Philippine Christian University
INFORMATION AND COMMUNICATIONS TECHNOLOGY CENTER
Tel. Nos. 5310-0651/8524-7684 e-mail: team.itd@pcu.edu.ph
URL: https://www.pcu.edu.ph; dasma.pcu.edu.ph; mjcn.pcu.edu.ph

Inter-Office Memo (Manila Campus and MJCN Campus)

MEMORANDUM ICT-2K22-078

TO : ALL ACADEMIC AND ADMINISTRATIVE UNITS
[Academic in-Campus Cluster c/o the Office of the Vice President for Academics]
[Globalization and Extension Cluster c/o the Office of the Vice President for Globalization and Extension Program (OVGEP)]
[Finance and Administration Cluster c/o the Office of the Vice President for Finance and Administration (OVPFA)]
[as administered by the Technical and Student Services Cluster c/o the Office of the Vice President for Information and Communications Technology (OVPICT)]

FROM : PROF. MARIO G. MIRANDA, II
Vice President for Information and Communications Technology
(Head, Technical and Student Services Cluster)

DATE : 08 March 2022 (Tuesday)

RE : UNIVERSITY DATA MANAGEMENT POLICY

POLICY ICT-017: UNIVERSITY DATA MANAGEMENT POLICY

POLICY STATEMENT: All Academic Units, Administrative Units and members of the PCU Community must access and utilize University data in ways that safeguard the data and protect the institution.

Academic Units, Administrative Units and members of the PCU Community must ensure:

1. Compliance with regulatory and statutory requirements of government agencies (National Privacy Commission (NPC), NBI, DOJ, DICT etc.) in-charge of digital data as well as third-party and other contractual data obligations.
2. Data is used for the purposes for which it is collected with emphasis on sensitive data or data subjects and any restrictions for its use are observed as outlined in RA 10173 or the Data Privacy Act of 2012.
3. Data is collected, stored, and disposed of in ways appropriate to the risk and impact of unintended disclosure as outlined in ISO 9001:2015 on risk management.

For research data, the principal proponent is accountable for all decisions regarding their research data. With reference to the guidelines set by the National Privacy Commission (NPC), personal information *does not apply* for journalistic, artistic, literary or research purposes.

For decisions regarding institutional data, such as access, classification and appropriate use, members of the PCU community must consult the designated Data Manager or the Data Privacy Office (DPO) that has accountability for the data. These roles and accountabilities are defined and outlined in the *University Data Governance Framework* to be published, thereafter, in sequence of this memorandum.

PHILIPPINE CHRISTIAN UNIVERSITY
Office of the President
RECEIVED
BY:
DATE/TIME: 3/10/2022 9:40 AM

PURPOSE AND OBJECTIVES: **Philippine Christian University** is responsible for ensuring the availability, confidentiality and integrity of all information to which it is entrusted. University data, whether managed and residing on **University Information and Communications Technology** resources, stored on personal devices, managed by a third party or a business partner, or outsourced to a service provider, is an important asset that must be governed, protected and appropriately safeguarded.

Improper use of the University's data may result in harm to the University, its faculty, staff, students and alumni. This harm could impact the university's mission of teaching and learning, research and service delivery. It exposes the University to criminal, financial and reputational risks. ***Members of the PCU Community have the responsibility to appropriately use, maintain and safeguard University data.***

This **policy** will provide a framework to safeguard and protect the University's data while providing flexibility to support the broad range of academic, research and administrative activities.

GUIDING PRINCIPLES: This **policy** is guided by the principles and values outlined in the **Philippine Christian University mission statement, vision statement, ICTC vision statement, ICTC mission statement, ICTC core values and thrust, University quality policy** among the **Academic and Administrative Units** and by the principles outlined in the **University's ICTC enterprise architecture.** It was also developed in the context of the following data management principles:

- Protecting the University's data is a responsibility shared by all members of the PCU community. Data protection begins with the person or office creating the data and is the continuing responsibility of all who subsequently access and use it.
- University data is critical to the University's academic, research and administrative activities. In order to reduce the damaging impact of data loss on business continuity, academic activities and research programs, University data must be appropriately safeguarded.

- The requirement to safeguard University data must be balanced with the need to access and use data in support of the pursuit of legitimate academic, research and administrative activities.
- Reference and particulars on Data Privacy may be viewed on the official website of the University or the National Privacy Commission.
- The University uses a risk-based approach as outlined in the guiding procedures and tenets of ISO 9001:2015 following the best practices in data management, to select appropriate access controls to minimize risk to an acceptable level and to design security and privacy into its data infrastructure.

DEFINITION OF TERMS:

- **University data** – Data that is created, collected and stored (either electronically or in hard copy) by Departments/Colleges/Units and members of the PCU community, in support of academic, research and administrative activities. University data may include the following (these are not mutually exclusive):

  - ✓ **Data subject** – An individual whose personal information is processed.
  - ✓ **Institutional data** – Data that is created, collected and stored by all units and members of the PCU community, in support of academic and administrative activities. Administrative data about teaching, learning, research and scholarly activity, such as grades, attendance, research grants held and publications generated, is considered institutional data.
  - ✓ **Research data** – Data that is created by or derived from research, scholarly and artistic activities.
  - ✓ **Personal data** – Data that contains personal information about an identifiable individual, if compromised or used inappropriately, this would have implications to the privacy of an individual.
  - ✓ **Personal information** – Any information whether recorded in a material form or not, from which the identity of the 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.
  - ✓ **Sensitive data** – Data that is identified as **classified information that must be protected and is inaccessible to outside parties unless specifically granted permission**. The data can be in physical or electronic form, but either way, sensitive data is regarded as private information or data.
  - ✓ **Third-party data** – Data that is created or owned by a third party and is being used in support of academic, research and administrative activities. This data if compromised or used inappropriately would have implications for the third party. This includes data such as licensed software or software components and copyrighted material.

- **Derived data** – Data that is changed from the original data using a mechanism such as an arithmetic formula, composition or aggregation.
- **Data management** – Encompasses activities that relate to the creation, collection, storage, maintenance, cataloguing, use, dissemination and disposal of University data.
- **Data Manager** – An individual who develops and governs data-oriented systems designed to meet the needs of the University in his or her specific designation, function, role and responsibilities or otherwise stated, an individual designated to do research for the advancement of the University.
- **National Privacy Commission (NPC)** - An independent body created under Republic Act No. 10173 or the Data Privacy Act of 2012, mandated to administer and implement the provisions of the Act, and to monitor and ensure compliance of the country with international standards set for data protection.
- **PCU community** – All PCU students, employees, faculty, post-doctoral fellows, alumni, agents, contractors, authorized guests, persons or organizations acting for or on behalf of the University.

DEFINITION OF TERMS (continued):

- **Republic Act No. 10173 or the Data Privacy Act of 2012** - A law that seeks to protect all forms of information, be it private, personal, or sensitive. It is meant to cover both natural and juridical persons involved in the processing of personal information.
- **University owned** – Assets purchased by University funds including research grants administered by the University or acquired by the University through some contractual agreement.
- **ICT/IT services** – Technology-based services managed or hosted by a PCU community member, the University or vendors/contractors.
- **ICT/IT infrastructure** – ICT/IT assets including, but not limited to, servers, databases, data, software, end-point devices, the University network, Internet connections, central authentication, telephone systems and data centers, whether provided directly or indirectly by the Information and Communications Technology Center (ICTC) or classified as a contracted service.
- **ICT/IT outsourcing** – The use of external service providers to deliver ICT/IT-enabled business process, application service and infrastructure solutions. Outsourcing can include, but is not limited to, utility services, Software as a Service (SaaS) and cloud-enabled outsourcing.

POLICY SCOPE: This **policy** is applicable to all PCU community members and all Philippine Christian University Academic and Administrative units, ancillary units and any affiliated organizations (collectively referred to as "units") that create, modify or make use of University data.

It covers all University data regardless of where it is stored (on-campus or off-campus sites), where it is being accessed from (on-campus or off- campus sites) and whether the data is in raw form, derived, summarized or aggregated.

The policy has been developed in the context of, and is designed to complement the following:

- Existing University policies and regulations, the provisions of which is identified in the University Manual, particularly those governing use of University property and services; computer use; Information Technology or Information and Communications Technology security and control; privacy; risk management; records management; responsible conduct of research; disciplinary procedures; copyright and intellectual property.
- Legislation and statutory laws and are mandated by the National government or Local Government;
- Legal contracts and agreements with external sponsors, granting agencies, and others;
- Collective agreements.

For decisions regarding institutional data, such as access, classification and appropriate use, members of the PCU community must consult the Data Manager that has accountability for the data. These roles and accountabilities are defined in the *University Data Governance Framework*.

ROLES AND RESPONSIBILITIES: Data Managers within the University have specific data management accountabilities and responsibilities as outlined in the *University Data Governance Framework.*

A. Information and Communications Technology Center (ICTC):

The **University's Information and Communications Technology Center (ICTC)** is responsible for maintaining the availability and security of the University's data infrastructure ensuring that authorized users have access to the data they require for academic, research and administrative activities.

ICTC is responsible for implementing security and access measures that mitigate the risk of unintended disclosure of electronic data. This includes, but is not limited to, continually improving end-user awareness of proper data management; maintaining physical security of data infrastructure; implementing appropriate data access; and providing data cataloging technologies to users.

B. Departments/Colleges/Units:

Academic, administrative and ancillary units are responsible for ensuring they access and use University data (both electronic and hard copy) in a manner that minimizes risk to the University.

The best way to minimize risk to electronic University data is to use the university-approved ICT infrastructure (including data centers and end-point devices) and services for all University activities to the greatest extent practicable.

C. PCU Community Members:

Individual members are responsible for ensuring they access and use University data (both electronic and hard copy) in a manner that minimizes risk to the University. They must understand that data management is a shared responsibility across the PCU community and they must abide by data management procedures and practices. These responsibilities include:

- ✓ Using data only for authorized and intended purposes.
- ✓ Understanding the data and guarding against misinformed or incorrect interpretations. For any questions regarding the data, they should contact the **Data Manager** in their respective Cluster or functional unit **or** the **Data Privacy Office (DPO)** with data management accountability for that data.
- ✓ Respecting the privacy of the data and the individuals that it represents. This includes not disclosing personal information, nor accessing or manipulating such data for personal gain or interest.
- ✓ Ensuring that they do not knowingly falsify data nor inappropriately delete or reproduce data.

NON-COMPLIANCE TO POLICY ICT-017: If there is reason to suspect that laws or University policies have been, or are being violated, or that continued access poses a threat to the University's data, data infrastructure, PCU community members or the reputation of the University, access to the University's data and data infrastructure may be restricted or withdrawn.

Following due process, the University may take action against anyone whose activities are in violation of the law or of this policy. The actions taken may include, but are not limited to:

- ✓ Revocation of access to the University's data, ICT/IT services, ICT/IT infrastructure or parts of it. This will be explained further in the Acceptable Use Policy and other ICT Policies, to be promulgated by the University and ICTC, in sequence of this Memorandum.
- ✓ Disciplinary action for students following the University Student Manual administered by the Student Services Office – Office of Student Affairs, as approved by the University President and the PCU – Board of Trustees.
- ✓ Disciplinary action for employees.

Ignorantia legis neminem excusat (Ignorance of the law excuses no one).

Please be guided accordingly.

Approved by:

JUNIFEN F. GAUUAN, Ph. D.
University President

Distribution:

- ✓ Distributed in print for the offices of Data Managers and the DPO
- ✓ Distributed electronically via the University's Official email and systems
- ✓ Published in the official University Website of the PCU Manila Campus