Capacity Building of Teachers and Parents in Cyber Safety and Security: the COL experience

International Conference on Cyberlaw, Cybercrime & Cybersecurity
India | 23-25 November 2022
Commonwealth Heads of Government Meeting
Vancouver, 1987
To help Commonwealth governments and institutions use technologies to improve and expand access to education and training
Building resilience
COL’s strategic interventions

• During the pandemic, institutions were largely unprepared for the sudden transition to online learning

• COL offered multi-dimensional support to Commonwealth governments, institutions and community-based organisations to minimise loss of learning and to be resilient
Capacity building of teachers in technology-enabled learning

Key activities included design and delivery of online courses for teachers:

• In Trinidad and Tobago, almost half of all the teachers in the country were covered by COL’s capacity building activities

• Over 4,000 teachers trained in the Pacific
Emerging Recognition: Parents as Co-educators in Preventing Learning Loss

COL’s Parental Learning for Uninterrupted Schooling (PLUS)

- COL organised community-based programmes in Ghana covering about 4,800 parents in 40 communities

Online courses on Family and Inter-Generational Learning

- Offered with UNESCO Institute for Lifelong Learning covering parents, teachers as well as key other stakeholders
Cybersafety 
a major concern for stakeholders

• In many Commonwealth developing countries, parents and students shared just one device for learning as well as other purposes
• Students tended to disregard safety norms
  • often parents and teachers did not understand the implications
• This led to frequent cyberattacks on students as well as teachers
Teachers and learners were exposed to cyberattacks

• “E-mail takeover”
• “My identity was stolen and used in messenger”
• “My Facebook account was hacked!”
• “My staff has experienced cyber breaches due to mismanagement of their Zoom classes and not following security protocols, perhaps due to lack of understanding. The staff was retrained and students suspended as identified for hacking the classes.”
Pedagogical impact of cyber attacks

- Disrupted teaching and learning
- Slow or no access to learning systems
- Delayed assessments
- Loss of teaching and learning materials
  - For example, ransomware attacks or hacking led to any or all of the above outcomes
- Loss of teacher-student trust- due to hacking and impersonation
- Impact on mental health for victims of cyberbullying
Teacher’s role

• Teachers an important intermediary in ensuring safe access

• Need to build teacher capacity in cybersecurity stressed even before Covid-19 (2018)

• Teachers’ e-readiness critical in building resilient educational systems (2020)
Training teachers in Cybersecurity

- During 2020-21, COL offered four MOOCs in Cybersecurity
- About 7,000 teachers from 96 countries enrolled
Topics Covered

Introduction to cybersecurity
Cyber safety for students
Cyber attacks in online learning
  • Protecting data
  • Ensuring online communication and learning devices are secure
It helped me protect the school email account, learner and teacher digital devices.

“I was able to apply use VPNs, managing cookies, and blocking websites as I utilized learning platforms. Additionally, the encryption of sensitive data such as students' and parents' personal data and students' grades was meaningful.”

I have learned skills in document sharing with students and securing their scores and data. I can also support the institution to understand the risks involved in online classes.
Open Resources Available
Inferences for Policy and Practice

• Cyber safety and security topics should be included in teacher training at the pre-service level
  • New curricula must be developed through international cooperation
• Few developing countries have cyber safety regulations in place and the number needs to increase
• Governments should consider ways to offer secure internet for schools and institutions
Thank you