly and certainly identify an individual, like:

- Personal details such as name;
- Contact information such as address, email, mobile and telephone numbers.

What are examples of Sensitive Personal Information?

These refers to information that may be used to damage or discriminate against individuals such as:

- Individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- Academic information such as grades, course and academic standing;
- Employment information such as government-issued numbers, position and functions;
- Applicant information such as academic background and previous employments;
- Medical information such as physical, psychiatric and psychological information.

What are some examples of Organizational, Physical and Technical Security Measures?

It is the duty of UP Diliman to implement reasonable and appropriate organizational, physical and technical security measures for the protection of personal data. Below are some examples:

Organizational Security

- Trainings and seminars about Data Privacy and Security
- Privacy Impact Assessment

Physical Security

- Secured storage type and location
- Authorized personnel to access the data storage facility
- Monitoring and limitation of access to data storage facility
- Implementation of Clean Desk Policy

Technical Security

- Implementation of Password policy
- Identification using multi-level authentication