KINGDOM OF ESWATINI

ESCCOM ESWATINI COMMUNICATIONS COMMISSION

SZ CIRT ESWATINI COMPUTER INCIDENT RESPONSE TEAM

unesco

OUR RIGHTS OUR LIVES OUR FUTURE

Eswatini Online Safety Landscape

Keeping Children Safe in the Digital Environment

Eswatini Online Safety Landscape

Keeping Children Safe in the Digital Environment

The explosion of information and communication technology (ICT) has created unprecedented opportunities for adolescents and young people to know their rights. More and more children are connecting for the first time every day, either on personal or shared devices. However, wider and more easily available access to the Internet and digital technology also poses significant challenges to children's rights, including their safety.

Impacts range from threats to protection of personal data and privacy, to harassment and cyberbullying, harmful online content, grooming for sexual purposes, and sexual abuse and exploitation. Addressing the national challenge of child online protection in Eswatini requires a unified and strategic response, anchored in national coordination and reenforced through international cooperation. With more reliance on digital technologies, the COVID-19 pandemic aggravated previously existing risks for children online and stressed the urgent need for action. The challenges and threats persist due to the borderless nature of the online environment among other reasons. An inclusive, multifaceted child online protection strategy with effective and targeted measures and activities including financial and human resources to implement the strategy is necessary at all levels.

Only with a coordinated and cooperative multi-stakeholder approach will children and future generations be protected and empowered to thrive in digital environments.

With 69 per cent of young people online in 2019, and one in three children with Internet access at home, the Internet has become an integral part of children's lives, presenting many possibilities for children and young people to communicate, learn, socialize and play, exposing children to new ideas and more diverse sources of information, opening opportunities for political and civic participation for children to thrive, be creative, and meaningfully contribute to a better society. The internet has become a viable means for access to basic education, social interactions, and access to help and support services.

The importance of protecting and empowering children in Eswatini

While supporting and promoting children's rights, the same online environment may expose children to risks, some of which can translate into potential harms. In Eswatini, the rise in cyberbullying, sexual grooming, and digital exploitation has been noted since 2019, with reports increasing amid the pandemic. Cyberbullying incidents have increased by 55 per cent since 2015, affecting students' emotional well-being and academic performance. Incidents of online predation doubled during the pandemic, highlighting the need for vigilance in digital spaces. Child online protection therefore seeks to reduce risks and protect children from harms they may encounter online. These include:

Content risks: exposure to inaccurate or incomplete information, misinformation, disinformation, inappropriate or even criminal content such as exposure to adult/extremist/violent/gory content, self-abuse and self-harm related content, destructive and violent behaviour, radicalization or subscribing to racist or discriminatory ideas.

Contact risks from adults or peers: harassment, exclusion, discrimination, defamation and damage to reputation, gender-based violence GBV) and sexual abuse and exploitation including extortion, grooming (sexual), child sexual abuse material, trafficking and sexual exploitation of children in travel and tourism as well as extremist recruitment.

Contract risks: exposure to inappropriate contractual relationships, children's consent online, embedded marketing, online gambling, as well as violation and misuse of personal data such as hacking, fraud and identity theft, scams, profiling bias.

Conduct risks: such as sharing of self-generated sexual content or risks characterized through hostile and violent peer activity such as cyberbullying, stalking, exclusion and harassment.

More than a third of young people in 30 countries report being cyberbullied, with 1-in-5 skipping school because of it. Some 80 per cent of children in 25 countries report feeling in danger of sexual abuse or exploitation online.

A Framework for School Cybersecurity

At the national level in Eswatini, child online protection efforts are guided by the Computer Crime and Cybercrime Act of 2022, which outlines offences related to digital harm, including cyberbullying, exploitation, and unauthorized access. However, implementation remains fragmented. Few relevant stakeholders are meaningfully engaged, and children, along with their parents, carers, and guardians, are seldom consulted in policy design or response mechanisms. The Children's Protection and Welfare Act of 2012 and the Sexual Offences and Domestic Violence Act of 2018 provide broader frameworks for safeguarding children, yet online safety is rarely integrated into these systems.

The private sector's responsibilities toward children's digital rights are often overlooked, and online safety mechanisms are seldom embedded within the national child protection and violence prevention agenda. The complexity of risk and protective factors—and the interlinkages between offline and online violence against children—are not consistently recognized or addressed. Without harmonized strategies or cross-sectoral coordination, efforts to promote child online safety remain sporadic and limited in scale.

Challenges remain in the development of necessary national policy frameworks with regard to safety-by-design of digital platforms, digital literacy and broad societal awareness of child online protection issues. Without filling these gaps, the transition towards an inclusive digital environment with economic and social inclusion will remain hard to achieve, bringing further consequences for the national economy and beyond. At the design and solutions development level, there is also an opportunity to bring industry and child participation together. Examples of these efforts include Eswatini's partnerships with UNESCO and the National Cybersecurity Agency (ESCCOM) for developing cyber safety guidelines.

A framework of five foundational pillars to create a secure digital environment in schools is proposed:

Pillar	Description
Governance, Leadership, and Accountability	Establishes structures for oversight, with clear accountability for school leaders and national agencies like ESCCOM.
Secure and Resilient Digital Infrastructure	Requires "Security by Design" for networks, devices, and platforms, including firewalls, updates, and parental controls.
Digital Citizenship and Curriculum Integration	Integrates digital literacy into education, focusing on skills like critical thinking and responsible behavior to build a "human firewall."
Whole-of-Community Engagement	Involves parents, educators, and communities in awareness and prevention efforts.
Incident Response and Resilience	Prepares for incidents with reporting mechanisms, counseling, and recovery plans to minimize harm.

These pillars align with ITU recommendations for holistic strategies, including international cooperation and child participation in policy development. The framework is accompanied by guidelines and toolkits for school online safety for School Administrators, Teachers and Librarians, Parents, and Children.

Call to action

Eswatini must prioritize a national Child Online Protection Strategy, aligning with UN CRC General Comment No. 25 (on children's rights in relation to the digital environment)https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation . This includes:

- Integrating digital literacy into curricula, with modules on child online safety, responsible digital citizenship and technology-facilitated GBV.
- Strengthening reporting mechanisms (e.g., helplines like 116) and whistleblowing systems for digital abuse or misconduct.
- Fostering multi-stakeholder collaboration among government, schools, parents, and industry, including empowering educators, parents, and adolescents with tools to recognize and respond to risks like cyberbullying, online grooming, sextortion, and online predation.
- Investing in empowerment through civic education on rights, resilience, and risks, promoting safe use of platforms like WhatsApp and Instagram (prevalent among youth

for communication but prone to misinformation and cyberbullying), and building digital citizenship skills to navigate harms.

- Adopting best practices such as strengths-based approaches, whole-school strategies, and continuous review to ensure programmes address emerging risks and support help-seeking behaviors.