Data Privacy Council Education Sector Advisory No. 2020-1
Data Privacy and Online Learning

I. General Provisions

A. Purpose

This document aims to guide schools and other educational institutions, as well as other stakeholders in the education sector, in their efforts to ensure adequate data protection in the conduct of online learning and other related activities.

B. Nature and Scope

This document is meant to be a set of recommendations and shall not be treated as some type of policy. Each educational institution retains the prerogative to decide on the measures it shall deem appropriate for its context. It may define, adopt, and implement its own data protection policies that seek to protect personal data under its control or custody.

While this document covers different areas relevant to online learning, it is not intended to be an exhaustive list of such concerns. Neither does it include issues which, while related to online learning, do not involve the processing of personal data.

This Advisory may be updated periodically, as the need arises.

C. Definitions

Whenever used in this document, the following terms shall the have their corresponding meanings provided here:

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 his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so.
2. "Data Privacy Act of 2012" or "DPA" refers to Republic Act No. 10173 (AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND

COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES).

3. "Data processing systems" refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing;
4. "Data sharing" is the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor;
5. "Data subject" refers to an individual whose personal, sensitive personal, or privileged information is processed;
6. "Learning Management System" or "LMS" refers to a software application for the administration, documentation, tracking, reporting, automation and delivery of educational courses, training programs, or learning and development programs.
7. "Social Media refers" to interactive computer-mediated technologies that facilitate the creation or sharing of information, ideas, career interests and other forms of expression via virtual communities and networks.
8. "Personal data" refers to all types of personal information as defined under the DPA.
9. "Personal information" or "PI" refers to 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.
10. "Personal information controller" or "PIC" refers to 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.
11. "Personal information processor" or "PIP" 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.
12. "Privileged information" refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.
13. "Sensitive personal information" or "SPI" refers to personal information:
    a. About an individual, race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
    b. About an individual, 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.

D. Key Points and Principles

When conducting personal data processing activities deemed necessary or related to online learning, the following points and principles shall be observed to greatest extent possible:

1. *Accountability*. An educational institution is accountable for all the personal data it collects and processes. This obligation subsists even in the following conditions:
    a. It outsources or subcontracts its personal data processing activities
    b. It has properly obtained the consent of its students (or their parent or legal guardian, in the case of minors).
2. *Information about Education as Sensitive Personal Information.* According to the DPA, information about education is SPI. As such, its processing is generally prohibited. It may only be processed in specific circumstances provided in the law (*see*: Section 13, DPA):
    a. when the data subject has given consent
    b. when the processing is provided by applicable law or regulations, that afford adequate data protection
    c. when processing is necessary to protect the life or health of the data subject or another person, and the data subject is unable to give consent
    d. when processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations. However, processing must be confined only and related to the bona fide members of such organizations or associations. The information must also not be transferred to third parties, and the affected data subjects must have given their consent prior to processing.
    e. when processing is necessary for purposes of medical treatment. However, such treatment must be performed by a medical practitioner or a medical institution, and an adequate level of data protection is ensured.
    f. when processing involves information necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings
    g. when processing involves information necessary for the establishment, exercise, or defense of legal claims
    h. when the information is to be provided to government or a public authority pursuant to a constitutional or statutory mandate.
3. *Legitimate Interest*. In order for legitimate interest to be an appropriate basis for the lawful processing of personal information, the following three-part test must be met:
    a. Purpose Test – Does the processing have a legitimate interest or purpose?
    b. Necessity Test – Is the processing necessary to achieve such interest or purpose? Is there a less intrusive way to achieve the purpose?
    c. Balancing Test – Is such interest or purpose not overridden by the concerned individual's rights and freedoms?

    For additional guidance on this matter, refer to the following NPC Advisory Opinions: (i) NPC Advisory Opinion No. 2018-020; (ii) NPC Advisory Opinion No. 2018-050; (iii) NPC Advisory Opinion No. 2020-006
4. *Legitimate Purpose.* The processing of personal data must have a declared and specified purpose that is not contrary to law, morals, or public policy. (*see*: Section 11(a), DPA)
5. *Proportionality*. The processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to its declared and specified purpose. It shall only

be undertaken if the purpose thereof cannot be reasonably fulfilled by other means.(*see*: Section 11(d), DPA)

6. *Transparency*. An individual must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of the PIC, his or her rights as a data subject, and how these rights can be exercised. Any information and communication relating to the processing of personal data must be easy to access and understand using clear and plain language.(*see*: Section 11, DPA)

II. Areas of Concern

A. On the use of a Learning Management System and Online Productivity Platforms

1. Where an educational institution has officially adopted a particular Learning Management System (LMS) or Online Productivity Platforms (OPP), all activities pertaining to online learning should, to the extent possible, be conducted via such a platform.
2. Where the official LMS or OPP adopted by an educational institution is its own (i.e., it has developed), the educational institution shall make sure it has adequate data protection features and is governed by an appropriate policy and/or manual.
3. Where the official LMS or OPP adopted by an educational institution is owned and/or provided by a third party, its use should be covered by a Data Processing Outsourcing Agreement, or any equivalent document. For this purpose, the presence or insertion of standard data protection clauses in the contract between the educational institution and the LMS or OPP provider and/or the terms and conditions governing the use of said LMS or OPP may be deemed sufficient (*see also*: NPC Advisory Opinion No. 2020-018).
4. An announcement or posting that involves personal data (e.g., grades, results of assignments, etc.) should be made in a manner that only makes it viewable by its intended recipient/s. For instance, exam results should be given on an individual basis and not released en masse even if the students belong to the same class.
5. Downloading of personal data stored in the LMS or OPP should be kept to a minimum and/or limited to that which is necessary for online learning. Ideally, a policy should determine what is necessary for such purpose. In line with this, it is also important that any downloaded data be retained only until there is a legitimate need for such offline copy. This, too, may be covered by an appropriate policy.
6. There should be mechanisms in place so that submissions (e.g., assignments, projects, etc.) may be carried out in a safe and secure manner. Submissions via social media platforms are discouraged since these platforms were never designed for such purpose.
7. Exercise caution when integrating applications, tools, and other services to an LMS or OPP. They may introduce vulnerabilities to an otherwise secure system. A Privacy Impact Assessment may be undertaken by a multidisciplinary team before formalizing any planned

integration. The team shall review key areas such as security, data protection, compatibility, and administration.

B. On other available unofficial supporting tools for online learning

1. The use of tools or technologies for online learning that have not been officially adopted by an educational institution (i.e., there is no formal relationship between the institution and the developer of these tools) should be limited. Since no active effort has been made to make sure there is adequate protection in their use, the security of any personal data processed through them may be suspect—or worse, nonexistent.
2. If or when these tools are being evaluated in terms of the level of protection they provide to personal data uploaded to them or processed through their use, an educational institution may determine if they are covered by any industry-accepted certification or third party audit report, such as:
    a. Philippine National Standards (PNS) ISO/IEC 27001:2018 Information technology - Security techniques - Information security management systems
    b. PNS ISO IEC 27018:2015 Information technology - Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
    c. PNS ISO/IEC 29100:2019 Information technology – Security techniques – Privacy framework (equivalent of NIST's Privacy Framework)
    d. ISO 27701:2019 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
    e. SOC2 - System and Organization Controls (SOC) Type 2 - Trust Services Criteria
    f. HECVAT - Higher Education Community Vendor Assessment Toolkit
3. The geographical location of the developer or provider of an online tool or platform (including its data centers) as well as the governing laws in said jurisdiction should also be considered as part of the evaluation. While the DPA has extra-territorial application, its enforcement may be rendered impossible or at least extremely difficult, depending on said location and the laws therein.
4. Ideally, a Privacy Impact Assessment (PIA) should be conducted prior to the use of these tools in order to determine the level and type of attendant risks. The PIA should include a proper Personal Data Inventory.

C. On the use of social media

1. All personal data posted on social media are considered public by nature unless appropriate privacy tools and settings made available by the platform are properly utilized. (*see*: Vivares vs. St. Theresa's College, GR No. 202666, September 29, 2014). NOTE: While the DPA was already in force when this decision came out, the law was not consulted by the Supreme Court presumably since the events that led to the case occurred before the law was enacted.). However, this does not mean they can be used or processed by any person or entity for any purpose or reason. Their processing must still comply with the DPA.

2. Posting or sharing of personal data (e.g., photos, videos, etc.) on social media must always have a legitimate purpose. Such purpose, along with the type of personal data involved, often determines whether or not the consent of affected data subjects is necessary prior to such posting or sharing.
3. Even when posting of personal data is determined to be allowed:
    a. the numerous risks inherent in social media platforms should still be properly appreciated. Adherence to the principles of legitimate purpose and proportionality is encouraged at all times.
    b. it must be carried out using only authorized or official social media accounts of the educational institution (or any of its units or offices). There should be appropriate rules or protocols governing the use of these official accounts.
4. If personal data is posted on social media as a course requirement, the lifespan of such data usually coincides with that of the course. Thus, once the course has concluded, it means the lifespan of the data will have also elapsed. It must then be removed or deleted, unless there is some other lawful basis for keeping it online.
5. If personnel of an educational institution have collected personal data in their official capacity and/or during an official activity, such data must not be used for personal purposes or reasons. The posting of such data using personal social media accounts may be a violation of the educational institution's social media policy, if any, and could merit disciplinary action. On the other hand, if they have collected personal data in their individual or personal capacity, but then decide to use it for work-related purposes, they should first ask permission from the affected data subjects in accordance with the principles of fairness and transparency.

D. Publication of information or files in via other means or platforms

Personal data (including the files or records that contain them) stored or uploaded to an LMS or OPP may be covered by a number of legal or technical requirements (e.g., confidentiality, access restriction, retention, and even intellectual property laws). As such, publicly disseminating, reposting, or resharing them may run afoul of not just the DPA but also other applicable laws and regulations. Extreme care must be exercised when handling them. Consulting the appropriate offices and, when necessary, securing consent or authorization is strongly advised before any of the foregoing actions are taken.

E. On the storage of personal data

1. Ideally, all personal data collected during the conduct of an online course should be stored in the LMS or OPP adopted by the educational institution in order to ensure adequate data protection measures are in place. If they will be collected outside of the LMS or OPP, proper data protection and data governance policies should be developed for such purpose. These policies should preserve the confidentiality, integrity, and availability of the data.
2. Storing of personal data collected as part of the conduct of a class in a personal account or device should be avoided or at least kept to a minimum in order to minimize the risk of unauthorized use or access. Official educational institution accounts typically include access

to official storage facilities. Personal data collected via official activities should be kept in such facilities so that they stay within the official work environment of the concerned institution.

3. Unless some other lawful basis for their continued retention exists, personal data should be disposed of securely when the declared purpose for its collection and processing is no longer valid.

F. On the use of webcams and the recording videos of online discussions

1. Whenever possible, the use of webcams in synchronous online classes or sessions should be optional.
2. When the education institution is considering the recording of these online classes or discussions, the principles of *Legitimate Purpose* and *Proportionality* should be primary considerations. Among the legitimate uses of recorded sessions could include:
    a. Review of the lecture presentations (e.g. slides) and ensuing class discussions at a later time.
    b. Viewing by students (and/or their parents) who are unable to attend, subject to appropriate school protocols.
3. Where consent is necessary for the recording of these classes or sessions (as determined by attendant circumstances) and the data subject is a minor, consent must be obtained from the parent, legal guardian, or any other person validly exercising parental authority over the child. and consider having the legal guardian or parent present.
4. When the student is a minor, consider having the parent or legal guardian present during these recorded classes or sessions.
5. Posting the recorded classes or sessions or making them available on public platforms (e.g., social media, school website, etc.) must also adhere to the principles of *Legitimate Purpose* and *Proportionality*. Individuals who may be affected thereby must have been informed beforehand of the school's intention to make the recording public. Depending on the nature of the recording, prior approval of said individuals may also be necessary.
6. Educational institutions should establish a policy or guidelines governing the use of webcams and the recording of online classes or sessions. Such policy should take into account not only its legitimate interests, but also individual privacy rights. It should also address the possible recording and use of such classes or sessions by the participants themselves.

G. Online proctoring

1. When determining the propriety of carrying out online proctoring, the principles of *Legitimate Interest* and *Proportionality* should be key considerations. Specifically, the interests of the students should be weighed against those of the educational institution in order to ascertain the appropriate balance. A similar approach must be taken when looking at the invasive nature of online proctoring and the legitimate aim it seeks to achieve.

2. Explicit consent of the student (or parent or legal guardian, in the case of minors) should be obtained prior to the conduct of online proctoring and the use of related tools or technologies.
3. In carrying out online proctoring, take note of the following critical data processing activities:
    a. The tool or technology to be used may request for the installation of software such as a secure browser or a plugin to a browser.
    b. The tool may also require access to scan the computer for processes that are running and the number of monitors currently connected.
    c. The tool may perform various forms of verification or identification processes, including the taking of images of the student and the venue or room where the exam will be taken.
    d. The session may be recorded for the entire duration of the exam and automated processing techniques may be incorporated to detect potential cheating behavioral patterns from the student.
4. To the extent possible, human-based evaluation should still be included as a secondary validation process for any or all data processed in the course of or as a result of automated proctoring.

H. Data Security

To ensure proper protection of personal data, refer to the following resources published by the NPC:

1. FAQs on Data Security
2. 30 Ways to Love Yourself Online: A Beginner's Guide to Personal Data Privacy
3. NPC COVID-19 Bulletins
4. Data Breach Prevention
5. NPC Advisory No. 2020-02: Guidelines on the use of videoconferencing technology for the remote appearance and testimony of parties before the National Privacy Commission