Republic of the Philippines
Department of Education
OFFICE OF THE UNDERSECRETARY
Tanggapan ng Pangalawang Kalihim

MEMORANDUM
OU-LAPP No. Q-231, s.2021

FOR : **Undersecretaries**
Assistant Secretaries
Bureau and Service Directors
Regional Directors
Schools Division Superintendent
Heads of Public and Private
Elementary and Secondary Schools
Others Concerned

FROM : **TONISITO M.C. UMALI, Esq**
Undersecretary
DepEd Data Protection Officer

SUBJECT : **NATIONAL PRIVACY COMMISSION**
PUBLIC HEALTH EMERGENCY BULLETIN NOS. 16 and 17

DATE : 16 March 2021

Enclosed for guidance and ready reference are **Public Health Emergency Bulletins No. 16: *Privacy Dos and Don'ts for Online Learning in Public K-12 Classes* and No. 17: *Update on the Data Privacy Privacy Best Practices in Online Learning*** from the National Privacy Commission (NPC) dated 5 October 2020 and 16 February 2021 respectively. These NPC Bulletins may also be accessed through the following link: www.privacy.gov.ph.

These Bulletins are being issued with the end in view of addressing the various data privacy concerns in online learning. It is hoped that these Bulletins may serve as a practical guide in upholding the data privacy rights of our learners and teachers during the conduct of effective online learning.

Immediate and wide dissemination of this memorandum is desired.

Encl: As stated

Undersecretary Tonisito M.C. Umali, Esq.
Legislative Affairs, External Partnerships, and Project Management Service
R-104 Rizal Building, DepEd Complex, Meralco Avenue, Pasig City
Telephone No. (02)8633-7224 ; Fax No: (02)8633-1940 ; Email: tonisito.umali@deped.gov.ph

NPC PHE Bulletin No. 16
Privacy Dos and Don'ts for Online Learning in Public K-12 Classes
October 1, 2020: 11:08 AM GMT+0800 | Last Edit: October 5, 2020

As public K-12 classes nationwide are set to open in October, students, parents, guardians, teachers and schools would do well to heed guidelines on online learning that list dos and don'ts aimed at safeguarding sensitive personal information of pupils.

Issued by the Data Privacy Council for the education sector and the National Privacy Commission (NPC), the guidelines cover areas, such as online decorum, learning management systems, online productivity platforms, social media, storage of personal data, webcams and recording videos of discussions, and proctoring.

Listed are the dos and don'ts for online learning in K-12 classes:

For students
DOs

- Creating strong passwords when signing up on e-learning platforms. Passwords should be at least 12 characters containing upper- and lower-case letters, numbers, and, if possible, symbols.
- Staying alert during online classes, especially when sharing videos, photos, and files.
- Using customized backgrounds to avoid accidental disclosure of personal information.
- Installing and regularly updating an anti-virus program.
- Muting the microphone and turning off the camera by default, especially when not speaking or reciting.
- Turning off the microphone and camera when leaving one's station for, say, bathroom breaks.

DON'Ts

- Connecting phones, laptops, and other gadgets to free or public Wi-Fi networks. (In unavoidable circumstances, ensure that the public network has a password and is not accessible to everyone.)
- Sharing submissions for an unlimited time. (When the content no longer needs to be shared, delete it.)
- Sending assignments, projects and other requirements to teachers via social media.
- Taking screenshots of the video feed of teachers and classmates.
- Spamming the chat.
- Giving out online links and their passwords to people who should not be in the class.

For parents or legal guardians

DOs

- Helping the child or ward check and customize privacy settings of the device or application for online learning.
- Teaching them basic online security (e.g. enabling two-factor authentication and avoiding sharing homework, passwords, and other personal information even with friends).
- Taking a moment to peruse the school's privacy policy.
- Ensuring that your consent is obtained for the recording of classes. Consider being present during these sessions, especially if the student is a minor.

DON'Ts

- Leaving the child, especially minors, unsupervised during the conduct of online learning.

For teachers

Teachers must always consider the privacy, equity, & peculiarity among students when conducting online classes:

- **Privacy**
  Students might feel uncomfortable displaying their living space to their peers. Family members might not want their image or video to be captured.
  Students might also take a screenshot of their classmate's video feed, which is prone to cyberbullying and privacy issues.
- **Equity**
  Not all students have reliable internet access. Some might have low bandwidth, cannot afford to stream videos, or have limited access to digital devices.
- **Peculiarity**
  Some students might feel shy or anxious on camera, affecting their performance in class.

DOs

- Making webcam use optional in online classes.
- Recording online classes as long as it has legitimate uses (e.g. review the lecture presentations and viewing by students who are unable to attend).
- Considering the principles of legitimate interest and proportionality during online proctoring, in which a student's test duration is monitored using a webcam, microphone, or accessing the student's screen. Weigh the interests of the students against those of the educational institutions to determine the appropriate balance.
- Obtaining the explicit consent of the student (or parent/legal guardian for minors) before the conduct of online proctoring.
- Letting students decide whether they would turn on the cameras of their devices. They should be permitted to use virtual backgrounds and fun filters.
- Asking questions regularly to assess students' understanding. Allow them to respond through audio or the videoconferencing app's chat and features, such as polls and nonverbal actions (e.g. thumbs up), instead of requiring them to turn on their cameras.

DON'Ts

- Posting announcements that involve personal data, such as grades and results of assignments. For example, exam results should be given on an individual basis and not released en masse.
- Allowing students to submit projects and assignments via social media platforms.
- Storing personal data collected as part of the class in a personal account or device.
- Correlating student's use and eye contact with participation, grading and attendance (e.g. giving students plus points if their cameras are on).
- Removing students from the class or forcing them to turn their cameras on.

For schools

DOs

- Adopting a particular learning management system (LMS) or online productivity platforms (OPP) where all activities pertaining to online learning should be conducted.
- Ensuring that the LMS or OPP has adequate data protection features.
- Informing students before collection about the personal data to be processed and the reasons using timely, age-appropriate, clear and concise language.
- Exercising caution when integrating apps, supporting tools and other services with an LMS or OPP, as these other services may come with vulnerabilities.
- Being familiar and up to date with all privacy-related trends. This will be of help in crafting data policies that meet the level of protection students need.
- Referring to NPC resources to ensure proper protection of students' personal data.
- Forming a data breach response team responsible for creating and implementing an incident-response procedure.
- Establishing policies and implementing them effectively to prevent or minimize breaches and to ensure timely discovery of a security breach.
- Conducting and investing in security audits and tests, such as privacy-impact assessment source-code audit, vulnerability assessment and penetration testing.
- Strengthening systems against prominent web attacks.

  A well-structured system, including both the front-end and back-end, ensures the protection of data against common web attacks.
  - The vulnerabilities found in the conduct of audits and tests must be fixed first before the system is used further.
  - It is important to secure the communication between a user's browser and the school website site to add another layer of protection to the system.
- Updating systems and their components.
  - The security and privacy vulnerabilities yesterday may not be the same today.
  - Make a conscious effort to continuously improve or update systems and implement best practices in configuring or hardening them (e.g., database encryption at rest, encryption in transit, network access controls, data access controls and audit logs).
  - Install a web application firewall to deter distributed denial of service attacks.
- Backing up data.

  When conducting regular maintenance like a system update, upgrade or configuration, run a full backup of the school website.

  A full backup must follow the system documentation consistently and obtain a

clearance from an accountable officer in the school, such as the Data Protection Officer.

Online backups are also a convenient way to ensure an accessible copy of the website when the need arises. The "3-2-1" strategy can be used:

- 3 total copies of the data
- 2 copies are local but on different mediums
- 1 copy is offsite, which may be geographically separated or in an online cloud computing platform

- Migrating to the cloud is an option.

  Use of cloud computing services reduces capital expenses like housing and maintaining the school's data centers with servers, storages and other ICT active components.

  In addition, the cloud eliminates the tedious task of upholding the security of the school infrastructure. The cloud service provider does that for the school.

  However, keep in mind that proper security and routine maintenance of the web application that runs in the cloud is the school's full responsibility.

DON'Ts

- Keeping personal data longer than their intended purpose. (Set retention periods and employ mechanisms for frequent purging of messages or interactions between teachers, students and parents.)

***

NPC PHE Bulletin No. 17
Update on the Data Privacy Best Practices in Online Learning
February 16, 2021 | 4:13 PM GMT+0800 Last Edit: February 16, 2021

As schools remain constrained to conduct blended learning in lieu of face-to-face classes due to the risks of the COVID-19 pandemic, various inquiries were received from stakeholders on the conduct of synchronous online classes and other related matters.

The National Privacy Commission, in its continuing efforts to provide responsive advice and guidance, underscores the need to balance effective teaching and learning online while upholding data privacy rights.

The Commission recognizes the efforts of the online/blended/synchronous learning mechanisms with the aim of simulating what is supposed to be happening in an actual physical classroom pre-pandemic, to somehow call to mind a sense of normalcy for education. However, we must be reminded that there is considerable difference in context as learners are at home and that this structure cannot fully compare to what happens in an actual physical classroom.

With this, the Commission had dialogues with regulators such as the Department of Education and Department of the Interior and Local Government, to gather inputs on the actual experiences of learners, educators, schools, and parents since the school year started, to help assess and adequately address the concerns raised in order that learning can be better facilitated.

Taking into account that the conduct of synchronous online classes is considered the best substitute for face-to-face classes based on existing research and studies on the matter, below are the some of the recommended practices which may be implemented:

1. Schools should create policies or guidelines on the use of cameras for the conduct of online classes and examinations, as may be reasonable and necessary to supervise and monitor learners and help educators in teaching. Opening of cameras during synchronous learning is not prohibited.

   Policies or guidelines should also be considered on the following:

   a) Encourage the use of virtual backgrounds whenever possible to avoid displaying private living spaces.
   b) Consider equality and fairness in situations if learners experience technical difficulties, limited internet connection, device malfunctions, glitches on the online platforms and other analogous circumstances, and determine the alternative ways to monitor online classes and examinations in these situations.

2. Schools should likewise improve existing student codes of conduct, handbooks, or similar internal policies or rules to adequately regulate student behavior during online classes. Schools must remind learners that the screen capturing, sharing, posting in social media, or any other similar kind of processing of chats, images, videos, and sounds

involving their classmates and teachers during online classes may be subject to data privacy and other related regulations.

3. Schools should strictly enforce their social media policy. Educators and other school personnel who may have collected personal data in their official capacity and/or during an official school activity must be reminded that the same cannot be used for personal purposes, i.e., posting in their personal social media accounts.

4. Online classes may be recorded for purposes of viewing by learners who may have missed a particular class, subject to existing school policies on attendance. The same recording may likewise be used by the school and educators for training purposes. It is best that learners and/or parents and guardians are informed beforehand of this processing activity.

5. Submissions of assignments and other school requirements may be done through available online messaging applications on a case-to-case basis, considering the circumstances of the learner and/or educator. But this should be done in a manner where the submissions are sent directly to the appropriate teacher or school personnel and not to be made publicly available.

6. Educators and school personnel are reminded that communications involving personal data such as exam grades, results of assignments, report cards, reminders on unpaid school fees, etc. should be sent directly to the concerned recipient/s only and should never be posted in a manner that can be accessed or seen publicly.

7. All policies, guidelines, or codes, where the same would involve the processing of personal data, should always adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality. The best interests of the learner shall be of paramount consideration.

8. The above recommendations should be read together with the requirements of existing child protection policies and anti-bullying policies, as necessary and appropriate.

***

To: All School Administrators, Principals & Teachers In-Charge
(Elementary & Secondary)
FOR YOUR INFORMATION & APPROPRIATE ACTION

MARIE CAROLYN B. VERANO, CESO V
Schools Division Superintendent