Inputs for a Study on Solutions to Promote Digital Education for Young People and to Ensure Their Protection from Online Threats

CALL FOR INPUT | OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS

January 30, 2024

(Edited by Harisa Shahid, Ankita Rathi, and Jenna Manhau Fung, Kenneth Leung)

Overview

In consideration of the NetMission'sAsia-Pacific Policy Organization (APPO) submission, which builds upon two reports focusing on the online safety policies of Australia, Nepal, and Myanmar, we can offer a succinct framework or set of recommendations through the lens of a tailored approach, emphasizing "accessibility, awareness, and accountability." This approach acknowledges that a one-size-fits-all solution is not feasible due to varying eSafety levels across these countries.

(a) Accessibility in Low eSafety Regions (Myanmar): For countries like Myanmar, where eSafety is low, the priority should be ensuring open and unrestricted Internet access and promoting digital education. This involves integrating strategies from our reports, such as the use of VPNs to circumvent Internet restrictions and advocating for Internet freedom. The aim is to provide an environment where information is freely accessible and digital literacy can flourish.

(b) Awareness in Mid-Level eSafety Regions (Nepal): In countries like Nepal, with a moderate level of eSafety, the focus should shift towards narrowing the digital divide and enhancing eSafety awareness. This includes embedding practical skills and Internet usage practices into school curriculums. Our reports suggest specific strategies for combating issues like cyberbullying, providing a foundation for developing these practical skills.

(c) Accountability in High eSafety Regions (Australia): For countries with a high level of eSafety, such as Australia, the emphasis should be on fostering digital citizenship and wellbeing, along with other more abstract concepts. In this context, our reports provide a basis for developing eSafety recommendations and advice, including measures to counter child sexual abuse material (CSAM). The goal here is to cultivate a responsible and ethically aware digital community.

This three-pronged approach of "accessibility, awareness, and accountability" caters to the specific needs and eSafety levels of different countries, providing a nuanced and effective strategy for enhancing digital safety and education in the Asia-Pacific region.

Description of entity/organization

NetMission.Asia is a network of passionate young people in Asia Pacific dedicated to engaging and empowering youth on Internet governance discourse to create an impact in Asia Pacific. Supported by DotAsia Organisation, NetMission.Asia has been actively participating in various Internet conferences both regionally and globally, including ICANN meetings, IGF, APrIGF, and Asia Pacific Internet Governance Academy (APIGA). NetMission.Asia has also been organizing the annual Youth Internet Governance Forum (yIGF) around Asia Pacific since 2010 to support and encourage youth participation in Internet governance.

Contact information

- Email: info@netmission.asia
- Website: https://netmission.asia

Accessibility, Awareness and Accountability

Our research has focused on the eSafety landscape in Myanmar, Nepal, and Australia, recognizing the diverse challenges each country faces in promoting digital education for young people and safeguarding them from online threats. Understanding that there is no one-size-fits-all solution, our framework revolves around the key pillars of Accessibility, Awareness, and Accountability.

In regions with low eSafety levels like Myanmar, our recommendations highlight the importance of an open and non-obstructed Internet to ensure unimpeded access to digital education. For countries with mid-level eSafety, such as Nepal, our emphasis lies in narrowing the digital divide and enhancing eSafety awareness, focusing on practical skills integrated into school curriculums. In high eSafety regions like Australia, the focus shifts to accountability, with recommendations revolving around fostering digital citizenship, digital well-being, and addressing more abstract concepts. Our approach acknowledges the specific needs of each country, providing more tailored solutions to address the distinct challenges faced by young people in the digital realm.

Myanmar

Myanmar, as in many of its Asia Pacific neighbours experiences a digital divide, with disparities in Internet access and infrastructure, making equitable access to digital education a big problem According to the GSMA report on Mobile Phone, Internet & Gender in Myanmar, women in Myanmar are 29% less likely to own a mobile phone than men, according to the national baseline survey. This gender gap in ownership was higher among lower-income households. Limited technological infrastructure in remote areas is a significant hurdle faced by marginalized youth, hindering their ability to fully participate in digital learning.

According to the Digital 2023 Mayanmar Report , Myanmar's Internet penetration rate stood at 44.0 percent of the total population in 2023 which is indeed a significant rise from previous years but still 56.0 percent of the population remained offline at the beginning of the year.This stark disparity leaves countless young people, especially those residing outside major urban centers, excluded from the digital realm. Then comes the challenge of Device Affordability, even in areas with Internet availability, affordability remains a critical obstacle. The high cost of devices, coupled with limited disposable income in many households, creates a significant barrier to entry.

The ***low eSafety*** level in Myanmar is a significant challenge for young people in accessing digital education, especially in marginalized and vulnerable situations. The 2022 draft Cyber Security Law, if enacted, threatens Internet freedom by allowing authorities to block websites and criminalize the use of Virtual Private Networks (VPNs). Article 62 of the draft law specifically ***criminalizes the use of VPNs without permission***. This could result in ***restricted access* to online educational resources**, impacting young people, especially those in marginalized and remote areas.

The usage of VPNs is also banned in other countries such as China, Russia, Belarus, North Korea, Turkmenistan, Uganda, Iraq, Turkey, UAE, and Oman. Specifically, China has already banned the use of popular social media platforms and search engines such as Facebook and Google. These restrictions are a big challenge for young people in vulnerable situations to access available digital resources for education easily.

Without access to online resources and platforms, marginalized youth fall further behind their peers who enjoy digital connectivity. This widens the educational gap and young people lacking Internet access miss out on crucial information and training regarding online safety practices, leaving them vulnerable to ***cyberbullying, misinformation, and online exploitation.*** Furthermore, The lack of access to technology restricts opportunities for young people to develop essential digital skills, crucial for future employment and participation in the digital economy.

By ***prioritizing accessibility***, we can lay the foundation for a safer and more inclusive digital environment in Myanmar. Empowering young people with knowledge and skills through accessible digital education is crucial for their protection and participation in the digital world. We urge OHCHR and the international community to support initiatives that promote ***open Internet access***, ***digital literacy***, and ***responsible online behavior*** in Myanmar.

Nepal

According to a statement from Nepal's Cyber Bureau, the number of cybercrime cases in the nation has sharply increased in the last 12 months. Between September 2022 and April 2023 alone, the Bureau had registered a total of 4,936 cases, a number higher than all cases registered in the whole fiscal year (4486 cases). Authorities cite that the problem is compounding due to inadequate technical human resources and a lack of a comprehensive framework to curb such instances effectively. According to the Bhotahity-based bureau of Nepal police, there have been a total of 16,190 complaints since 2020. To visualize the frequency and intensity of online safety incidents, it gets an average of 60 to 70 complaints a day.

As a legal attempt, the Nepali government passed The Cyber Security Bylaw 2077, the Electronics Transactions Act, 2063, and the Privacy Act 2075 to protect data privacy at the individual level, IT infrastructure at the organizational level and Internet usage at the commercial level. All of them have impacts on shaping the cybercrime sphere in Nepal. But are these regulations sufficient to be comprehensive? The existing framework is not very comprehensive and strong enough to deter criminals or bullies online. For instance, there is a lack of clarity on the definition of the term, “cyberbullying itself”. Further, Nepal also faces challenges in terms of enforcement, awareness, coordination, and capacity building among relevant stakeholders to prevent a cyberbullying instance or reporting after it has occurred.

In Nepal, the prevalence of cybercrimes like financial fraud, identity theft, phishing, and malware, especially when students and educators use digital platforms, places the country at a ***moderate level of eSafety risk***. This deters the use of online resources, limits the accessibility of digital tools, and hinders the adoption of e-learning methodologies. The ***prevalence of cybercrimes underscores the necessity for digital literacy and cybersecurity education as integral components of digital education***. Students and teachers need to be educated on how to identify and protect against such threats.

Educators should be trained not only in digital tools and e-learning methodologies but also in online safety which will enable them to guide students effectively and incorporate eSafety practices into their teaching. Interactive and engaging content such as videos, infographics, and webinars can be particularly effective. Peer-to-peer education programs can also be effective, as young people often relate better to their contemporaries. Workshops or information sessions for parents can help them understand the online environments their children are navigating. Utilizing community centers and libraries as hubs for digital literacy training can make resources accessible to a broader audience, including those in rural areas. Engaging popular media personalities and social media influencers to spread awareness about digital literacy and cybersecurity can be a powerful tool, especially for youth.

By prioritizing ***Awareness***, in Nepal, the government and educational institutions can take significant steps towards mitigating the risks associated with cybercrime. We urge OHCHR to apply/follow these recommendations for the countries which have a moderate level of eSafety risk. These recommendations may help them ***create a more informed and cautious digital community***, particularly among young people, and ***foster an environment where digital education and online resources are utilized safely and effectively***.

Australia

In the landscape of securing a digital environment and promoting digital education for the youth, the principle of “***Accountability***” stands out as a pivotal solution. Accountability serves as the key element for building trust, transparency, and responsible digital behavior. Australia serves as a noteworthy example where robust measures have been implemented to ensure accountability in the digital realm. Its digital landscape, known for its robust infrastructure, requires a strategic approach centered around nourishing ***digital citizenship*** and advancing ***digital well-being***. As the country witnesses an increasing integration of the Internet into daily life, the government has implemented crucial measures to ensure the protection of its citizens, particularly young people, in the digital realm.

The Online Safety Act of 2021, enacted in February 2021, reflects a comprehensive effort to modernize regulatory frameworks and combat the rising instances of online harm. The Act provides new powers and resources to the eSafety Commissioner, who plays a pivotal role in overseeing online safety. Notably, the legislation emphasizes a ***risk-based approach***, holding online service providers accountable for the safety of their users. The Act categorizes harmful online content into "Class 1" and "Class 2," addressing issues such as child sexual exploitation material and terrorist content. It establishes clear expectations for online service providers, including social media platforms and search engines, urging them to develop industry codes and mechanisms to prevent the distribution of harmful content.

Moreover, the eSafety Commissioner has been granted substantial authority to issue removal notices and impose fines on non-compliant platforms. The Online Safety Act not only focuses on individual harms but also addresses collective harms, highlighting the importance of a coordinated effort across regulatory bodies such as the ACCC and ACMA. The establishment of the Digital Platform Regulators Forum in 2022 underscores the government's commitment to fostering collaboration among regulatory bodies to tackle issues like algorithmic impact and enhance transparency in digital platforms' activities.

By holding online platforms accountable for the content they host, Australia ensures that digital educational materials meet high standards of ***accuracy***, ***appropriateness***, and ***reliability***. This commitment to accountability minimizes the presence of misinformation and harmful content in the digital learning environment, thereby fostering a more conducive atmosphere for education.

As the government progresses with the implementation of industry codes, it remains crucial to strike a balance between protecting online safety and respecting user privacy. The recent fines imposed on online platforms, including Elon Musk's social media platform X, demonstrate a commitment to enforcing online safety standards. The implementation of measures against Child Sexual Abuse Material (CSAM) showcases the commitment to protecting users, especially minors, from online threats.

This proactive stance not only upholds the nation's commitment to online safety where education can thrive but also sets a benchmark for other regions grappling with similar challenges in the digital realm.