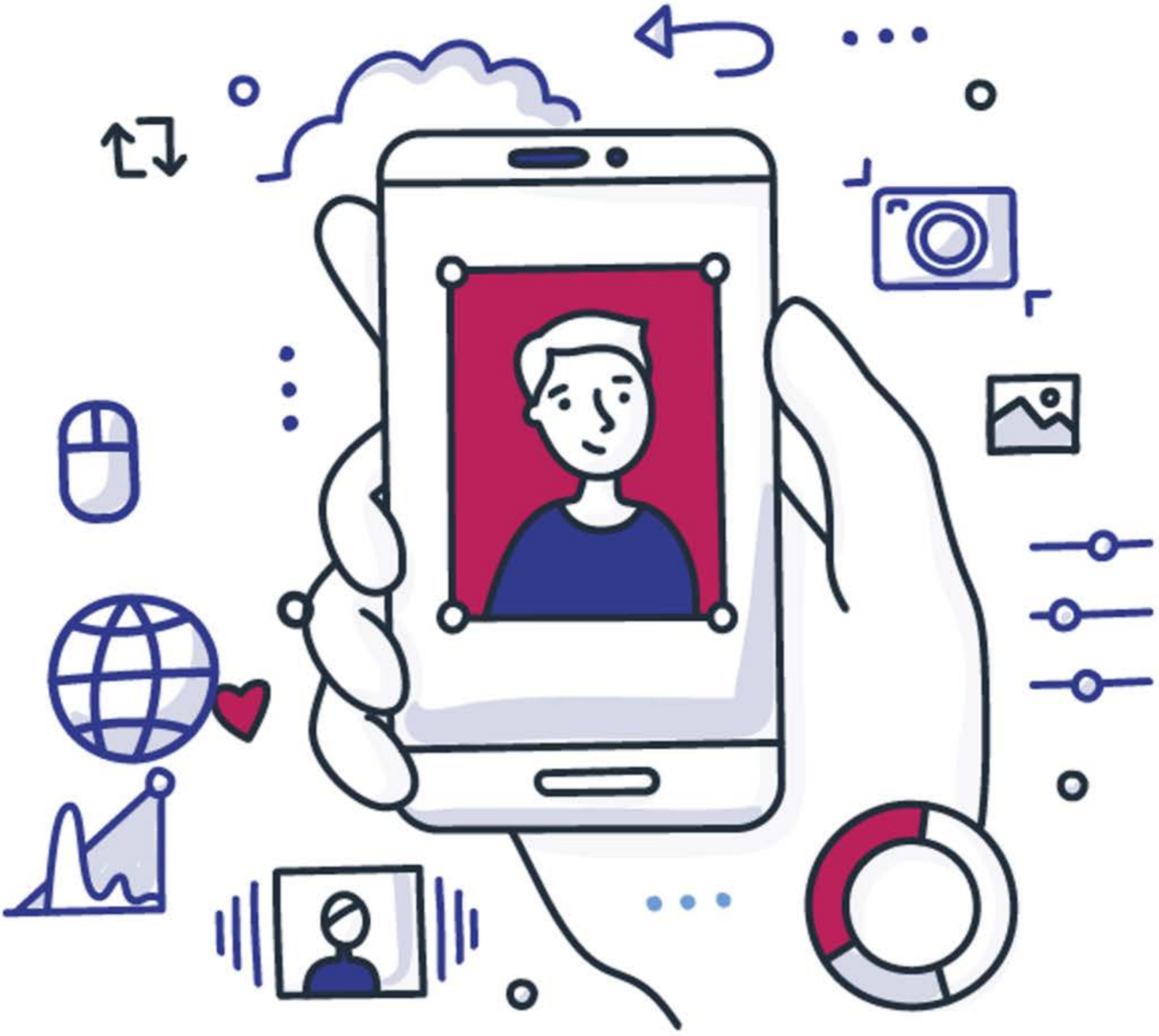
SEAMEO INNOTECH

# Knowledge Forum on the Cybersafety of Filipino Learners

## SUMMARY REPORT

27 May 2019 | SEAMEO INNOTECH, Quezon City



# KNOWLEDGE FORUM ON CYBER SAFETY OF FILIPINO LEARNERS

27 May 2019 | SEAMEO INNOTECH
Quezon City, Philippines

## BACKGROUND

Information and Communications Technology plays a major role in the lives of Filipinos – from staying connected with their families and communities to nation-building. Of the 105 million population, 67 million were recorded to be internet users in the Philippines .  The internet is already embedded in the lifestyle of majority of the youth, esp. of the digital natives .

In 2015, the Department of Education and Stairway Foundation, Inc. collaborated for a nationwide study on cyber safety where children aged 7-16 years old were surveyed. The study revealed that 9 out of 10 children were using the internet for: 1) research (school assignment); 2) social media; 3) video streaming, downloading and other activities; and 4) online gaming . The study also showed that 4 out of 10 children aged 7-12 years and 5 out of 10 children aged 13-16 years had their social media accounts visible to anyone. In terms of engaging with online strangers, 7 out of 10 children don't chat with strangers. And 3 of 10 children surveyed posted personal information online.

The Cyber Safety study also found out that 3-4 of 10 children surveyed knew of other children who were victims of cyberbullying. Cyberbullying is usually done through social media, chatting or texting in the form of threats, photo editing, exposing of one's secret conversation, humiliation or creation of poser account, exclusion, etc. The study also identified the following as cyberbullies: 1) classmates, 2) schoolmates, 3) people who obviously use fake profiles, 3) unknown people who don't seem to be using fake profiles, 4) children from other schools, 5) unspecified.

Measures in addressing these online risks have been provided by several laws existing in the country such as the Department of Education Child Protection Policy, Anti-bullying Act and the Data Privacy Act. Despite these laws, there are still gaps on the ground that need to be tackled to ensure that the learners and children know the online risks.

In 2016, an ASEAN Framework on Personal Data Protection stating a set of principles to guide the implementation of measures at both national and regional levels to promote and strengthen personal data protection in the region was developed.  The following is a snapshot of provisions or policies relating to data protection and privacy in other Southeast Asian countries :

⦿ Brunei Darussalam – There is no comprehensive law on data protection at the moment but the country has been guided by a Data Protection Policy since 2014. This policy covers personal data (in electronic or manual form) maintained by government agencies and educational institutions.

⦿ Cambodia – The Ministry of Post & Telecommunication ICT License (Article 27) states that “all ICT & Telecommunication operators and all relevant person must protect personal information, security, and safety of using their ICT & Telecommunication System”

⦿ Indonesia – The Ministry of Information and Communication Regulation No.20/2016 details more comprehensive regulation on Personal Data Protection. Law No. 11 of 2008 regarding Information and Electronic Transaction and Government Regulation No. 82 of 2012 regarding the Provision of Systems and Electronic Transactions (“PP 82/2012”) has also been enhanced.

⦿ Lao PDR – There are no plans by the Lao People’s Democratic Republic to legislate a statute on privacy and data protection but the Law on Protection of Electronic Data (2017) and the Law on Prevention and Combating Cyber Crime (2015) relate to the protection of personal information.

⦿ Malaysia – Malaysia is currently enforcing the Personal Data Protection Act 2010 (PDPA) through its Personal Data Protection Department.

⦿ Myanmar – In March 2017, Myanmar promulgated a 4-page law entitled Protecting the Privacy and Security of Citizens (Union Parliament Law 5/2017). According to the unofficial translation of the law7 by the Myanmar Center for Responsible Business (MCRB), the law explicitly prohibits interception of a citizen’s electronic communications, private correspondences and, physical privacy, unless otherwise warranted by an “order”.

⦿ Singapore – The Personal Data Protection Act 2012 (PDPA) has been in force since 2014 and is being implemented by the Personal Data Protection Commission.

⦿ Thailand – The Notification of the Electronic Transaction Committee on Policies and Practices for the Protection of Personal Information of Government Agencies BE 2553 (2010) and the Information Act for Public Sector BE 2540 (1997) protect its citizens’ personal information that are being processed by state agencies. The Personal Data Protection Act is under development and expected to be published soon.

⦿Vietnam – The most comprehensive legal framework on data protection is the Law on Cyber Information Security (Law No. 86/2015/QH13) (the "LCIS").

In the Philippines, the Data Privacy Act was passed in 2012, which paved way to the establishment of the National Privacy Commission. The Commission was formed in 2016 to administer and implement the provisions of the Act, and to monitor and ensure compliance of the country with international standards set for data protection . The Commission leads awareness campaigns on Data Privacy and Protection to different sectors – including the Education sector.

Initiatives from the Department of Education and the National Privacy Commission in mitigating online risks that our children and learners are vulnerable with can further be enhanced. Stakeholders from educational sector can work together to identify the gaps and boost measures in the prevention of online risks on the ground.

SEAMEO INNOTECH as a regional organization dedicated to identifying common and distinct education issues in Southeast Asia is devoted to raise awareness and help develop solutions that will address issues relating to the educational sector including online risks and data privacy concerns, which have direct effect on the welfare and well-being of every learner in the country and the region as a whole. This learning exchange will eventually kick-off a series of knowledge forum on cybersafety and digital citizenship in the region.

## OBJECTIVES

To dig deeper on how the educational sector could help mitigate and reduce online risks among learners, a knowledge roundtable forum is proposed to be conducted. The forum aims to:

⦿ Showcase and disseminate related research and knowledge products on e-Citizenship and Cyber Safety.

⦿ Create awareness on the provisions of Data Privacy Act, DepEd Child Protection Policy and Anti-bullying Act;

⦿ Gather and document best practices from both private and public schools on data protection and prevention of online abuses; and

⦿Identify gaps in the existing practices of schools in ensuring digital safety of learners.

## EXPECTED OUTPUTS

The knowledge forum on the protection of learners in cyberspace is part of the envisaged series of knowledge fora on key issues in education across the region. The forum is seen as a platform for exchange and discussions on relevant educational concerns, particularly on data protection of learners in the country as well as significant conversations on issues related to the prevention of online abuses. Below are the foreseen concrete outputs of the forum:

⦿ Documentation of best practices from both private and public schools on data privacy protection and prevention of online abuses, including identified gaps in the existing practices of protecting learners from online abuses and risks, and a collective declaration or manifesto of commitment to uphold Cyber Safety among Filipino learners;

⦿ Popularized information materials (e.g. Infographics and Primer) on the Data Privacy Act specifically designed for schools and education personnel;

⦿ Identified areas in school management and delivery of education services for further research, training and capacity building programs and knowledge management and networking services

## FORUM SUMMARY

As a kick-off to the series of knowledge learning activities for the 50th anniversary of SEAMEO INNOTECH, the Knowledge Forum on Cybersafety of Filipino Learners was organized last May 27, 2019. With the goal of stirring conversation on cybersafety of Filipino learrners, the knowledge forum was able to gather teachers, policy makers and individuals from the civil society.

During the opening remarks, Undersecretary Josephine G. Maribojoc highlighted the efforts of the Department of Education (DepEd) in promoting the rights of the child against all forms of abuse and violence through its Child Protection Policy. And because online child protection concerns were increasingly becoming a big concern, DepEd issued a department order supporting the Anti-Bullying Act of 2013 that covers bullying online of learners.

Usec. Maribojoc emphasized the importance of building cyberworld defenses for the learners and including them in the process of building a cybersafe learning environment. Teaching cyber life skills may help learners strengthen their cyberworld immune system. She added that there is a need to have a whole-of-society approach, not just school interventions, to effectively and consistently reduce the online risks of learners in the cyberworld.

Atty. Erlaine Vanessa Lumanog of the National Privacy Commission also shared the importance of data privacy. She further explained the provisions in the Data Privacy Act of 2013, emphasizing the need for all data collectors to protect the security, integrity and confidentiality of all the personal information they collect. Atty. Lumanog also highlighted the seven rights of the data subjects: 1) right to information, 2) right to object, 3) right to access, 4) right to correct, 5) right to erase, 6) right to damage, and 7) right to file a complaint.

Stairway Foundation, Inc. gave a brief overview on the research that the group conducted on Cybersafety. Mr. Ysreal Diloy of Stairway Foundation, also presented the emerging definition of digital divide in the context of cybersafety – where a household or a society may share the same technology platforms (hardware and social media), but children and adults may use (and look at these platforms) differently.

To prove his point, he provided an example of the evolution of pop culture and how technology has changed it. He showed photos of popular celebrities from the 50s to the early 2010s, where most of the audience were able to identify the individuals presented, primarily because of their presence on traditional media. However, when he started showing slides of social media personalities and popular applications, some members of the audience were having difficulties in identifying the individuals or apps shown in the slides. He further emphasized that the digital divide in the context of cybersafety has implications on a child’s protection online.

Mr. Diloy presented the importance of three Cs in cybersafety – content, contact and conduct. A child or learner can be at risk based on the content he or she accessed online. A child is at risk through online interactions, or through contact; and lastly, a child can be at risk based on how he/she conducts himself/herself online.

Mr. Diloy concluded his presentation by emphasizing on the need to establish policies and systems that will make the online environment safe for learners, the need to build the capacity of duty bearers and stakeholders so they can effectively protect the learners, and the importance of enhancing the online protective behaviors of learners so that they can enjoy the benefits and opportunities of CyberSpace.

SEAMEO INNOTECH and Stairway Foundation shared the resources and materials they individually have developed in promoting and establishing a cybersafe environment. SEAMEO INNOTECH showcased the Mobile Technology for Teachers (MT4T) toolkit and the e-Citizenship e-book. The MT4T toolkit is a teacher resource that promotes the use of mobile technology in Southeast Asian educational settings. The kit provides a basic guide in using mobile devices, such as smart phones and tablets and their accompanying applications, as tools for teaching and learning in the classroom and for teachers' personal and professional development; while the e-Citizenship e-book is a resource that aims to update teachers on the ins and outs of information and communications technology (ICT), particularly mobile devices and the internet highlighting aspects of digital safety, security, and privacy in their classrooms. The e-book also aims to provide teachers with a repertoire of tips, strategies, and activities for young people to be safe, healthy and responsible users of ICT.

Stairway Foundation introduced the CyberSafe Learning Resources Eco-system - a pool of resources that Stairway Foundation has developed in collaboration with strategic partners. This pool of resources includes CyberSafe Lesson Plans, Dalir-eskwela, and CyberSafe ELearning. The CyberSafe Lesson Plans is an initiative with DepEd through the Office of the Undersecretary for Legal Affairs. This particular set of resources was developed out of the expressed needs from teacher participants during the National DepEd Child Protection Trainings for an online safety lesson plans for learners. The Dalir-eskwela is a series of video clips that highlight good online content and child-safeguarding practices. The development of these video clips is a collaboration among DepEd, Stairway Foundation and the Internet and Mobile Marketing Association of the Philippines (IMMAP). Lastly, Stairway Foundation showcased the e-learning platform called Cybersafe ELearning. It is an e-learning platform for child sexual abuse and exploitation prevention training. Cybersafe ELearning is a set of six interactive and engaging e-learning tutorials on Child Rights, Child Sexual Abuse Prevention and Cyber Safety.

After the presentations, a workshop was conducted. The participants were asked to list down ideas on how to effectively communicate the importance of cybersafety to parents, teachers and learners. They were then asked to identify one idea from the list that they deemed to be innovative and effective in communicating and fostering a cybersafe environment. Top ideas that came out were presented during the plenary.

Mr. Bennet Benoza, of SEAMEO INNOTECH, emphasized the importance of partnership or a community where knowledge exchange happens in creating and fostering a cybersafe learning environment. He hoped for the community to continue the exchange on cybersafety and other issues that affect the Filipino learners even after the forum. He closed the forum by giving thanks to each and everyone in the room for actively participating throughout the day.

# OPEN FORUM

***Question 1: What to do if sensitive information/data is already "out" (i.e. for adults, credit card information was already captured, or sensitive cyber videos of students were being shared among peers)?***

National Privacy Commission (NPC): There should be prudence in sharing information. The Data Privacy Act prohibits the misuse of information by any institution. If an individual feel that his or her info has been misused or abused, there is a mechanism where the individual can complain so that the institution involved will be held liable.

Stairway Foundation, Inc. (Stairway): In the case of indecent videos being shared among learners, DepEd has protocols on Child Protection Policies. The teachers and school management can avail of training on handling cases of abuse with cyber component. Outside school, parents can seek assistance from specialized anti-cyber crime units: the Anti-cyber Crime unit of the Philippine National Police or the National Bureau of Investigation's Anti-Cyber Crime Division. Online or cyber abuse of children is a law enforcement concern.

***Question 2: The school has plans of subscribing into a mobile device management software which will be installed in the gadgets owned by students. By doing this, is the school violating any provision in the Data Privacy Act? Does the school need to have a consent form?***

NPC: DPA does not prohibit the type of equipment that the individual has. The law promotes privacy of information within the bounds of law. In terms of consent, if the child is below 18 years old, consent from the guardian must be obtained; while if the child is of legal age, consent should be coming from the child. Consent can be in written or recorded form. It is important that content should be documented.

***Question 3: In relation to mental health wellness, is it ok for schools to ask for pyschological abstracts of the child?***

NPC: Psychological reports or medical abstracts are considered sensitive personal information because it involves the health information of the data subjects, in this case, the child. The school needs to have an established school policy regarding mental health wellness. The school still needs to obtain consent from the parents. Communication, between the parents and school, is key towards this process.

***Question 4: A question related to an online engagement his son was part of. Her son, when he was still a minor, was involved in translating business documents from Mandarin to English. The son reasoned out that it was an opportunity for him to practice his Mandarin to English translation skills. Was there an exploitation in this kind of involvement?***

Stairway: First thing to consider was the appropriateness of the materials or documents translated by the child. Based on the story, there is imbalance of power and a number of cybersafety red flags, esp. since the son was still a minor when it happened. It's always safe to act in the least risky manner in a situation like this.

***Question 5: SEAMEO INNOTECH was part of the Digital Kids Survey that was conducted in four countries Vietnam, Fiji, Bangladesh and Korea. Similar studies to be done by UNICEF in the Philippines. The Digital Kids study revealed that majority of the kids interviewed would not report to teachers or parents when there are confronted with cybersafety concerns. Instead, these kids would seek guidance from their peers. What are the implications of these?***

Stairway: Peer advocacy is important. In Plan International, they develop peer advocates where they engaged youth as peer advocates. It is important to include the youth and children in participating to the cybersafety conversations. At Stairway, the focus is on duty bearers and stakeholders. Still anticipating on the results of the Philippine Kids Online study, but, in the field, majority of the children don't disclose with their parents or teachers because of digital divide. The goal now is to bridge this digital divide so children will see adults as someone whom they can trust, relate with and approach.

## WORKSHOP OUTPUTS

### IDEAS ON HOW TO EFFECTIVELY COMMUNICATE THE IMPORTANCE OF CYBERSAFETY TO LEARNERS

**1**

- Don't add strangers on FB; add your friends only
- Tell our parents to know our activities online
- Limit time when using gadgets/internet
- Focus/spend more time on physical play or games
- Set aside/budget time for social media; make sure to work on assignment first
- Post more contents/information about cybersafe environment on FB account
- Post/share educational games/fun contents/interactive activities online
- Block bullies/malicious contents online
- Learn to say no
- Think before I click

**2**

- Tap the support of stakeholders to conduct seminar for students on cybersafety and in supervising who are engaged in computer games
- Follow rules and regulations regarding the proper use of cellular phones
- Join clubs or organizations
- Participate in school activities
- Be a responsible user of social media
- Practice cyberlife skills
- Attend seminar on cybersafety
- Engage in physical activities like games instead of using gadgets and internets

**3**

- Time management
- Be a responsible user
- Think before you click
- Be a positive peer
- Report victims
- Choose appropriate mobile app
- Avoid posting negative or harmful issues
- Decipher unhealthy issues
- Define advantages and disadvantages
- Do not share too much information online
- Share and spread positive and good posts/pictures
- Don't be too public. Filter your status posts.
- Report bullies.
- Consult parents and teachers.
- Join activities and organizations.
- Have time for socialization.
- Set priorities.
- Follow ethical standards or netiquette.
- Discover new interests/hobbies.
- Set play dates with friends.
- Obey your parents.
- Bonding time with family.
- Quality over quantity

**4**

⦿ Creating partnership with internal and external groups
⦿ Doing research
⦿ Benchmarking
⦿ Seeking experts/peer advice
⦿ Peer mentoring
⦿ Commitment signing
⦿ Training the parents
  a. Advocacy involvement
  b. Use the filtering and automation features of devices
  c. Use advance search, child-friendly search engines

⦿ Adjust google settings
⦿ Produce their own campaign materials
⦿ Seek answers to questions about cyber issues
⦿ Form their own cybersafety groups
⦿ Create them digital drive
⦿ Discourage the use of social media

## IDEAS ON HOW TO EFFECTIVELY COMMUNICATE THE IMPORTANCE OF CYBERSAFETY TO PARENTS

**1**

⦿ ONLINE
  a. Know their passwords
  b. Limit screen time
  c. Rewards/punishments

⦿ LIMIT
  a. 1-day battery life
  b. Unplug after 10 PM
  c. Block sites
  d. Youtube kids
  e. Use only educational apps
  f. Friday to Sunday only

⦿ OFFLINE
  a. Set rules, say "NO", be firm
  b. No wifi
  c. Talk/quality time
  d. Use post its
  e. Parents should set good example (limited screen time)

**2**

⦿ Child-friendly rules in the family
  a. Involve children in drafting for ownership
  b. Set screen time
  c. Child-friendly xontent
  d. Common apps for family

⦿ More quality time with children
⦿ Know/befriend your children's friends

⦿ Strengthen family values (Conscious)
  a. Love
  b. Trust
  c. Respect
  d. Kindness
  e. Communication

⦿ Continuous supervision and guidance
  a. School-parent communication

⦿ Be familiar with children's online activities
  a. Screen
  b. Bonding
  c. Learning

⦿ Enhance knowledge
  a. Use of apps
  b. Social media platforms
  c. Parental control features in games
  d. Sharing among co-parents

⦿ Online family groups (FB, viber, etc.)

3

For the parents
⦿ Symposium/ orientation on Cybersafety
⦿ Workshop (privacy settings of gadgets/sites)
⦿ Parent-teacher meeting (progress of learner)
⦿ Re-echoing of “this forum” to parents
⦿ Infographics – dissemination
⦿ Website for parents
⦿ Mentoring
⦿ Guidance counselor’s report
⦿ Modules for parents on cybersafety

By the parents
⦿ Parental
⦿ Limit on the gadget usage (by schedule)
Constant supervision
⦿ Quality off-screen time with Children

## IDEAS ON HOW TO EFFECTIVELY COMMUNICATE THE IMPORTANCE OF CYBERSAFETY TO TEACHERS

1

Ways to create a cybersafe environment for our learners
⦿ Sell the idea (Cybersafety)
⦿ Equipping/capacitating teachers
⦿ Curriculum integration across disciplines
⦿ Institutionalize cybersafety for localized policies and campaigns
⦿ Consultations/dialogues and corresponding evaluation with learners and stakeholders
⦿ Policy Evaluation

2

Policies
⦿ Technology-use
⦿ Fair use
⦿ Internet use
⦿ Social Media
⦿ Delegation of responsibility on cybersafety concerns
⦿ Response policies
⦿ Partnership and cooperation policy with other organization

Monitoring
⦿ Filtering
⦿ Blocking
⦿ Safety prompts
⦿ Visual cues and guides
⦿ Logs monitoring
⦿ Partial surveillance
⦿ Assignment of point persons

Control
⦿ Protection from surveillance
⦿ Malwares
⦿ Adware
⦿ Hacking
⦿ Fraud
⦿ Violence
⦿ Scareware

Literacy
⦿ Dissemination of information
⦿ Digital literacy
⦿ Trainings and seminars
⦿ Encouraging action research about cybersafety
⦿Community involvement
⦿ Implementation of cybersafety to learners

3

⦿ Prohibitions for the use of cellphones during class hours
⦿ Quarterly trainings for students Re: cybersafety
⦿ Integration of cybersafety across learning areas
⦿ Signages and reminders on responsible use of social media
⦿ Creation of mascot against “manyaks”, stalkers, haters
⦿ Benchmarking to other schools
⦿ Create a “Cybersafe garden”
⦿ Conduct cybersafe seminars for teachers, learners and parents
⦿ Creation of room for cyber addict
⦿ Involve clubs on information dissemination
⦿ Cybersafe evaluation drill
⦿ Cybersafe fire wall against harmful sites
⦿ Posting of images about code of ethics in using technology/internet
⦿ Film showing about cyber bullying
⦿ Organizing cybersafe warriors
⦿ Creating video vlog about cybersafe community
⦿ Creating cybersafe mural
⦿ Animation for cybersafety

## NEXT STEPS

**A. Development of Cybersafety Infographics**

Outputs from the workshop will be used as a reference in the development of Cybersafety Infographics

**B. Creation of a Peer Learning Community on Cybersafety and Digital Citizenship**

Participants of the Knowledge Forum on Cybersafety will initially be part of a community of practice. The goal of a peer learning community is to gather and showcase best practices on Digital Citizenship.

As an initial activity, teachers, school administrators and learners will be gathered to:

***1. Raise interest in Cybersafety and Digital Citizenship - Peer Learning Community (PLC)***

- The need for a critical understanding of Cybersafety and Digital Citizenship
- The importance of investing for the adoption of a Digital Citizenship strategy in the education sector – national and regional scope
- The benefits of collaboration and peer learning

***2. Gather feedback on the priorities and structure of the Peer Learning Community (PLC)***

- Identify barriers  in the adoption of a Digital Citizenship strategy in the Education sector

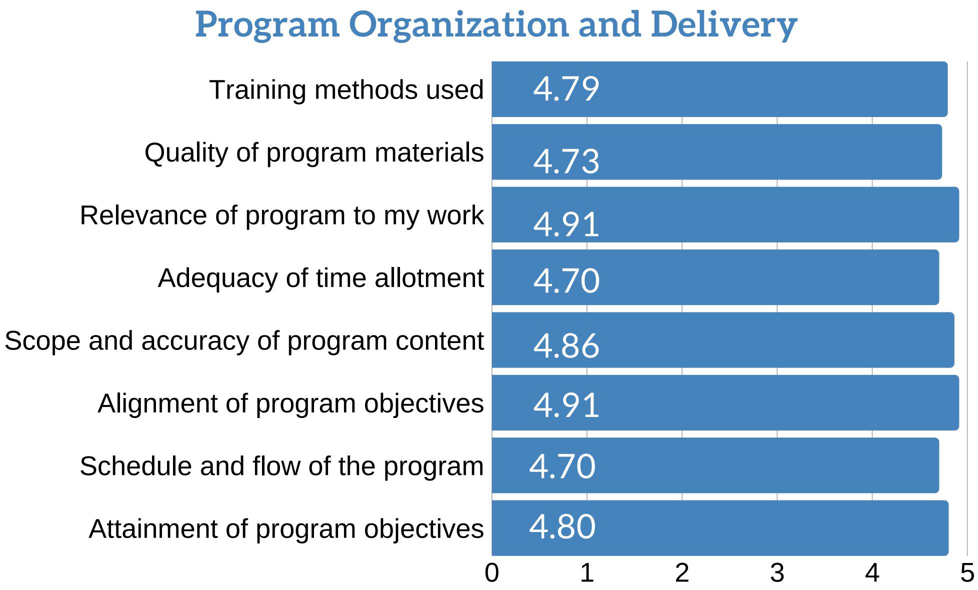
***3. Explain the requirements/conditions for successful participation in the Digital Citizenship PLC***

## FORUM EVALUATION

The forum was attended by a total of 84 external participants, and 30 SEAMEO INNOTECH staff. Feedback from the participants on the forum was gathered, and of the 84 external participants, 66 were able to provide their evaluation forms to the KMNO team.

The workshop was evaluated into three categories: program organization and delivery, and program management, administrative and support services. The following 5-point rating scale was used: excellent (5), very satisfactory (4), satisfactory (3), fair (2), needs improvement (1). Non- applicable elements were omitted from this report.

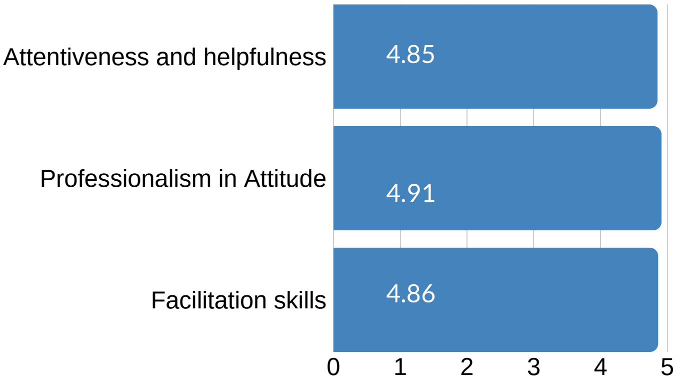
In program organization and delivery, the following elements were assessed: attainment of program objectives, schedule and flow of the program sessions, alignment of program objectives, content, methods and assessment approaches, scope and accuracy of program content, adequacy of time allotment, relevance of program to my work, quality of program materials and handouts, and training methods used. In this category, relevance of program to my work and alignment of program objectives, content, methods and assessment approaches got the highest rating of 4.91, while adequacy of time allotment and schedule and flow of the program sessions got the lowest rating of 4.70.



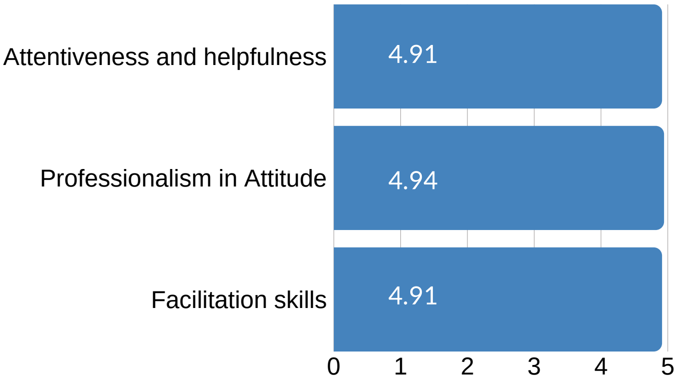
The lowest rating is consistent with the participants' feedback on one of the identified areas that needs to be enhanced, which is time allotment.

*"Time allotment for each topic"*
*"I think the areas that could be further improved is the time allotment, the topics are very useful and I want to have longer time for each content"*
*"Time allotment"*
*"Only the time allotment and schedule of flow"*
*"Longer time for theoretical discussion"*
*"More time for activities and Q&A"*
*"More time"*
*"Could have more time for each topic, "bitin" "*
*"Time management is a bit off but otherwise good job"*
*"Give more time for Q and A portion"*
*"time frame"*

Evaluation of the program management category is based on two sub-categories: **program management team** and **program support**. This category mainly looks at the behavior and capacity of the staff involved in organizing the forum. Professionalism in attitude got the highest score in both sub categories.



Program Management Team



Program Support

In terms of ***administrative and support services,*** the venue got a rating of 4.91. The food service was also evaluated under this category. Quality of food got the highest rating of 4.91 while the manner of serving got a rating of 4.82.

Overall, the forum received a 4.87 rating which is equivalent to “excellent”.

Participants’ feedback were also captured. Below is the word cloud of both ***what they liked*** and ***what needs to be enhanced***. The top 5 features that the participants liked the most about the forum were: the set of speakers, the program flow, the forum being informative, the timeliness/relevance of the forum and the workshop activity.

Most of the remaining comments were congratulatory remarks from the participants.

As for the areas that need enhancements, participants pointed out the following: time allotment, provision of forum materials, and representation of participants.

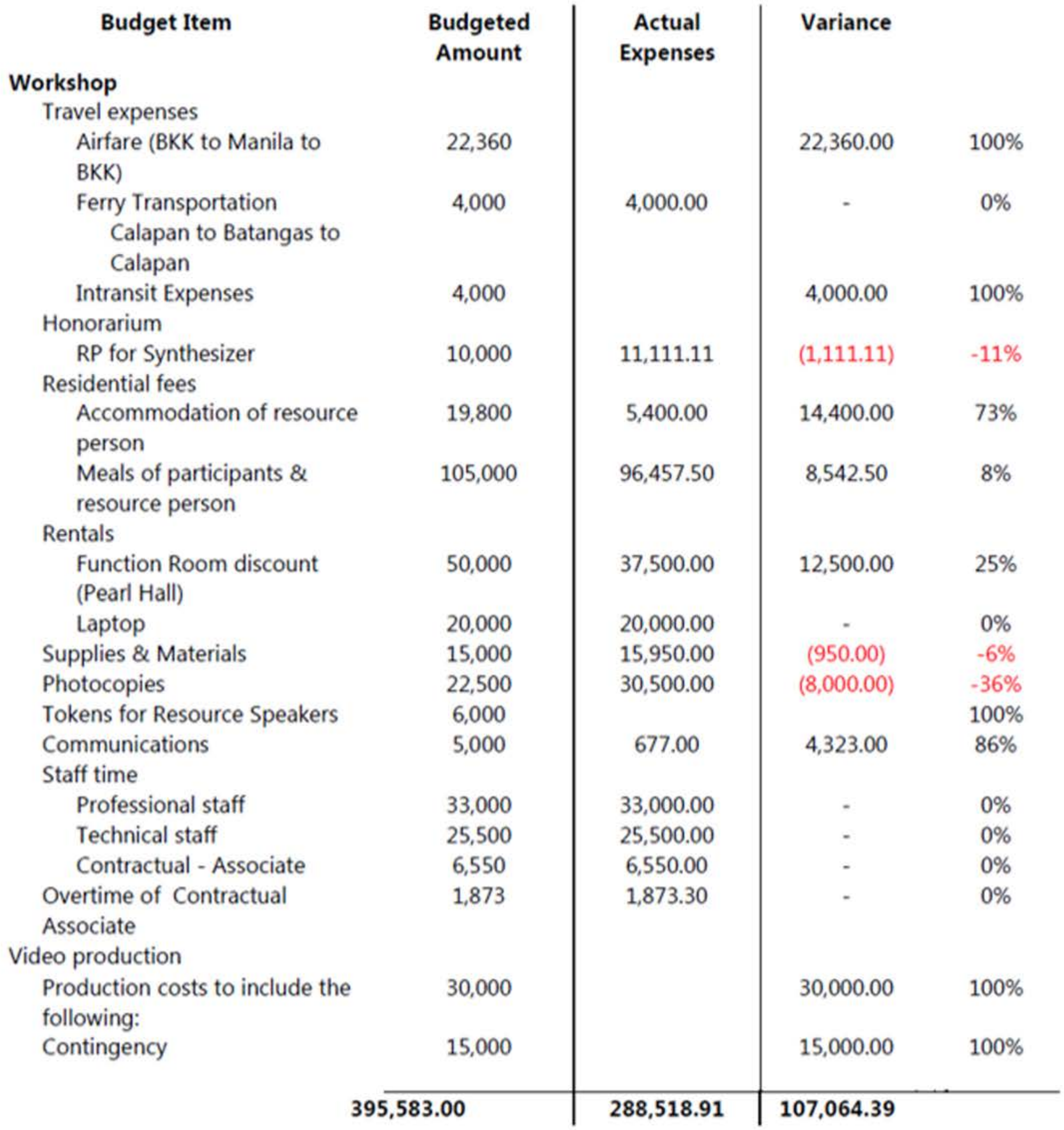
What they liked?

informative
timely
excellent
speakers
program
Congratulations
workshop
Thank-you
topics
topic
good
well
relevant
strengthen
knowledge
thinking
activities
objectives
giving
forum
ideas
help
helpful
like
Timely
teacher
significant
interactive
Facilitators
knowledgeable
useful
must
Design
Keep
venue
Content
Resource

What needs to be enhanced?

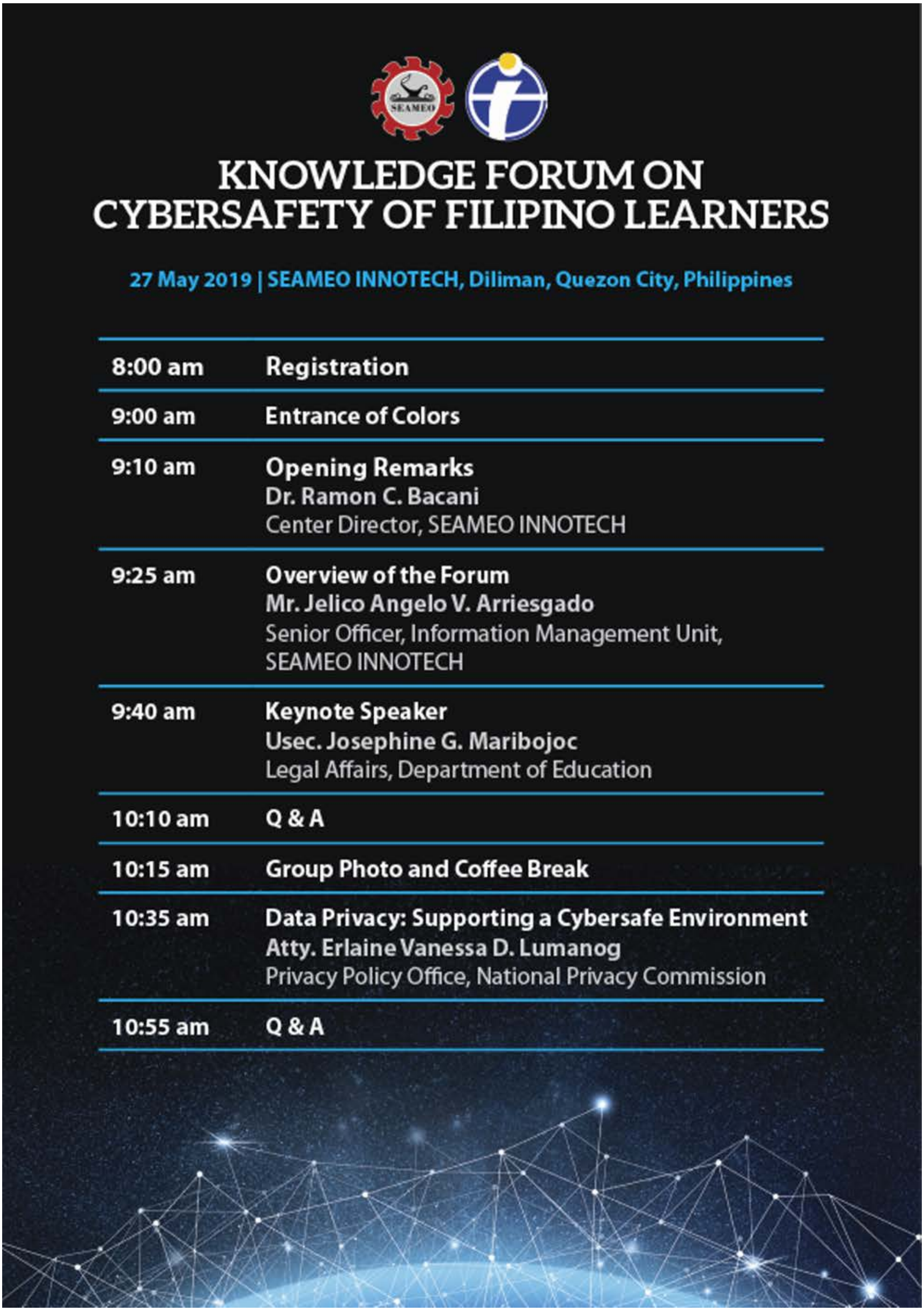
time
allotment
Provide
provide
materials
activities
teachers
Time
participants
activity
Congratulations
management
topics
topic
handouts
cybersafety
workshop
school
None
Give
will
use
just
successfully
implementing
conducted
enhancement
Cybersafety
Groupings
speakers
Excellent
Workshop
Request
defined
schools
comment
consideration
seminar
shoould
forum
Filipino
frameprogram
want
security
content
project
Google
features
flow
copy
laptop
learners
shaping
admin
excellent
engages
representation
participation
Providing
maximize
schedule
Knowledge
discussion
Thank-you
theoretical
speeches

# FINANCIAL REPORT



| Budget Item | Budgeted Amount | Actual Expenses | Variance | |
|---|---|---|---|---|
| **Workshop** | | | | |
| Travel expenses | | | | |
| Airfare (BKK to Manila to BKK) | 22,360 | | 22,360.00 | 100% |
| Ferry Transportation Calapan to Batangas to Calapan | 4,000 | 4,000.00 | - | 0% |
| Intransit Expenses | 4,000 | | 4,000.00 | 100% |
| Honorarium | | | | |
| RP for Synthesizer | 10,000 | 11,111.11 | (1,111.11) | -11% |
| Residential fees | | | | |
| Accommodation of resource person | 19,800 | 5,400.00 | 14,400.00 | 73% |
| Meals of participants & resource person | 105,000 | 96,457.50 | 8,542.50 | 8% |
| Rentals | | | | |
| Function Room discount (Pearl Hall) | 50,000 | 37,500.00 | 12,500.00 | 25% |
| Laptop | 20,000 | 20,000.00 | - | 0% |
| Supplies & Materials | 15,000 | 15,950.00 | (950.00) | -6% |
| Photocopies | 22,500 | 30,500.00 | (8,000.00) | -36% |
| Tokens for Resource Speakers | 6,000 | | | 100% |
| Communications | 5,000 | 677.00 | 4,323.00 | 86% |
| Staff time | | | | |
| Professional staff | 33,000 | 33,000.00 | - | 0% |
| Technical staff | 25,500 | 25,500.00 | - | 0% |
| Contractual - Associate | 6,550 | 6,550.00 | - | 0% |
| Overtime of Contractual Associate | 1,873 | 1,873.30 | - | 0% |
| Video production | | | | |
| Production costs to include the following: | 30,000 | | 30,000.00 | 100% |
| Contingency | 15,000 | | 15,000.00 | 100% |
| | **395,583.00** | **288,518.91** | **107,064.39** | |

## CYBERSAFETY PROGRAM

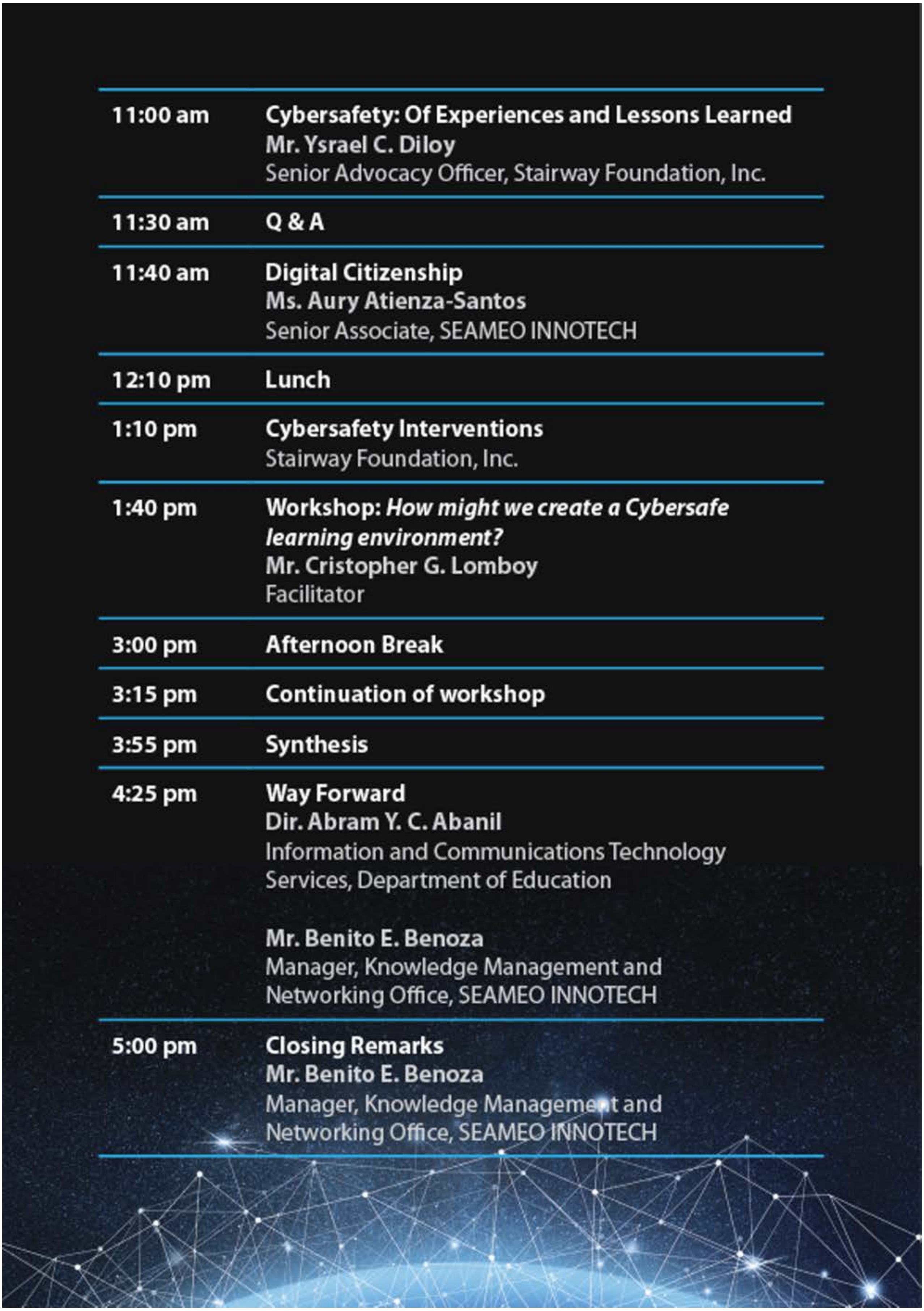


# KNOWLEDGE FORUM ON CYBERSAFETY OF FILIPINO LEARNERS

27 May 2019 | SEAMEO INNOTECH, Diliman, Quezon City, Philippines

| | |
|---|---|
| 8:00 am | **Registration** |
| 9:00 am | **Entrance of Colors** |
| 9:10 am | **Opening Remarks**<br>Dr. Ramon C. Bacani<br>Center Director, SEAMEO INNOTECH |
| 9:25 am | **Overview of the Forum**<br>Mr. Jelico Angelo V. Arriesgado<br>Senior Officer, Information Management Unit, SEAMEO INNOTECH |
| 9:40 am | **Keynote Speaker**<br>Usec. Josephine G. Maribojoc<br>Legal Affairs, Department of Education |
| 10:10 am | **Q & A** |
| 10:15 am | **Group Photo and Coffee Break** |
| 10:35 am | **Data Privacy: Supporting a Cybersafe Environment**<br>Atty. Erlaine Vanessa D. Lumanog<br>Privacy Policy Office, National Privacy Commission |
| 10:55 am | **Q & A** |

# CYBERSAFETY PROGRAM



| | |
|---|---|
| 11:00 am | **Cybersafety: Of Experiences and Lessons Learned**<br>**Mr. Ysrael C. Diloy**<br>Senior Advocacy Officer, Stairway Foundation, Inc. |
| 11:30 am | **Q & A** |
| 11:40 am | **Digital Citizenship**<br>**Ms. Aury Atienza-Santos**<br>Senior Associate, SEAMEO INNOTECH |
| 12:10 pm | **Lunch** |
| 1:10 pm | **Cybersafety Interventions**<br>Stairway Foundation, Inc. |
| 1:40 pm | **Workshop:** ***How might we create a Cybersafe learning environment?***<br>**Mr. Cristopher G. Lomboy**<br>Facilitator |
| 3:00 pm | **Afternoon Break** |
| 3:15 pm | **Continuation of workshop** |
| 3:55 pm | **Synthesis** |
| 4:25 pm | **Way Forward**<br>**Dir. Abram Y. C. Abanil**<br>Information and Communications Technology Services, Department of Education<br><br>**Mr. Benito E. Benoza**<br>Manager, Knowledge Management and Networking Office, SEAMEO INNOTECH |
| 5:00 pm | **Closing Remarks**<br>**Mr. Benito E. Benoza**<br>Manager, Knowledge Management and Networking Office, SEAMEO INNOTECH |

**SEAMEO INNOTECH**

The Southeast Asian Ministers of Education Organization Regional Center for Educational Innovation and Technology envisions a better future for every learner in Southeast Asia.

It provides innovative and technology-oriented learning services and research-based solutions to enable the education community in Southeast Asia to effectively respond to current and emerging needs and concerns.

Commonwealth Avenue, Diliman, Quezon City
1101 Philippines

☎ (+632) 8 924 7681 to 84

(+632) 8 921 0224

✉ info@seameo-innotech.org

f seameoinnotech

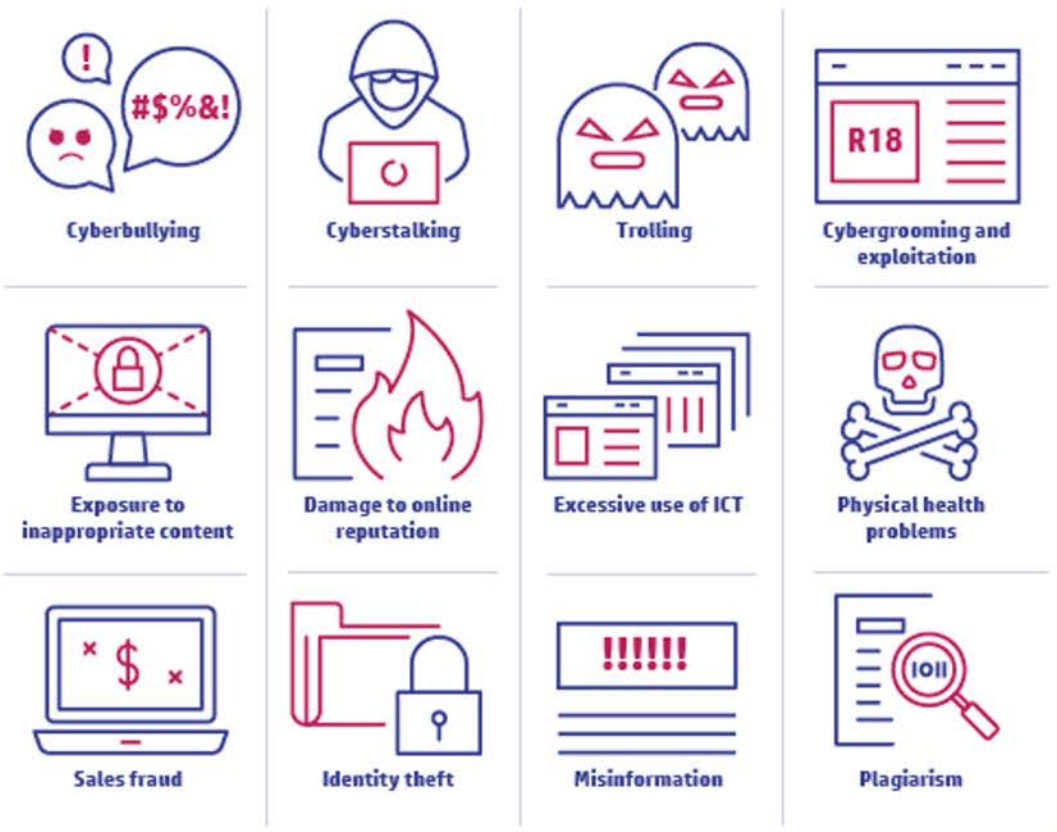
**www.seameo-innotech.org**
ISO 9001 & 29990 CERTIFIED

# Are Filipino Learners Cybersafe?

Information and communications technology plays a major role in the lives of Filipinos—67 million of the 105 million population were recorded to be internet users in the Philippines. A cybersafety study in 2015 revealed that Filipino digital natives are vulnerable to online risks and abuses.

In May 2019, SEAMEO INNOTECH gathered Filipino educators and education officials to discuss the online risks and cybersafety of learners in the Philippines.

## COMMON ONLINE RISKS AND ABUSES



Cyberbullying

Cyberstalking

Trolling

Cybergrooming and exploitation

Exposure to inappropriate content

Damage to online reputation

Excessive use of ICT

Physical health problems

Sales fraud

Identity theft

Misinformation

Plagiarism

# How to mitigate online risks?

Teaching cyber skills to children gives them the necessary defenses to survive in the cyber world. Instilling the importance of respect, privacy and integrity to influence online behavior of these children may address risks involving online conduct.

In 2012, the Philippines passed the **Data Privacy Act (RA 10173)** to assure the free flow of information to promote innovation and growth, while also protecting the users' fundamental rights to privacy.

**What should we know about the Data Privacy Act?**

- Information of individuals should be respected
- Individuals should have the right to control the collection of, access, and use of their information

**To comply with the Data Privacy Act, schools, institutions, and online platforms should do the following:**

- Draft a data privacy policy and mechanism
- Inform individuals on the kind of data they gather, how these will be collected and used, and provide an opportunity for individuals to confirm or decline the collection and use of their data
- Provide robust systems and processes for ensuring the security of users' data
- Implement effective systems to prevent, detect and respond to data breaches

### TYPES OF PERSONAL INFORMATION

1. **Personal Information** is any information from which the identity of an individual can be ascertained by the entity holding the information, or when put together with other information would directly identify an individual.
2. **Sensitive Personal Information** includes race, ethnic origin, marital status, age, color and religion, philosophical, or political affiliations; health, education, genetic, or sexual life of a person, court proceedings; Information issued by government agencies such as social security numbers, health records, licenses, suspension or revocation, and tax returns; and information specifically established by an executive order or an act of Congress to be kept classified.
3. **Privileged Information** is any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication such as information between client and his lawyer, or husband and wife.

# How to promote cybersafety?

**TO STUDENTS**

- Joining or establishing a cybersafety-oriented club
- Creating a cellphone wallpaper template that reminds to think before they click
- Activation of fingerprint log-in or creating an airtight password
- Downloading and installing of age-appropriate and learner-friendly mobile apps

**TO TEACHERS**

- Integration of cybersafety concepts in the curriculum
- ICT system in school has a firewall that filters inappropriate content, monitors logs, and blocks cyber threats
- Creation of a cyber superhero—a public face of cybersafety who fights online predators

**TO PARENTS AND THE COMMUNITY**

- Learning exchanges on cybersafety
- Cybersafety posters displayed in schools and in the community

Scan the QR code for the full report on the ***Knowledge Forum on Cybersafety of Filipino Learners.***

Commonwealth Avenue, Diliman, Quezon City
1101 Philippines

(+632) 8 924 7681 to 84

(+632) 8 921 0224

info@seameo-innotech.org

seameoinnotech

**www.seameo-innotech.org**
ISO 9001 & 29990 CERTIFIED