Capacity-building of teachers and parents in cyber safety and security: The COL experience

24 November 2022

Video Presentation
International Conference on Cyberlaw, Cybercrime and Cybersecurity
India

Presented by Professor Asha Kanwar
President & CEO, Commonwealth of Learning (COL)

Co-written with Dr V Balaji, Vice President, COL, and
Dr Betty Ogange, Education Specialist: Teacher Education, COL

Let me begin by thanking Mr Pawan Duggal, Chancellor of Cyber Law University for the invitation to share the experience of the Commonwealth of Learning in cyber security and safety. The Commonwealth of Learning or COL is an intergovernmental organisation established by Heads of Commonwealth Governments when they met for CHOGM in 1987. Our headquarters are in Metro Vancouver, Canada with a regional office in New Delhi. COL's mandate is to help governments and institutions expand access to quality learning education and training through the use of technologies.

Covid-19 caused the worst disruption in human history where neither governments nor institutions were prepared. With its expertise in distance and online learning, COL provided various instruments, guidelines and resources to help stakeholders deal with the learning crisis and develop resilient systems and strategies to deal with future disasters.

Teachers around the world needed support with integrating ICT into teaching and COL offered online training to teachers in many Commonwealth countries. In Trinidad and Tobago COL's training covered almost half of all the teachers in the country. Similarly the coverage was extensive in Fiji and other Pacific island countries.

During the pandemic. parents and siblings had a key role to play in ensuring continuity in learning. COL launched a set of projects in Ghana to sensitise over 4800 parents in how to contribute to uninterrupted learning. In partnership with the UNESCO Institute of Lifelong Learning two online courses were developed on family and inter-generational learning.

The increasing use of technology highlighted the salience of cyber safety for all stakeholders: students, teachers, and parents. Students and parents often shared one device. Students were either not aware of or disregarded essential safety norms while online. This led to many attacks on students as well as parents which spread to the teachers as well.

Commonwealth of Learning CC BY-SA 4.0

Common examples include loss of identity, and hacking of email and social media accounts. In some institutions Zoom sessions were 'bombed" disrupting classes and requiring disciplinary measures.

Disruption of classes was just one consequence of a cyber attack. Others included significant delays in assessments; or loss of learning materials or loss of access to course platforms. Hacking and impersonation eroded the trust between students and teachers. Cyberbullying led to an adverse impact on the mental health and well-bring of both teachers and students.

Teachers are the most important intermediaries in averting cyber attacks and managing the impacts on learning. They can help students in observing cyber safety norms. However, their capacities need to be built. It is significant that UNESCO recognised their role even before Covid-19 advocated for building their "e-readiness" in cyber security. Lack of resources to manage cyber security in institutions is also a known limitation.

COL offered cybersecurity courses using COL's MOOC platforms and attracted about 7,000 teachers from 96 countries. The topics covered: introduction to cybersecurity; cyber safety; and data protection from cyber attacks. Ensuring the security of online communications and devices was an important aspect of this course. The post-course surveys showed that the outcomes were positive. Some teachers felt they could now apply measures for protecting access devices and email accounts. Others felt that they now understood how the impact could be different for learners with disabilities. A few teachers said that they were able to apply the lessons learned to protect the student-facing systems such as LMS better and initiate measures to prevent malicious software in students' devices. In general, many felt that they had improved knowledge of cyber risks in learning and could help their institutions.

What is important is that many teachers are willing to sensitise others for which COL developed two manuals. These are OER and can be adopted or adapted in different contexts.

With the growing ubiquity of technology, it is clear that cyber safety and security must be integrated in pre-service teacher training. Many countries may not be able to develop the curricula on their own and this is where international cooperation becomes necessary. Most countries still do not have cyber safety regulations in place and that needs to change. Governments will have a key role to play in offering secure internet to schools and teaching institutions to minimise disruptions from cyber attacks. This is an urgent matter that requires urgent attention.

Commonwealth of Learning CC BY-SA 4.0