development academy of the philippines

MEMORANDUM CIRCULAR	REVISED DAP DATA PRIVACY AND INFORMATION PROTECTION POLICY	Date: October 13, 2025
Number: MC-2025-021		Page: 1 of 7

REFERENCE DOCUMENTS

- Republic Act 10173: Data Privacy Act of 2012
- Implementing Rules and Regulations of RA 10173
- NPC Circular 2023-05 on Personal Data Protection
- NPC Circular 2023-06 on Security of Personal Data in Government and Private Sector
- Board Resolution No. 21 s.2025 Appointing Mr. Leocadio S. Sebastian as the Acting President and CEO and Acting Member of the Board of Trustees of the Development Academy of the Philippines
- Board Resolution No. 012 s.2024 Confirming the Authority of the President of the Development Academy of the Philippines (DAP) as its Chief Executive Officer, to Promulgate Internal Management Policies and Implementing Rules and Regulations via Office Orders, Special Orders, and Memoranda-Circulars
- MC-2024-016: DAP Data Privacy and Protection Guidelines
- SO-2024-155: Designation of DAP Data Protection Task Force Members

I. RATIONALE

It is the policy of the State to protect the fundamental human right to privacy and communication while ensuring the free flow of information to promote innovation and national development. The State recognizes the vital role of information and communications technology (ICT) in nation-building and the inherent obligation to ensure that personal data handled by both government and private institutions are secured and protected in accordance with the Data Privacy Act of 2012 and consistent with the principles of transparency and access under the Freedom of Information framework.

In line with this, the Development Academy of the Philippines (DAP), in the fulfillment of its mandates on capability building, research, and technical and consulting services, recognizes its responsibility to safeguard all information it collects, processes, and stores. The DAP shall therefore establish, implement, and continuously improve appropriate safeguards and mechanisms to protect personal data in all its operations and engagements.

II. OBJECTIVES

This Policy prescribes general guidelines consistent with the Data Privacy Act of 2012 and related National Privacy Commission (NPC) issuances to ensure: compliance with data protection laws and regulations; safeguarding of the privacy rights of individuals; mitigation of risks associated with data breaches; and promotion of accountability and trust among stakeholders.

It likewise provides institutional measures addressing cybersecurity risks, the use of emerging technologies such as artificial intelligence and the Internet of Things (IoT), and the lawful management of CCTV footage and other forms of visual documentation.

III. DEFINITION OF TERMS

1. **Consent of the data subject** refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic, or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

2. **Closed-Circuit Television or CCTV** refers to closed-circuit television or camera surveillance system in a fixed and stationary location that can capture images of individuals or other information relating to individuals.

3. **Data subject** refers to an individual whose personal information is being processed.

4. **Personal information** refers to any information whether recorded in a material form or not, from which the identity of any 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.

5. **Personal information controller** refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes: a person or organization who performs such functions as instructed by another person or organization; and an individual who collects, holds, processes, or uses personal information in connection with the individual's personal, family, or household affairs.

6. **Personal information processor** refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

7. **Processing** refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data.

8. **Privileged information** refers to all forms of data that are under the Rules of Court and other pertinent laws that constitute privileged communication.

9. **Sensitive personal information** refers to personal information concerning:

    a. an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
    b. 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;

c. 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,

d. Specifically established by an executive order or an act of Congress to be kept classified.

IV. DATA PRIVACY PRINCIPLES

The DAP adopts the following principles in the collection and processing of personal data:

1. **Legitimate Purpose**

   Personal data shall be collected and processed only for purposes declared by the DAP, which must not be contrary to law, morals, or public policy.

2. **Proportionality**

   Collection and processing shall be limited to information necessary to achieve declared and legitimate purposes and shall be retained only as long as required.

3. **Transparency**

   Data subjects shall be informed of the purpose, risks, and safeguards involved in data collection and processing prior to such collection.

V. DATA PROTECTION OFFICER AND TASK FORCE MEMBERS

Pursuant to NPC regulations, the Data Protection Officer (DPO) shall be assisted by the Data Protection Task Force in enforcing and monitoring compliance with data privacy laws within the DAP.

The Task Force shall include focal persons designated from the following offices:

1. Office of the President
2. Legal Services Office
3. Information and Communications Technology Division
4. Human Resource Management and Development Department
5. Office of the Academy Registrar
6. Corporate Operations and Strategy Management
7. Graduate School of Public and Development Management
8. Programs Operations Group
9. DAP Conference Center
10. DAP Sa Mindanao
11. Internal Audit Services

12. Institutional Marketing Center
13. Finance Department
14. Security

VI. IMPLEMENTING GUIDELINES

1. Processing and Collection of Personal Data

All personal data processing activities shall be documented and submitted to the DPO and Legal Services Office. The DPO and Task Force shall maintain adequate records of processing operations, ensure regular monitoring, and convene at least quarterly to review compliance and security safeguards. Only necessary personal data shall be collected, and consent shall be obtained when required by law, evidenced by written, electronic, recorded, or any other practicable means applicable in a given situation.

2. Use of Personal Data

Collected personal data shall be used solely for documentation, reporting, program implementation, and legitimate institutional purposes. The DPO and Task Force shall review, update, and harmonize data management systems across DAP centers and groups to ensure uniform compliance and minimize redundancy.

Personal data collected through survey tools, registration systems, and academic or employment records shall be protected from unauthorized disclosure. The use of official photographs and videos for marketing or external publication shall be coordinated with the Institutional Marketing Center to ensure quality control and proper authorization.

3. Safeguarding and Security of Data

The DAP shall implement organizational, physical, and technical measures to maintain the confidentiality, integrity, and availability of personal data. Minimum standards include: security safeguards for networks and systems against unauthorized access or interference; regular testing and evaluation of data security controls; and assurance of system resilience and recovery capability.

4. Restriction and Opt-out Mechanisms

Participants or clients may restrict the use or disclosure of their personal data by indicating their preference in registration or consent forms. The DAP shall respect such choices and shall not lease, sell, or distribute personal information to third parties, except when authorized by law or with the consent of the data subject.

5. Use of Event Documentation, Photographs, Videos, and Testimonials

a. Documentation materials produced by DAP personnel during project implementation, events, and activities, including photographs, videos, and verbal or written testimonials, may be used by the DAP for internal documentation and reporting purposes, provided that participants are adequately informed beforehand

that such documentation will take place through any of the following: 1) **Registration forms**, 2) clear and visible **notices and signages** in conspicuous places, and 3) **announcements**. Participants must be given a reasonable opportunity to object or to opt out.

b. The DAP may use documentation materials for promotional and publicity purposes in compliance with the Data Privacy Act of 2012 and relevant NPC issuances. For all public DAP events and activities, including those attended by public officials, partners, or members of the general public, the DAP may rely on the lawful basis of legitimate interest, without requiring individual written consent, provided that participants are clearly informed in advance or at the event that photos, videos, and other materials will be taken and may be used for official DAP platforms, publications, or media partnerships, and all other communication channels of the DAP.

c. For private or closed events, the DAP's invitation shall inform/notify the participants/visitors that documentation will take place and that resulting materials may be used for reporting purposes. The same will be reiterated on the event proper.

d. The use and release of CCTV footage shall strictly comply with the Data Privacy Act, its Implementing Rules and Regulations, and the NPC's guidelines on video surveillance. Any publication or sharing of CCTV-derived materials shall follow the same lawful basis, notice, and security requirements applicable to other documentation materials.

e. The Academy shall implement appropriate technical and organizational measures to protect all documentation and visual materials from unauthorized access, use, alteration, or distribution.

f. The Data Protection Officer, in coordination with the Legal Services Office, shall handle any reported misuse, misrepresentation, or unauthorized dissemination of DAP-owned visual materials. Violations or breaches shall be dealt with in accordance with the Data Privacy Act, NPC regulations, and applicable internal disciplinary measures.

6. Data Breach Management

a. All new systems, applications, or processes that involve the collection, storage, or processing of personal data shall undergo a Privacy Impact Assessment (PIA) prior to implementation, while existing systems shall be regularly monitored and subjected to a PIA at least once every year.

b. Only regular employees of the DAP shall be designated to perform functions as Personal Information Controllers (PICs) or processors, and all such designations shall be duly recorded and monitored by the Data Protection Officer.

c. All PIA reports shall be submitted to the Corporate Operations and Strategy Management Office, with copies furnished to the DPO. A consolidated data privacy report shall form part of the annual Management Committee review.

d. When necessary, Data Sharing Agreements (DSAs) shall be executed with external entities to ensure compliance with the Data Privacy Act of 2012 and relevant issuances of the National Privacy Commission.

e. The DAP, through the ICTD and the DPO Task Force, shall ensure that all physical repositories and storage media—whether paper-based or electronic—are properly safeguarded against damage, unauthorized access, loss, or other security risks. Where data is stored in the cloud, the Academy shall exercise due diligence in evaluating and selecting service providers to ensure the safety and security of information.

f. All information systems used for the collection and processing of personal data shall be assessed and tested for integrity and security prior to deployment. Access to such systems shall be limited to authorized personnel through appropriate authentication controls, and regular monitoring and audits shall be conducted to ensure continuous compliance with data protection standards.

g. Any actual or suspected personal data breach shall be immediately reported to the DPO, who shall, within seventy-two (72) hours, notify the NPC in accordance with prescribed reporting requirements. The DPO shall maintain and implement an incident response procedure to ensure prompt containment and resolution of such incidents.

h. Upon confirmation of a breach, the DPO shall convene the Data Breach Response Team (DBRT) to conduct immediate containment, investigation, and mitigation activities. The DBRT shall determine the cause, extent, and impact of the breach, and submit a written report with recommended corrective actions to the DAP President within one (1) month from the occurrence of the incident.

i. The DPO and the DBRT shall regularly review and update all security, breach management, and data protection procedures to strengthen institutional safeguards and prevent the recurrence of similar incidents.

7. Posting

The DAP shall ensure that the most recent and approved version of the DAP Data Privacy and Protection Policy (DPPP), together with the DAP's National Privacy Commission registration details and Seal of Approval, is prominently posted on the official DAP website and other official digital platforms.

A link to the DPPP shall also be included in all mass communications, online registration forms, and similar correspondences transmitted to clients, participants, and partners to promote awareness of the DAP's data privacy practices.

All postings shall clearly display the contact information of the DAP Data Protection Officer to whom data subjects may address inquiries, requests, or concerns regarding the collection, processing, and protection of their personal data.

VII. ACCOUNTABILITY CLAUSE

All DAP officials, employees, and personnel share responsibility for upholding and demonstrating full compliance with the DAP's Data Privacy and Protection Policy. Each individual is accountable for ensuring that personal and institutional data under their custody are collected, processed, stored, and disclosed in accordance with the Data Privacy Act of 2012, its Implementing Rules and Regulations, and relevant NPC issuances.

Any act of negligence, misuse, unauthorized disclosure, tampering, theft, or sale of personal or institutional data, including but not limited to administrative and financial records, institutional permits, student records, personnel files, contracts, and official photographs or video materials, shall be subject to proper investigation and due process.

Violators, whether individuals or groups, shall be held administratively, civilly, and/or criminally liable as may be applicable, and sanctioned in accordance with existing laws, NPC regulations, and DAP's internal disciplinary rules.

EFFECTIVITY

This Memorandum Circular shall take effect immediately upon approval and issuance. It shall remain in force until amended, repealed, or superseded by subsequent directives. All prior issuances, memoranda, or policies inconsistent herewith are hereby repealed or modified accordingly.

LEOCADIO S. SEBASTIAN, PhD, CESO I
Acting President and CEO

dap
PCEO-05321