Republika ng Pilipinas
KAGAWARAN NG KATARUNGAN
Department of Justice
Manila

DEPARTMENT OF JUSTICE
OFFICE OF CYBERCRIME
22 September 2020

PUBLIC ADVISORY
ON THE CONDUCT OF ONLINE CLASSES USING VIDEO CONFERENCING SERVICES

This Public Advisory is issued by the Department of Justice (DOJ) – Office of Cybercrime (OOC) in response to the emerging security risks associated with the utilization of various video conferencing services in the conduct of online classes in the midst of the COVID-19 pandemic.

Pursuant to Republic Act (R.A.) No. 11480, which amended R.A. No. 7797, the Department of Education (DepEd) announced the decision of President Rodrigo R. Duterte to defer the school opening for School Year (SY) 2020-2021 from 24 August 2020 to 05 October 2020, as recommended by the Secretary Leonor Magtolis Briones. This is in response to the implications of imposition of various levels of community quarantine in Metro Manila and in the provinces of Cavite, Bulacan, Laguna, and Rizal.[1]

On 15 August 2020, the DepEd also clarified that private or non-DepEd schools that have already started their classes, or are scheduled to start classes ahead of the aforesaid period, are allowed to proceed provided they are strictly using only distance learning modalities and that there are no face-to-face classes. Hence, the adoption of distance learning modalities through the use of various video conferencing services by the educational institutions.

While video conferencing services open doors to new opportunities that make access to education easy, application of information and communication technology in the conduct of online classes can cause many security risks, such as loss of confidentiality, availability, and integrity of computer data, as well as the exposure of students to abusive strangers and harmful online contents.

Every effort shall be exerted to promote the welfare of children and enhance their opportunities for a useful and happy life[2]. Children should also be protected from all types of child abuse including psychological and physical abuse, neglect,

---

[1] Department of Education's Official Statement on the Opening of Classes, 15 August 2020. Accessed on 17 September 2020. https://www.deped.gov.ph/2020/08/14/official-statement-on-the-opening-of-classes/.

[2] Section 2, Republic Act (R.A.) No. 7610.

Reproduction No. 106, S. 2020

cruelty, sexual abuse and emotional maltreatment[3], or any act by deeds or words which debases, degrades or demeans their intrinsic worth and dignity as a human being[4]. Republic Act (R.A.) No. 7610 or the "Special Protection of Children Against Abuse, Exploitation and Discrimination Act" provides sanctions against those who abuse, exploit or discriminate against children.

In order to prevent similar incidents from happening and to ultimately protect children from online abuse and harmful contents during online classes, the DOJ-OOC hereby issues the following advisories:

A. FOR SCHOOL ADMINISTRATORS

1. **NEVER share meeting room credentials, both the ID and Password, to the public.** Make it a habit to provide this information only to the registered students and their parents. Another good practice would be sending the Meeting ID and Password in a separate communication.

2. **ALWAYS set meeting configurations as follows:**

   a. Accept participants' request to join meeting individually.
   b. Provide a standard naming instruction for the participants, *e.g.*, SURNAME, First Name, Middle Initial.
   c. Start meeting with participants' video off.
   d. Require a password from the participants.
   e. Mute participants upon entry.
   f. Disable desktop/screen share for participants who are not assigned in the virtual meeting room as host/s.

3. **DO NOT set meeting configurations as follows:**

   a. Allow participants to join before the host.
   b. Allow participants to rename themselves.
   c. Allow participants to send message to one another.
   d. Allow participants to access the file transfer.
   e. Allow participants to share their screens.
   f. Allow participants to use annotation tools to add information to shared screens.
   g. Allow participants to share whiteboard during a meeting.
   h. Allow users to replace their background with any selected image.

4. **NEVER leave students alone in a virtual classroom.** Make sure that a school administrator is always present to supervise the activities in a virtual classroom.

5. **ALWAYS update the application you downloaded to its latest version.** Every service/application connected to the internet is vulnerable to cyber-attacks. It is crucial that users regularly update their apps once it is

[3] Section 3 (b) (1), R.A. No. 7610.
[4] Section 3 (b) (2), R.A. No. 7610.

available. These software updates usually include patches to the app's reported vulnerabilities.

B. FOR PARENTS

Parents are encouraged to promote and implement proper netiquettes to be observed by children under their supervision. In the case of ***Vivares, et al. v. St. Theresa's College, et al.***[5], the Supreme Court ruled that there's no substitute for parental involvement and supervision when it comes to digital literacy and good cyber citizenship, to wit:

> "Considering the complexity of the cyber world and its pervasiveness, as well as the dangers that these children are wittingly or unwittingly exposed to in view of their unsupervised activities in cyberspace, the participation of the parents in disciplining and educating their children about being a good digital citizen is encouraged by these institutions and organizations."

Parents and guardians should conscientiously guide their children and wards, respectively, in their online activities, especially during online classes. This includes their capacity to teach them how to discern information online and to provide guidance on how to implement safety measures to prevent becoming a victim of cybercrimes.

Equally important is to let the children know by heart what digital literacy and digital citizenship mean. "Digital literacy" is the ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills[6], while "digital citizenship" refers to the norms of appropriate, responsible behavior with regard to technology use[7]. Understanding and teaching the philosophy behind these concepts to the children will empower them with the required insights and know-how to help them navigate the web both safely and effectively[8].

It is, thus, incumbent upon the parents and guardians to instill to their children and wards, respectively, the exercise of due diligence in their online dealings and activities.

C. FOR THE PUBLIC

Report any irregularities or unwanted incidents during online classes to the appropriate enforcement agencies. If a participant encounters or obtains actual

---

[5] G.R. No. 202666, 29 September 2014.
[6] Accessed on 18 September 2020, https://www.edweek.org/ew/articles/2016/11/09/what-is-digital-literacy.html
[7] Accessed on 18 September 2020, www.digitalcitizenship.net/nine-elements.html
[8] Accessed on 18 September 2020, https://www.educatorstechnology.com/2018/01/11-great-kids-safe-search-engines.html

knowledge of any facts or circumstances of incidents of harassment and/or abuse, or commit harm against another, he/she is encouraged to report the said incident to the following law enforcement agencies as soon as reasonably possible:

PHILIPPINE NATIONAL POLICE – ANTI-CYBERCRIME GROUP	Email Address:	acg@acg.pnp.gov.ph
	Mobile No.:	(+63) 998-598-8116
	Telephone Nos.:	(+632) 8414-1560
	Website:	https://pnpacg.ph/main
	E-Complaint:	https://acg.pnp.gov.ph/eComplaint/
	Facebook:	https://www.facebook.com/anticybercrimegroup
NATIONAL BUREAU OF INVESTIGATION – CYBERCRIME DIVISION	Email Address:	ccd@nbi.gov.ph
	Telephone No.:	(+632) 8523-8231 to 38 local 3455
	Website:	www.nbi.gov.ph
DEPARTMENT OF JUSTICE – OFFICE OF CYBERCRIME	Email Address:	cybercrime@doj.gov.ph
	Telephone No.:	(+632) 8524-8216
	Website:	www.doj.gov.ph/office-of-cybercrime.html
	Facebook:	https://www.facebook.com/OfficeofCybercrimePH

For your guidance and information.

ATTY. CHARITO A. ZAMORA
Officer-in-Charge
DOJ Office of Cybercrime