

June 18, 2020

To: **De La Salle Araneta University (DLSAU) Faculty and Staff**

Fr: **Mr. RONALD IBARLIN**
Director, Human Resource Development and Management

Re: **Data Protection and Social Media Policy**

RATIONALE

At the core of privacy protection are the rights of an individual to know the data maintained on him/her, challenge their veracity and relevance, limit their non-routine use and dissemination, and be assured that their quality, integrity and confidentiality are maintained. It is with this thrust that the Data Privacy Act of 2012, which protects individual personal information in information and communications systems in the government and the private sector, was signed into law. In compliance thereof, the DLSAU Data Protection Policy aptly responds to the requirement and need to protect confidential private and sensitive information that is maintained in the various spheres of the institution.

POLICY

This Data Protection Policy refers to DLSAU's commitment to treat information of Lasallian Partners, stakeholders and other interested parties with utmost care and confidentiality. With this policy, we ensure that we gather, store and handle data fairly, transparently and respectfully towards individual rights.

Further, the policy sets out how DLSAU processes the personal data that it holds relative to students, employees, and third parties. It outlines the school's responsibilities under data protection legislation and regulation, setting out how it will comply, and provides instruction for employees in handling personal data.

SCOPE

The policy applies to all Lasallian Partners (regardless of the type of employment or contractual arrangement), and to the extent practicable, contractors, consultants, and any other external entities that Lasallian Partners collaborate with or act on behalf of DLSAU.

DEFINITIONS

The following are some relevant key terms in the policy:

1. Collection – refers to the process of gathering, acquiring or obtaining personal information from any source, by any means, in circumstances where the individual is identified or is reasonably identifiable.
2. Consent – refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his/her personal data. It 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.
3. Data – refers to any information being processed using equipment operating automatically in response to instructions given for that purpose and that has been recorded with the intention that it should be processed by means of such equipment, or is recorded as a part of a relevant filing system, or with the intention that it should form part of a relevant filing system, or information that does not fall within the previous definitions but forms part of an accessible record.
4. Data Privacy Act – refers to Republic Act No. 10173 or the Philippine Data Privacy Act of 2012, its IRR and any issued and/or subsequent circular memorandum and advisories to be issued by the National Privacy Commission (NPC).
5. Data Protection Officer – refers to the individual assigned by DLSAU to be accountable for its compliance with the DPA, its IRR, and other issuances of the NPC.
6. Data Protection Policy – refers to this Data Protection Policy, which governs the School's practices of handling data. It instructs employees on the collection and the use of the data, as well as any specific rights the data subjects may have.
7. Data Subject -- refers to an individual whose personal information is processed.
8. Information and Communications System – refers to a system for generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or which data is recorded, transmitted or stored and any procedure related to the recording, transmission or storage of electronic data, electronic message, or electronic document.
9. Personal Data – collectively refers to personal information, sensitive personal information, and privileged information.
10. Personal Data Breach – refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

11. Personal Information – refers to any information, whether recorded 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.

12. 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.

13. Privileged Information – refers to all forms of data, which, under the Rules of Court and other pertinent laws, constitutes privileged communication.

14. Privacy Notice – is a statement made to a data subject that describes how DLSAU collects, uses, retains and discloses personal data.

15. 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.

16. Sensitive Personal Information – is information that meets the “personal information” criteria and also reveals race, ethnic origin, marital status, age, health, education, political opinions, religious or philosophical beliefs, among others.

DATA PROTECTION PRINCIPLES

DLSAU is a controller of personal data relating to its past, present and future Lasallian Partners, students, parents/guardians and other members of the school community. It is, therefore, obliged to comply with principles of data protection set out in the Data Privacy Act of 2012 as to how personal information must be treated, which can be summarized as follows:

1. Collected for declared, specified and legitimate purposes only –The school will inform individuals of the reasons for data collection and the uses to which their data will be put. All information is kept with the best interest of each individual in mind at all times.

2. Processed fairly and lawfully – Information on students is gathered with the help of parents/guardians and Lasallian Partner. Information is also transferred from their previous schools. In relation to information DLSAU holds on other individuals (Lasallian Partner, individuals applying for positions within the school, parents/guardians of students, etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the school.

3. Accurate, relevant and up to date – Students, parents/guardians, and/or Lasallian Partner should inform the school of any change which the school should make to their personal data and/or sensitive personal data to ensure that the individual's data is accurate, relevant and up-to-date. Once informed, the school will make all necessary changes to the relevant records. Records must not be altered or destroyed without proper authorization.

4. Adequate and not excessive in relation to the purposes for which they are collected and processed – Only the necessary amount of information required to provide an adequate service, conduct business, and discharge responsibilities will be gathered and stored. It will also be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: Provided, That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: Provided, further That adequate safeguards are guaranteed by said laws authorizing their processing.

5. Retained only for as long as necessary – As a general rule, personal information will be kept for the duration of the individual's time in the school. The school may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and/or defending a claim under employment legislation and/or contract and/or law.

RIGHTS OF DATA SUBJECTS

DLSAU shall process data in line with the data subject's rights stipulated under the Data Privacy Act of 2012 as follows:

1. Be informed whether personal information pertaining to him or her shall be, are being or have been processed;
2. Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:
 - a. Description of the personal information to be entered into the system;
 - b. Purposes for which they are being or are to be processed;
 - c. Scope and method of the personal information processing;
 - d. The recipients or classes of recipients to whom they are or may be disclosed;
 - e. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;

f. The identity and contact details of the personal information controller or its representative;

g. The period for which the information will be stored; and

h. The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

i. Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification of data subject: Provided, That the notification under subsection (b) shall not apply should the personal information be needed pursuant to a subpoena or when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of legal obligation;

3. Reasonable access to, upon demand, the following:

a. Contents of his or her personal information that were processed;

b. Sources from which personal information were obtained;

c. Names and addresses of recipients of the personal information;

d. Manner by which such data were processed;

e. Reasons for the disclosure of the personal information to recipients;

f. Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;

g. Date when his or her personal information concerning the data subject were last accessed and modified; and

h. The designation, or name or identity and address of the personal information controller;

4. Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: Provided, That the third parties who have previously received such processed personal information shall be informed of its inaccuracy and its rectification upon reasonable request of the data subject;

5. Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information; and

6. Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

GUIDELINES

The following guidelines are hereby set to secure data whether in transit or at rest:

1. Use of Information Systems

a. Data must be protected against divulgence to unauthorized recipients. File access control schemes must be observed by Lasallian Partners involved in data processing to create a protective barrier between a user and data files to which he is not authorized while permitting access to those which he is.

b. All Lasallian Partners shall be required to sign a Non-Disclosure Agreement which fully details their duty of confidentiality pertinent to the personal data shared to them and to which they are exposed.

i. Operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.

ii. Not make use of and reproduce personal data, except for the purpose required by their specific job functions.

iii. Not share personal data to any person or entity, except as allowed by data sharing agreements or applicable laws.

iv. Take such steps as are reasonable to preserve the confidentiality of personal data.

d. Records must be maintained with sufficient accuracy, completeness, timeliness, and pertinence as is relevant to their intended use.

e. The Lasallian Partner's duty of confidentiality remains as a continuing obligation to DLSAU for an indefinite period and extends beyond any termination of his/her employment period or contract.

f. In circumstances where consent is needed, the Lasallian Partner assigned shall obtain the explicit consent of the data subject as evidenced by any of the following modes: written,

electronic or recorded means, subject to the rules on authentication provided under existing laws and regulations e.g., the DPA, the Rules of Court and the Rules on Electronic Evidence. Such consent must be time- bound in relation to the declared, specified and legitimate purpose. When necessary, the Lasallian Partner shall provide data subject a mechanism through which they can subsequently rescind the permission(s) earlier provided and opt- out.

2. DLSAU Social Media Policy:

- a. Maintain professionalism and awareness of the audience in the exercise of the freedom to navigate and use any social media platform.
- b. Secure consent before posting any pictures or videos of DLSAU Students or fellow Lasallian Partners online.
- c. Refrain from sharing assessment results or any data and/or record of students or fellow Lasallian Partners in social media.

3. Dealing with a Data Access Request

- a. Individuals are entitled to a copy of their personal data upon a written request.
- b. A Lasallian Partner or stakeholder requesting over the phone to be furnished a copy of a personal data or document maintained on him/her must be redirected to put such request in writing, fill out a form or send an email as the appropriate protocol.
- c. The request must be responded to within a reasonable or specified time whilst observing holiday periods. The necessity of an extension must be duly explained to the requesting party.
- d. No personal data can be supplied to another individual apart from the data subject unless verified identity and authority exist.

4. Telecommuting

In compliance with the DLSAU Telecommuting Policy:

- a. Create a secure connection by setting up multi-factor authentication wherever possible to avoid data breaches.
- b. Do not use unsecured Wi-Fi or Bluetooth; a public Wi-fi network or Bluetooth is inherently less secure.
- c. Identify a specific and safe work area at home.
- d. Secure computers and/or devices from children and other family members.

e. Should a need to leave home arise, shut down or lock computers and/or devices.

5. Workplace Monitoring and Surveillance

a. Monitoring shall only be carried out to the extent necessary to deal with the legitimate academic and proprietary functions and/or purposes of DLSAU.

b. Personal data collected in the course of the monitoring shall be kept to an absolute minimum, by means that are fair under the circumstances, and be used for purposes consistent with, or directly related to, the purposes for which the monitoring was introduced.

c. Recorded information contained on CCTV footages should be routinely erased within 30-90 days. Although different circumstances may necessitate different retention periods, a shorter period should also be considered, e.g. if viewing of the recorded information reveals no incident or no incident is reported after a certain period.

d. Where the school has a reasonable cause to suspect that unlawful activities are taking place in the workplace, e.g. theft of school confidential data by any Lasallian Partner, and it may not be feasible using overt monitoring or other reasonable measures to obtain conclusive evidence that would identify the culprit/s concerned, the school may consider covert monitoring for the purpose of so doing, and for no other purpose. After which, the covert monitoring shall immediately cease.

6. Disciplinary Consequences

To establish accountability, DLSAU reserves the right to levy disciplinary actions for non-compliance, up to and including termination for violations of the Non-Disclosure Agreement and/or this Data Protection Policy.

EVALUATION

This policy shall be reviewed six (6) months after implementation and annually thereafter. Effectiveness of the policy shall be assessed through:

1. Review of the policy by November 10, 2020 as led by the Data Protection Officer to determine if objectives have been met and to identify barriers and enablers to ongoing policy implementation.
2. Feedback from Lasallian Partners

INFORMATION DESSIMINATION

Unit/department heads shall provide a copy of this memorandum to all of his/her team (permanent, probationary full-time, part-time and consultants).

Thank you! Animo La Salle Araneta!

Noted:

(Officially Signed) June 18, 2020
MR. CHRISTOPHER POLANCO
University Chancellor

(Officially Signed) June 18, 2020
DR. BJORN SANTOS
University President