CHILD SAFETY AND MONITORING DEVICE IDEATION

Given that the cyber world is a permanent feature of children's lives today, and that there are associated risks and benefits with this exposure to technology, how do we know what makes cyber safety strategies effective? As mentioned earlier, there is a lack of literature examining effective approaches to children and online safety. Most of the cyber safety literature has been dominated by studies on cyberbullying and online sexual exploitation of children rather than on what works, and on immediate rather than long term outcomes. 58 The needs of children have not been a priority in the literature. 59 In response to these challenges, a different approach to cyber safety has emerged which seeks to understand the reasons that make children and young people vulnerable to risks and to develop strategies accordingly. This new body of research on cyber safety has moved away from a fear-driven discourse to a well-informed, multi-dimensional discourse where the interplay between online and offline worlds is being documented and investigated. Emerging research is also documenting children and young people's skills, perspectives, and vocabulary about the cyber world. Such an approach is strengths-based, recognises and respects children's agency, and advocates for digital literacy of all stakeholders to help them navigate through the cyber world. Child rights and strengths-based approach: Earlier literature on cyber practices and digital citizenship framed children and young people in a limited, moralistic, and risk-dominated approach. More recent studies advocate the use of a child-rights approach, where children and young people have the right to access accurate and age-appropriate knowledge about the online world with equitable access to safe reporting pathways and legal processes. This approach is strengths-based60 (building on existing child and youth cultures, skills, and capabilities) and maximises the benefits of online engagement and limiting harm. 61 Promoting critical thinking in young minds: Another approach to cyber safety for children and young people draws on Vygotsky's theory of everyday concepts to advocate for an incremental approach to building children's knowledge about the online world, starting from when they are young (as early as two years old). 62 According to this approach, parenting and teaching approaches should merge everyday concepts with scientific concepts. For instance, as young children are taught about the concept of

stranger-danger in the real world, they need to be informed about the consequences of clicking pop-ups or in-app messages or requests in the online world. The studies highlight the importance of understanding how children perceive the internet and how their views are being shaped through their everyday online interactions. Age-appropriate exploratory discussions about how online information is 'socially constructed and distributed, and how it can be globally accessed' between children and adults has been found to be an effective cyber safety strategy. 63 Data from the 2019 Global Kids Online study shows that as children grow up, they climb the ladder of online participation, as seen in this image below. 64 Children start by enjoying videos, playing games, learning for school homework, and move on to civic participation, increasing their operational knowledge as they climb.

National and international approaches to address cyber safety

Using strategies to build resilience are not sufficient on their own to build digital literacy in children and young people and other stakeholders. These also need to be supported by policies and legal frameworks. 'Internet governance' has expanded from technical infrastructure to the domains of cybersecurity, human rights, and e-commerce and sits across multiple entities such as governments, private sector and civil society. This section explores some of the multi-stakeholder initiatives that have been implemented, emerging practices and approaches to cyber safety. The literature documents a rise in collaborative practices in research, program development, legislative policies and even cybercrime fighting. A recent OECD study surveyed 34 countries about their legal and policy responses regarding online safety for children. The study shows how governments are caught between balancing the complexities of managing the digital world and minimising harm while supporting greater use of technology. The study shows the different approaches adopted by countries in responding to such a challenging environment