La Consolacion
UNIVERSITY PHILIPPINES
THE CATHOLIC UNIVERSITY OF BULACAN
VALENZUELA ST., CAPITOL VIEW PARK SUBDIVISION, BULIHAN, CITY OF MALOLOS, BULACAN

DATA PRIVACY MANUAL

Table of Contents

I. Introduction

R.A. 10173 known as Data Privacy Act of 2012 aims to protect the fundamental human right of privacy, of communication while ensuring the free flow of information to promote innovation and growth.

Data privacy is important because failing to protect personal data imposes the risk of financial penalties, inefficiencies in processing, involvement by the National Privacy Commission and most importantly the loss of trust to the University. It is far more than just security and protection of personal data.

It is the policy of La Consolacion University Philippines to respect and uphold data privacy rights, and to ensure that all personal information collected from students, their parents or guardians, employees and other third parties, are processed pursuant to the general principles of transparency, legitimate purpose, and proportionality as stated in the DPA.

This Privacy Manual is hereby adopted in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR), and other relevant policies, including issuances of the National Privacy Commission.

This Manual outlines the data protection and security measures adopted by the School to protect data privacy rights, and shall serve as a guide in the exercise of rights under the DPA.

II. Vision-Mission-Goal

Vision

The Data Privacy Office provides services and activities in support of the University. Its focus is the cultivation of data privacy and data protection of personal data to achieve compliance with the National Privacy Commission.

Mission

The mission of the Data Privacy Office is to provide quality services such as: monitoring the compliance of the University to the Data Privacy Act of 2012; training employees to promote data privacy in their everyday task; inform and cultivate awareness on data privacy and data protection.

Goal

To assist all data subjects of the University to uphold their data privacy rights.

III. Scope

This Manual applies to all departments of the School, employees regardless of the type, students, officers and third parties whose information (applicants for admission or employment and former students or alumni whose school records are required to be kept and secured by the School.

Specifies a common privacy terminology, defines the actors and their roles in the processing of personal information and sensitive personal information. Describes privacy safeguarding considerations and provides references to known privacy principles.

The Privacy Manual is applicable to all personnel of La Consolacion University Philippines that is involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of personal information and sensitive personal information.

This Manual is reviewed annually and updated regularly to comply with the current data privacy laws, policies and regulations.

IV. Definition of terms

Access Control – means to ensure that access to assets is authorized and restricted based on business and security requirements

Anonymity – characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly

Attack – attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

Audit – systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.

Authentication – provision of assurance that a claimed characteristic of an entity is correct

Availability – property of being accessible and usable on demand by an authorized entity

Confidentiality – property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Consent – personally identifiable information principal's freely given, specific and informed agreement to the processing of their personal information

Controller – stakeholder that determines the purposes and means for processing personal information other than the data subject

Data subject - an individual whose personal data is processed

Event – occurrence or change of a particular set of circumstances

Information need – insight necessary to manage objectives, goals, risks and problems

Information security – preservation of confidentiality, integrity and availability of information

Information system – set of applications, services, information technology assets, or other information-handling components

Integrity – property of accuracy and completeness

Level or risk – magnitude of risk expressed in terms of the combination of consequences and their likelihood

Management system – set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives

Measure – variable to which a value is assigned as the result of measurement
Monitoring – determining the status of a system, a process or an activity

NPC - National Privacy Commission independent body mandated to implement the DPA

Personal information or Personal data – any information that (a) can be used to identify the data subject to whom such information relates, or (b) is or might be directly or indirectly linked to a data subject

PIC - Personal information controller, a natural or juridical person, or any other body who controls the processing of personal data

PIP - Personal information processor, a natural or juridical person, or any other body to whom a PIC may outsource or instruct the processing of personal data

Privacy breach – situation where personal information is processed in violation of one or more relevant privacy safeguarding requirements

Privacy controls – measures that treat privacy risks by reducing their likelihood or their consequences

Privacy policy – overall intention and direction, rules and commitment, as formally expressed by LCUP related to the processing of personal information in a particular setting

Privacy risk – effect of uncertainty on privacy

Privacy risk assessment – overall process of risk identification, risk analysis and risk evaluation with regard to the processing of personal information, also known as privacy impact assessment

Processing – operation or set of operations performed upon personal information

Processor – stakeholder that processes personal information on behalf of and in accordance with the instructions of the controller

Risk acceptance – informed decision to take a particular risk

Risk analysis – process to comprehend the nature of risk and to determine the level of risk

Sensitive Personal Information – category of personal information, either whose nature is sensitive, such as those that relate to the data subject's most intimate sphere, or that might have significant impact on the data subject

Stakeholder – person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity

Threat – potential cause of an unwanted incident, which can result in harm to a system or organization

Third party – stakeholder other than the data subject, controller and the processor, who are authorized to process the data under the direct authority of the controller or processor

Top management – person or group of people who directs and controls an organization at the highest level

Vulnerability – weakness of an asset or control that can be exploited by one or more threats

V. Data Subject rights

The Right to be Informed

As a data subject, you have the right to be informed that your personal data will be, are being, or were, collected and processed.

The Right to Access

This is your right to find out whether an organization holds any personal data about you and if so, gain “reasonable access” to them.

The Right to Object

You can exercise your right to object if the personal data processing involved is based on consent or on legitimate interest.

The Right to Erasure or Blocking

Under the law, you have the right to suspend, withdraw or order the blocking, removal or destruction of your personal data.

The Right to Rectify

You have the right to dispute and have corrected any inaccuracy or error in the data a personal information controller (PIC) hold about you.

The Right to Data Portability

This right assures that YOU remain in full control of YOUR data. Allows you to obtain and electronically move, copy or transfer your data in a secure manner, for further use.

The Right to file a Complaint

If you feel that your personal information has been misused, maliciously disclosed, or improperly disposed, or that any of your data privacy rights have been violated, you have a right to file a complaint with the NPC.

The Right to Damages

You may claim compensation if you suffered damages due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, considering any violation of your rights and freedoms as data subject.

VI. Role of the Data Privacy Officer

A. Monitors the compliance of the University with the Data Privacy Act of 2012, its IRR, issuances by the NPC and other applicable laws and policies through the following:
    a. collection of information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;
    b. analyzing and checking the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
    c. informing, giving advice, and issuance of recommendations to the PIC or PIP;
    d. ascertaining renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
    e. providing advice to the PIC or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;
B. Ensures the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the University;
C. Advises the University regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);
D. Ensures proper data breach and security incident management by the University, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
E. Informs and cultivates awareness on privacy and data protection within the University, including all relevant laws, rules and regulations and issuances of the NPC;
F. Advocates for the development, review and/or revision of policies, guidelines, projects and/or programs of the University relating to privacy and data protection, by adopting a privacy by design approach;
G. Serves as the contact person of the University vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the University;
H. Cooperates, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and
    a. Performs other duties and tasks that may be assigned by the University that will further the interest of data privacy and security and uphold the rights of the data subjects.

VII. Recognizing Personal Information and Sensitive Personal Information

It is important to be aware that an individual can be identified either:
Directly, if you are able to identify a specific individual solely through the data you are processing. Example: name, ID number, email address
Indirectly, if different sets of data from different sources, when combined, could identify a specific person. Example: gender, birthdate, license plate

VIII. What is personal information?

Personal information is any information that can identify a person. This could be a name or account number or could be a digital identifier such as IP address, username, or location data such as GPS coordinates.

- Name
- Address
- Place of work
- Telephone number
- Gender
- Location of an individual at a particular time
- IP address
- Birth date
- Birth place
- Country of citizenship
- Citizenship status
- Payroll and benefits information
- Contact Information

IX. What is sensitive personal information?

Some personal information is considered sensitive, as it could cause harm to the individual if leaked or misused. Personal information is classified as ‘sensitive if it relates to:

- Age
- Marital Status
- Racial or ethnic origin
- Political or religious beliefs
- Physical or mental health
- Sex life or sexual orientation
- Criminal offences and court proceedings
- Genetics
- Social security number
- Licenses or its denials, suspensions or revocation
- Tax returns
- Other personal information issued by government agencies
- Bank and credit/debit card numbers
- Websites visited
- Materials downloaded
- Any other information reflecting preferences and behaviors of an individual
- Grievance information
- Discipline information
- Leave of absence reason

X. When can personal information be processed?

1. Organizations must have at least one of the following valid lawful bases for processing:
2. Consent: of the individual to the processing of their personal information
3. Legitimate interest: of the organization or the third parties engaged
4. Contractual obligation: processing is needed in order to enter into or perform a contract
5. Legal obligation: for which the organization is obliged to process personal information for
6. Vital interest: of individuals, where processing is necessary to protect life, health, vitally important interest
7. Public Interest: national emergency, public order, public safety

XI. When can sensitive personal information be processed?

Sensitive personal information can usually only be processed with the individuals consent, unless the data is required for filing legal proceeding, or if there is any legal, public interest, regulatory requirement, or for protection of life and health.

XII. Privacy Principles

General Data Privacy Principles based on the Implementing Rules and Regulations of the Data Privacy Act of 2012:

TRANSPARENCY. Data Subject's consent should be obtained before collecting the information and the latter should be informed of the purpose for which the information is to be collected.

Example: In the enrolment process, upperclassmen are required to fill out the Student Data Sheet. The purpose of such collection of information is stated in the form and the consent of the student is obtained through the form which is filled out and signed by the student.

PROPORTIONALTY. Personal Information collected must be reasonably necessary or directly related to the School functions

Example: In the application for admission as a JHS student in LCUP, only information such as name, address, contact numbers, previous schools, parent's or guardian's name, which necessary for the evaluation for eligibility for admission to the School is collected.

FOR LEGIMATE PURPOSE. In collecting personal information, the School shall use the information only for legitimate purposes as discussed in Section VI of this Manual

Example: Personal information such as student's name, parents name and addresses and contact numbers etc., shall be used only for purposes such as enrolment, academic activities and availment of student services which is allowed under the provisions of the MORPE for Secondary Education

XIII. Privacy Statement and Privacy Policy

Privacy Statement

LCUP is committed to protect the privacy rights of individuals on personal information pursuant to the provisions of Republic Act No. 10173 or the Data Privacy Act of 2012, its Implementing Rules and Regulations and the Basic Education Act of 1982.

All employees, students and administration officers are enjoined to comply with and to share in the responsibility to secure and protect personal information collected and processed by LCUP in pursuit of legitimate purposes.

General Privacy Policy Statements

1. LCUP adheres to the general principles of transparency, legitimate purpose and proportionality in the collection, processing, securing, retention and disposal of personal information.
2. The students, parents, guardians, employees or third parties whose personal information is being collected shall be considered as data subjects for purposes of these policies.
3. Data subjects shall be informed the reason or purpose of collecting and processing of personal data.
4. The data subjects shall have the right to correct the information especially in cases of erroneous or outdated data, and to object to collection of personal information within the bounds allowed by privacy and education laws.
5. The data subject has the right to file a complaint in case of breach or unauthorized access of his personal information.
6. LCUP shall secure the personal information of students, parents, guardians, employees and third parties from whom personal information is collected and shall take adequate measures to secure both physical and digital copies of the information.
7. LCUP shall ensure that personal information is collected and processed only by authorized personnel for legitimate purposes of the School.
8. Any information that is declared obsolete based on the internal privacy and retention procedures of the School shall be disposed of in a secure and legal manner.
9. Any suspected or actual breach of the LCUP Data privacy policy must be reported to any member of the Data Privacy Response Team in accordance with the procedure provided in Article IX (ii) of this Manual.
10. Data subjects may inquire or request for information from the Data Privacy Response Team, regarding any matter relating to the processing of their personal data under the custody of LCUP, including the data privacy and security policies implemented to ensure the protection of their personal data pursuant to Article IX (i) of this Manual.

Privacy Policy

Collection of Data

The University collects students' personal information, including their full name, address, email address, contact number, birthday, education, health, marital status, family background, and other personal information obtained through interviews and during entrance examinations, guidance, and counseling activities.

Use of Data

All data gathered through offline and online mechanisms shall only be used for the specified purpose/s, such as admission, attendance to activities, evaluation, and counseling, and shall be accessed only by authorized school personnel.

Storage, Retention, and Disposal

The University will ensure that all personal data under its custody are protected against any accidental or unlawful disposal, alteration, and disclosure, as well as against any other unlawful processing. In addition, the University will implement appropriate security measures in storing collected personal information, depending on the nature of the information.

Disclosure and Sharing

Personal data under the custody of the University shall be disclosed only pursuant to a lawful purpose and authorized recipients of such data. Information such as name, course, year, and awards could be posted on the University website and social media accounts. All employees and personnel of the University shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of the contract, or other contractual relations.

Changing This Data Privacy Policy

Changes could be made to this Data Privacy Policy from time to time and posted on our website. Changes will be immediately enacted as soon as they are posted.

XIV. Personal Information Life Cycle

Collection

The University and its employees must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more function or activity of the University. LCUP employees may collect personal information only by lawful and fair means, and not in an intrusive way. Whenever LCUP employees collect personal information about an individual, they must take reasonable steps to ensure that the individual is aware of the following:

1. The identity and contact details of LCUP as the organization collecting and storing the information;
2. The purposes for which the information is collected;
3. The intended recipients or organizations to which LCUP usually discloses information of that kind;
4. Any law that requires the particular information to be collected;
5. The main consequences (if any) for the individual if all or part of the information is not provided; and
6. The latest version of the Data Privacy Policy of LCUP which can be accessed at https://www.lcup.edu.ph/dpo.php

Receiving Unsolicited Personal Information

Where LCUP employees receive unsolicited personal information about an individual they must immediately determine whether they could have collected the information in accordance with sections (personal information life cycle). If so, then this policy shall apply to the processing of such information. Otherwise, then they must either destroy or anonymize the information, if they failed to obtain the consent of the individual (lawfully and reasonably)

Collection of personal information for research and statistics

LCUP employees may also collect personal information for research about an individual from a party other than the individual concerned if:

1. The personal data is publicly available; or
2. There is consent from the data subjects for purpose of research,
3. Provided that adequate safeguards are in place and no decision directly affecting the data subject shall be made on the basis of the data collected or processed.

Collection of personal data for CCTV surveillance

Certain areas and buildings use CCTV system to monitor their exterior and interior 24 hours a day for security reasons. This data is recorded for 30 days. The use of CCTV and recording of CCTV data are only carried in accordance with LCUP approved guidelines

LCUP will take reasonable efforts to alert the individual that the area is under electronic surveillance by posting CCTV signage.

Use and Disclosure of Personal Information

As a general rule, LCUP employees must not use or disclose personal information about an individual other than for its primary purpose of collection, unless:

1. The individual has consented to the use or disclosure; or
2. The individual would reasonably expect LCUP to use or disclose non-sensitive information for a secondary purpose and the secondary purpose is related to the primary purpose; or
3. LCUP has reason to suspect that unlawful activity has been, or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
4. The use or disclosure is required or authorized by or under law, rule or regulation; or
5. LCUP reasonably believes that the use or disclosure is reasonably necessary for a specified purpose by or on behalf of an enforcement or other body; or

6. LCUP reasonably believes that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to public health or public safety or the life or health of an individual; or
7. LCUP must only use or disclose personal information in a manner consistent with any privacy notice provided to an individual.

Storage and Transmission
LCUP shall implement approved security measures to all personal information stored onsite.
Access to stored personal information shall be limited only to authorized and appropriate LCUP employees only.
LCUP allows outside transmission of information to the effect that encryption is employed to personal information identified as sensitive.

Retention
Personal data shall be retained only for the duration necessary to fulfill the identified lawful business purpose. All personal data of the data subjects shall be retained only for as long as necessary:
1. For the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated; or
2. The establishment, exercise, or defense of legal claims; or
3. For legitimate business purposes, which must be consistent with standards followed by the industry; or
4. In some specific cases, as prescribed by law.

LCUP shall develop guidelines and procedures for the retention of personal data. These shall address minimum and maximum retention periods, and modes of storage.

All hard, system, soft, and electronic copies will be disposed appropriately following our disposal and destruction policy. In cases in which we intend to keep the information after retention period, subsequent consent from the data subject must be obtained.

Personal data collected for other purposes may be processed for historical, statistical, or scientific purposes, and in cases laid down in law may be stored for longer periods, provided that adequate safeguards are guaranteed by said laws authorizing their processing, or consent has been obtained to retain and use for such purposes.

Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

Disposal and Destruction
Guidelines and procedures shall be developed for the secure disposal and destruction of personal data to prevent further processing, unauthorized access, or disclosure to any other party or public, or prejudice the interests of the data subjects. These shall also address disposal process on each of the following, but not limited to, the types of storage:
1. Files that contain personal data, whether such files are stored on paper, film, optical or magnetic media; and
2. Computer equipment, such as disk servers, desktop computers and mobile phones at end-of-life, especially storage media, provided that the procedure may include the use of degaussers, erasers, and physical destruction devices, among others.

Upon the expiration of identified lawful business purposes or withdrawal of consent, LCUP must take reasonable steps to securely destroy or permanently de-identify or anonymize personal information if it is no longer needed. Data may be anonymized, as deemed appropriate, to prevent unique identification of an individual.

Disposal should be in a manner that the personal data should be unreadable (for paper) or irretrievable (for digital records).

XV. Privacy Impact Assessments

Privacy Impact Assessment ("PIA") should be completed when there are events that significantly change in the privacy environment or affect the processing of personal information, consisting the significant events set forth as follows:

1. New processes or modification to the current process;
2. New projects;
3. Marketing initiatives; and/or
4. Changes in the IT System Infrastructure.

XVI. Data Breach Management

The University shall implement policies and procedures for the purpose of managing security incidents, including personal data breach. These policies and procedures must ensure:

Creation of a data breach response team shall be responsible for investigating the suspected security incident. The Data Privacy officer together with other University personnel appointed by the University President will compose of the data breach response team. All members must have a rank of administrator.

A member of the team can seek assistance from other personnel of his or her office, provided he or she remain the signatory in all related documents concerning the data breach investigation.

Duties and Responsibilities

Data Breach Response Team

- Investigate and assess reported and/or suspected security incident concerning personal information.
- Recommend remedial measures to be performed by the department involved with the security incident.
- Accomplish the data breach incident report form.

Data Privacy Officer

- Serve as the point of contact of all reports of a suspected security incident.
- Custodian of all reports and documents concerning all reported and suspected security incident.
- Assist the University in the performance of their functions under this policy.
- Notify the National Privacy Commission within 72 hours of a data breach.

University President

- Accept, reject, or otherwise take action based on the findings/recommendations of the data breach incident report.
- Appoint members of the data breach management team.
- Approve, rejects, recommend changes, or otherwise comment on proposed changes to this policy.

Departments

- Submit a data breach incident report.
- Implement measures to avoid or minimize the risk and impact of data breach incidents.
- Cooperate with the data breach response team.
- Assist the data breach response team in the investigation and resolving each reported incident.

Data Breach Notification

a) The National Privacy Commission and affected data subjects shall be notified by the University within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the University that, a personal data breach requiring notification has occurred.

b) Notification of personal data breach shall be required when sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the University or the National Privacy Commission believes

that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

XVII. Confidentiality and Non-Disclosure Agreement

Employees who collect, use, store, retain and dispose of personal information are required to sign a confidentiality and Non-disclosure agreement.

Definition of Confidential Information shall include but is not limited to:

a. personal information as defined under the Philippine Data Privacy Act (DPA). It is 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 e.g. home addresses and other contact details of students, personnel or persons who have contracts with LCUP.
b. sensitive personal information as defined under the DPA which includes personal information
    i. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
    ii. About an individual's 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;
    iii. 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
    iv. Specifically established by an executive order or an act of Congress to be kept classified.
c. Privileged information refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication
d. proprietary information such as trade secrets, confidential research data, information the disclosure of which would prejudice intellectual property rights
e. usernames, passwords, access codes and the like
f. information that is confidential under other applicable laws
g. information obtained by the University from third parties under non-disclosure agreements or any other contract that designates third party information as confidential

Obligations of employees

a) Not to acquire, use nor distribute such Personal Information without the express consent of the subject of such Personal Information, or if applicable law will allow such acquisition and disclosure of Personal Information without consent.
b) To acquire, use and/or distribute Personal Information solely for the purposes of carrying out the daily functions of Employee's job.
c) To disclose Personal Information only to authorized third parties. These agencies may include, but are not necessarily limited to, independent review agents, claims adjusters, benefits administrators, attorneys and employers.
d) To limit access to computerized Personal Information solely to staff, authorized users and administrative personnel and will abide by all security measures designed to assure that unauthorized personnel are not afforded access to Personal Information.
e) To not use any Personal Information for own benefit, publish, copy, or otherwise disclose to others, or permit the use by others for their benefit or to the detriment of the Disclosing Party, any Confidential Information.
f) To return to the Disclosing Party any and all records, notes, and other written, printed, or tangible materials in its possession pertaining to Confidential Information immediately if Disclosing Party requests it in writing.

XVIII. Inquiries and Complaints

LCUP should receive all inquiries and complaints related to the privacy of the data subject, as well as entertain and institute an investigation in relation thereof.

Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of LCUP, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the DPO and briefly discuss the inquiry, together with their contact details for reference.

Data Privacy Office Contact Information

Email: dpo.email.lcup.edu.ph
Data Privacy Complaints: https://bit.ly/dpo_complaint

XIX. Policies and Guidelines

Privacy Policy for Students, Parents and Guardians

Information We Collect, Acquire, and Generate

All personal information we collect follow the principle of Transparency, Proportionality and Legitimate Purpose. LCUP collects personal information upon admission and enrollment from the student, parent and/or guardian. Personal information collected include but not limited to:

- Personal details such as name, birth, gender, civil status and affiliations;
- Contact information such as address, email, mobile and telephone numbers;
- Academic information such as grades, course and academic standing;
- Medical information such as physical, psychiatric and psychological information.

Only authorized LCUP personnel shall have access to use the collected personal information. Collected information shall be used for the following:

- Evaluation of application to the University
- Enrollment process
- Admission
- Compliance with DEPED and CHED orders and memorandums;
- Academic records
- Recognition and awards
- Processing of grades
- Maintaining records of academic, co-curricular, and extra-curricular activities
- Maintaining student information systems
- Processing of scholarship application
- Maintaining alumni records
- Generating data for statistical and research purposes
- Communicating official school announcements
- Distribution of marketing and promotional materials regarding school related activities, events and projects
- Student organizations
- Collaboration with public and private agencies and institutions
- Student development and student welfare programs
- Medical, dental, psychiatric and psychological records
- Scholarship Programs
- Internship Programs
- Student Disciplinary process
- Security
- Accreditation
- Immigration assistance
- Other purposes necessary for LCUP to perform its obligation and function as a higher education institution

Sharing, Disclosure, or Transfer of your information may include the following:

- As part of the requirements of CHED/DEPED
- Processing of scholarship, awards, and membership to outside organizations
- Internship matching program
- Sharing of your personal information to parents and guardians for health, safety and security
- Requirements for accreditation
- Immigration, visa application and extension
- Live streaming of activities, events, programs of the University
- For research and publication

- For social media post for the purpose of marketing and promotion of school related activities, events and projects

Storage and Retention of your information

The University will ensure that all personal data under its custody are protected against any accidental or unlawful disposal, alteration, and disclosure, as well as against any other unlawful processing. In addition, the University will implement appropriate security measures in storing collected personal information, depending on the nature of the information.

Privacy Policy for Personnel

This policy covers how the University collect, use, store, retain and dispose of personal information from all personnel. La Consolacion University Philippines is dedicated to protecting and preserving the data privacy of our personnel. Therefore, we are committed to complying and implementing the Data Privacy Act of 2012.

Information We Collect, Acquire, and Generate
We collect your personal information in different forms. The information may be in paper or electronic form, photo and video, and biometric records. It may include the following:

- Personal details such as name, birth, gender, civil status and affiliations;
- Contact information such as address, email, mobile and telephone numbers;
- Academic information such as grades, course and academic standing;
- Medical information such as physical, psychiatric and psychological information.

Collected information shall be used for the following:

- Evaluating applicants and processing their applications
- Verifying the applicants submitted information
- Administering human resource and development program
- Processing payroll and benefits of employees
- Other similar or related tasks

Sharing, Disclosure, or Transfer of your information may include the following:
Submission of information to government agencies such as CHED, DEPED, SSS, PhilHealth, Pag-IBIG, and BIR

- Requirements for accreditation
- Live streaming of activities, events, programs of the University
- For research and publication
- For social media post for the purpose of marketing and promotion of school related activities, events and projects
- Other purposes, when necessary and under circumstances permitted or required by law

Storage and Retention of your information
The University will ensure that all personal data under its custody are protected against any accidental or unlawful disposal, alteration, and disclosure, as well as against any other unlawful processing. In addition, the University will implement appropriate security measures in storing collected personal information, depending on the nature of the information.

Changing This Data Privacy Policy

Changes could be made to this Data Privacy Policy from time to time and posted on our website. Changes will be immediately enacted as soon as they are posted.

Storage, Retention and Disposal Policy

The purpose of this Policy is to ensure that necessary records and documents of are adequately protected and maintained and to ensure that records that are no longer needed by La Consolacion University Philippines or are of no value are discarded at the proper time. This Policy is also for the purpose of aiding employees of La Consolacion University Philippines in understanding their obligations in retaining electronic documents - including e-mail, Web files, text files, sound and movie files, PDF documents, and all Microsoft Office or other formatted files.

The University will ensure that all personal data under its custody are protected against any accidental or unlawful disposal, alteration, and disclosure, as well as against any other unlawful processing. In addition, the University will implement appropriate security measures in storing collected personal information, depending on the nature of the information.

This Policy applies to all physical records generated in the course of La Consolacion University Philippines's operation, including both original documents and reproductions. It also applies to the electronic documents described above.

Guidelines for Consent Form

The processing of personal information should always adhere with the principle of Transparency, Legitimate purpose, and Proportionality

Data subjects (students, parents, employees, and guests) should always be informed regarding the nature, purpose, and processing of his/her personal information. The processing of personal information shall correspond with the stated privacy policy, privacy notice, and consent form which must not be contrary to law, morals, or public policy. Personal information processing should be adequate, relevant, suitable, necessary, and not excessive in relation with the privacy policy, privacy notice, and consent form.

The consent form must include the following:

1. General statement involving the collection of data.
2. Basis of processing (legal, contract, etc.).
3. Detailed explanation regarding the collection, storage, usage, security and disposal should be included.
4. Explanation of the purpose of the data being collected: marketing, profiling, or historical, statistical or scientific purpose.
5. Recipient/s of the personal information.
6. Define the length of time that the collected data will be used, stored and retained.
7. Discuss the security measures applied to protect the privacy of the data subject.
8. Discuss when the data collected will be disposed and the method of disposal.

Consent should be freely given, specific, informed and unambiguous indication of the data subject's agreement to the data processing of his or her information. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all data processing activities for the same purpose/s. When the processing has multiple purposes, consent should be given for all of them.

Consent Form Sample

La Consolacion University Philippines is committed in complying and implementing the Data Privacy Act of 2012. This form covers how the University collects, use, store, retain and dispose of personal information.

La Consolacion University Philippines is the personal information controller of your personal information.

The University will be collecting and using the following: [only include information that is required for needed or processing]

- Full name
- Address
- Email address
- Telephone Number

Your personal information collected will be used for the following purposes: [only include the purpose of the information being collected]

- Evaluation of application to the University
- Enrollment process
- Admission
- Compliance with DEPED and CHED orders and memorandums;
- Academic records
- Recognition and awards
- Processing of grades

The information collected may be shared, disclosed, or transferred to the following: [only include what is necessary]

- As part of CHED/DEPED requirements
- Requirements for accreditation
- Immigration, visa application and extension
- Live streaming of activities, events, programs of the University
- For research and publication

The University will ensure that all personal data under its custody are protected against any accidental or unlawful disposal, alteration, and disclosure, as well as against any other unlawful processing. In addition, the University will implement appropriate security measures in storing collected personal information, depending on the nature of the information.

Name:
Signature:
Date: