KINGDOM OF ESWATINI

ESWATINI COMMUNICATIONS COMMISSION

SZ CIRT ESWATINI COMPUTER INCIDENT RESPONSE TEAM

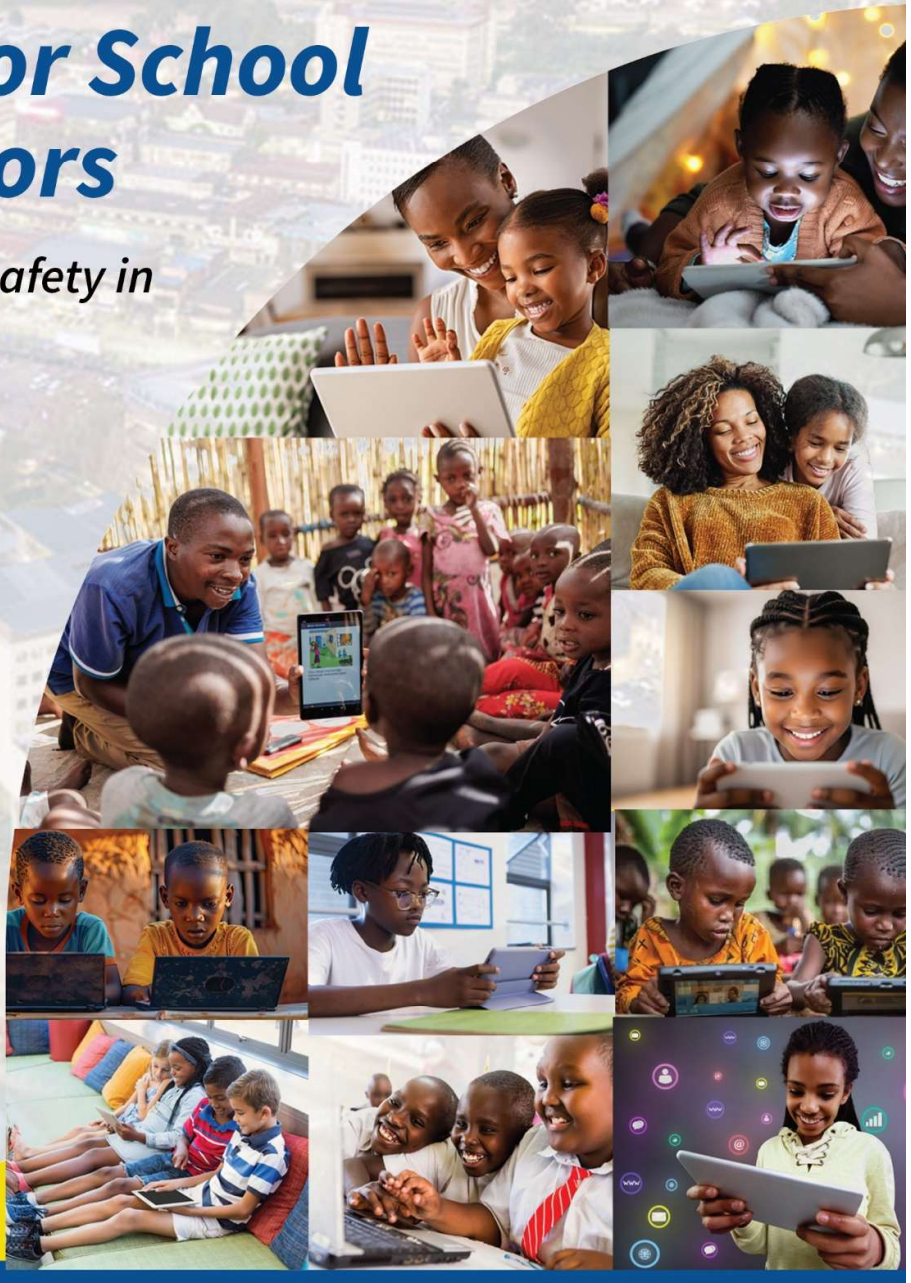
unesco

OUR RIGHTS OUR LIVES OUR FUTURE

ESWATINI CHILD ONLINE SAFETY GUIDELINES

Guidelines for School Administrators

Promoting Child Online Safety in Eswatini Schools



Guidelines for School Administrators

Promoting Child Online Safety in Eswatini Schools

Summary

In an era where digital connectivity is transforming education and daily life, safeguarding young people's online experiences is a critical responsibility. This document offers detailed guidance for school administrators in Eswatini to build and maintain safe digital environments for adolescents and young people. It emphasizes the need for robust policies, technical measures, training, and collaborations to address online risks while harnessing the benefits of technology. Key areas include governance, cybersecurity implementation, staff development, and community partnerships.

By focusing on students' rights to protection and participation, respecting their diversity, and using strengths-based approaches, administrators can foster resilience and prevent harm. The guidelines promote continuous improvement through regular reviews, data-driven assessments, and professional learning. Implementing these strategies will enhance student wellbeing, academic performance, and digital citizenship, aligning with national laws like the Eswatini Computer Crime and Cyber Act (2002) and broader goals for equitable education.

Introduction

Digital technologies offer immense opportunities for education, enabling access to knowledge, collaboration, and innovation. However, they also introduce risks that can affect students' safety and development. School administrators play a central role in creating environments where students can engage online responsibly and securely.

This guide provides practical, evidence-based strategies to help administrators design, implement, and evaluate online safety programmes. The focus is on recognizing students' rights in digital spaces, building awareness of risks without exaggeration, and promoting whole-school involvement to support every student's needs, regardless of gender, age, culture, ability, or location.

By adopting these guidelines, administrators can ensure online safety education is taught to every student at every level, using engaging methods and clear goals. This approach not only prevents harm but also empowers students to participate meaningfully in their digital education.

Importance of School Administrators in Online Safety

School administrators are essential leaders in promoting student wellbeing and preventing harm in digital environments. They oversee the integration of online safety into school operations, from policy creation to resource management and stakeholder engagement. This leadership ensures that safety measures are comprehensive, addressing both technical and relational aspects needed for students to navigate online spaces confidently.

Administrators help bridge gaps in access and skills, where device shortages and limited connectivity in rural areas exacerbate vulnerabilities. They play a key role in upholding students' rights to provision, participation, and protection online, acknowledging the opportunities technology provides while understanding that risks vary by platform, usage patterns, and individual factors. For instance, cyberbullying impacts emotional health and learning, while identity theft from weak accounts affects 1 in 50 children globally.

By modeling ethical behavior and fostering a supportive culture, administrators build resilience among students, encouraging help-seeking and critical thinking. Their efforts extend to partnerships with parents, educators, and external services, creating networks for advice and support. Ultimately, strong administrative leadership invests in students' future, enhancing their ability to use technology positively and reducing the likelihood of harm.

Guidelines:

1. **Governance and Risk Management**
   Effective governance ensures online safety is embedded in school structures, with regular reviews to identify and address weaknesses. This involves creating dedicated teams and policies that evolve with emerging issues.

   Actions:
   - Establish a school cybersafety team including administrators, teachers, parents, and students. Hold quarterly meetings to review incidents, update strategies, and share good practices for ongoing improvement.
   - Develop a tailored cybersafety policy that outlines rules for device use, data handling, and responses to issues like content exposure, contact from strangers, contractual risks (e.g., online scams), and conduct problems (e.g., bullying). Incorporate national laws such as the Eswatini Computer Crime and Cyber Act (2002) to cover risks including inappropriate content, harassment, and data misuse.
   - Conduct annual risk assessments to spot vulnerabilities, such as outdated networks or lack of monitoring on shared devices. Use data from these assessments to prioritize actions and ensure relevance to current threats.
   - Include cybersafety as a regular agenda item in governing body meetings. This promotes accountability and supports secure procurement processes for IT equipment and vendors, ensuring all purchases meet safety standards.
   - Safeguard personal data by complying with privacy regulations. Train staff on handling sensitive information and implement systems to detect and respond to breaches promptly.
   - Focus on student diversity in risk management, adapting measures for varying needs based on age, ability, socioeconomic background, or location. For example, provide accessible tools for students with disabilities to ensure equitable protection.

2. **Implementing Strong Cybersecurity Measures**
   Technical controls are foundational to preventing unauthorized access and harmful content. Administrators should prioritize measures that balance security with usability, avoiding overly restrictive approaches that could hinder learning.

   Actions:
   - Install firewalls, antivirus software, and secure networks to block threats. Enforce multi-factor authentication for all accounts to add layers of protection.

- Use content filtering and monitoring tools to restrict access to inappropriate material, such as violent or exploitative content, while respecting student privacy and avoiding surveillance that erodes trust.
- Enforce robust password policies: Require passwords with at least 8 characters, including a mix of letters, numbers, and symbols (e.g., Sh@#!$123), and set them to expire every 30 days. Use meaningful usernames and non-administrator logins for daily activities.
- Educate the school community on specific risks, including email phishing, hacking attempts, social engineering tricks, unsafe internet links, online subscriptions that collect data, and sharing personal identifiable information (PII). Provide examples of how these can lead to issues like identity theft or sextortion.
- Promote anonymous reporting mechanisms, such as whistleblowing systems or dedicated apps, for students and staff to flag incidents like online coercion or blackmail without fear of reprisal.
- Regularly update systems to address emerging technologies, such as IoT devices (e.g., connected smart boards) that may collect data, ensuring they do not introduce new vulnerabilities.

3. **Training and Awareness**

   Building capacity through education ensures that everyone in the school understands online safety. Training should use strengths-based methods, highlighting positive uses of technology while increasing awareness of factors that heighten or reduce risks.

   Action:

   - Mandate annual training for all staff on online safety, covering topics like recognizing signs of distress, managing emotions in digital interactions, and fostering respectful relationships. Track participation and include it in professional evaluations.
   - Proactively identify and disseminate free, high-quality cybersafety training courses to management and staff. This supports ongoing capacity building, strengthens digital literacy, and promotes a safer, more responsible online environment across the institution.
   - Require staff and students to sign an Acceptable Use Policy at the start of each year, which details expectations for ethical behavior, such as avoiding scare tactics in discussions and providing feedback on skills development.

- Cultivate an open environment where concerns can be reported without judgment. Encourage discussions that empower students to participate in their own safety education.
- Collaborate with organizations like ESCCOM for workshops on trends, including biases in machine learning tools or risks from loot boxes in games. Tailor sessions to build resilience, understanding that not all online risks result in harm.
- Ensure training is inclusive, meeting diverse needs—for example, providing materials in multiple formats for staff and students with disabilities or from rural areas with limited access.
- Share successful practices among schools to improve collectively, such as case studies of how addressing peer pressure has reduced addictive tech use.

4. **Collaborative Safety Measures and Advocacy**

   Online safety thrives through partnerships that extend beyond the school. Administrators should build supportive networks and advocate for broader changes to create sustainable protections.

   Actions:

   - Partner with parents, teachers, librarians, and community organizations for referrals, advice, and support. For instance, host joint sessions on help-seeking strategies and where to obtain guidance.
   - Integrate online safety into the school curriculum, teaching digital citizenship, media literacy for critical thinking, and social-emotional skills to manage relationships and resilience.
   - Address common vulnerabilities: Explain how cyberbullying affects wellbeing and how weak accounts lead to identity theft. Promote positive approaches, focusing on opportunities like civic engagement online.
   - Familiarize the community with national helplines (e.g., 116) and international tools like report abuse buttons for harmful content. Teach students how to block offenders and preserve evidence without sharing explicit material.
   - Advocate for policy improvements, such as government investments to expand ICT labs to 80% coverage in high schools by 2028/29, ensuring equitable access and safety.
   - Engage students in designing safety initiatives, empowering them to openly share their concerns and contribute ideas that reflect their experiences and promote meaningful participation.

Child Online Safety Checklist for Administrators

Use this checklist to assess and track progress:

Governance and Risk Management

- Have you established a school cybersafety team that includes administrators, teachers, parents, and students to ensure diverse perspectives?
- Do you schedule quarterly meetings for the cybersafety team to review recent incidents (e.g., bullying or data breaches) for lessons learned?
- During team meetings, do you update strategies based on new threats or feedback?
- In team meetings, do you share good practices, such as successful interventions or preventive measures, to foster ongoing improvement?
- Have you developed a tailored cybersafety policy that outlines clear rules for device use (e.g., acceptable times, locations, and purposes)?
- Does your cybersafety policy define protocols for data handling, including storage, sharing, and deletion?
- Does your cybersafety policy specify responses to common issues, such as exposure to harmful content (e.g., filtering guidelines), contact from strangers (e.g., reporting protocols), contractual risks (e.g., avoiding online scams or unauthorized subscriptions), and conduct problems (e.g., cyberbullying or harassment)?
- Have you incorporated relevant national laws, such as the Eswatini Computer Crime and Cyber Act (2002), into your cybersafety policy to ensure legal compliance?
- Does your policy address specific risks covered by laws, including inappropriate or harmful content, online harassment, and data misuse (e.g., unauthorized access or sharing)?
- Does your policy include provisions for annual reviews to evolve with emerging issues?
- Do you conduct annual risk assessments to identify vulnerabilities in infrastructure, such as outdated networks, unpatched software, or insufficient monitoring on shared devices?
- In your risk assessments, do you collect data from sources like incident logs, user feedback, and external threat reports?
- Do you prioritize actions based on risk assessment findings (e.g., addressing high-risk areas like weak Wi-Fi security immediately)?
- Do you ensure risk assessments remain relevant by aligning them with current threats, such as new social media trends or AI-related risks?
- Do you include cybersafety as a regular agenda item in governing body meetings?

- In governing body meetings, do you promote accountability by assigning roles for oversight (e.g., who reports on progress)?
- Do you support secure procurement processes by evaluating IT equipment and vendors for safety standards (e.g., data encryption, compliance certifications)?
- Do you ensure all purchases prioritize safety without compromising educational value?
- Do you comply with privacy regulations (e.g., data protection laws relevant to Eswatini or international standards like GDPR influences) to safeguard personal data?
- Have you trained staff on handling sensitive information, covering collection, use, storage, and disposal practices?
- Have you implemented detection systems (e.g., alerts for unusual access) and response protocols for data breaches (e.g., notification timelines, mitigation steps)?
- Do you adapt risk management measures to individual student needs based on age (e.g., simpler rules for younger students), ability (e.g., tools for neurodiverse learners), socioeconomic background (e.g., alternatives for those without home devices), or location (e.g., offline resources for rural areas)?
- Do you provide accessible tools and protections, such as screen readers or voice-activated safety features, for students with disabilities to ensure equitable safety?

Implementing Strong Cybersecurity Measures

- Have you installed antivirus software to detect and remove malware?
- Have you set up secure networks (e.g., encrypted Wi-Fi) to prevent interception of data?
- Do you enforce multi-factor authentication (MFA) for all accounts, including email, learning platforms, and admin systems?
- Do you use content filtering tools to restrict access to inappropriate material, such as violent, exploitative, or age-inappropriate content?
- Do you respect student privacy by limiting monitoring to necessary levels (e.g., avoiding constant surveillance)?
- Do you avoid approaches that erode trust, such as overly invasive tracking, while focusing on educational benefits?
- Do you require passwords with at least 8 characters, including a mix of uppercase/lowercase letters, numbers, and symbols (e.g., Sh@#!$123)?
- Do you set passwords to expire every 30 days and prohibit reuse of recent passwords?
- Do you use meaningful usernames that do not reveal personal information?

- Do you mandate non-administrator logins for daily activities to minimize risks from elevated privileges?
- Have you educated the school community on recognizing email phishing, such as suspicious emails with urgent requests for information?
- Have you addressed hacking attempts by explaining common methods like brute-force attacks?
- Have you discussed social engineering tricks, such as manipulation via fake calls or messages?
- Have you highlighted unsafe internet links and advised checking URLs before clicking?
- Have you warned about online subscriptions that collect data, including hidden terms and privacy implications?
- Have you educated on sharing personal identifiable information (PII), providing examples of risks like identity theft or sextortion?
- Do you use real-world examples to illustrate how these risks lead to harm?
- Have you implemented whistleblowing systems or dedicated apps for anonymous reporting of incidents?
- Do your reporting mechanisms cover issues like online coercion, blackmail, or other threats?
- Do you ensure reports can be made without fear of reprisal, with clear confidentiality policies?
- Do you conduct updates and patches promptly to close security gaps in systems?
- Do you evaluate new technologies, such as IoT devices (e.g., connected smart boards), for risks before integration?
- Do you address vulnerabilities from IoT devices that may collect data, ensuring no new vulnerabilities are introduced?

Training and Awareness

- Do you mandate annual training for all staff on recognizing signs of distress (e.g., withdrawal due to online issues)?
- Does staff training cover managing emotions in digital interactions (e.g., de-escalating conflicts)?
- Does staff training focus on fostering respectful relationships online?
- Do you track staff training participation through records or certifications?
- Do you include training compliance in professional evaluations to encourage participation?
- Do you require signatures from staff and students on an Acceptable Use Policy (AUP) at the start of each year?
- Does the AUP detail expectations for ethical behavior (e.g., respectful communication, no sharing of harmful content)?

- Does the AUP avoid scare tactics and instead provide constructive feedback on skills development?
- Do you encourage reporting of concerns without judgment?
- Do you promote discussions that empower students (e.g., peer-led sessions)?
- Do you involve students in their own safety education to build ownership?
- Have you partnered with entities like ESCCOM for workshops on trends?
- Do workshops cover topics like biases in machine learning tools or risks from loot boxes in games?
- Are workshop sessions tailored to build resilience, emphasizing that not all risks lead to harm?
- Do you use strengths-based methods in training, highlighting positive tech uses (e.g., collaboration tools)?
- Do you provide training materials in multiple formats (e.g., audio, braille, simplified language) to meet diverse needs?
- Do you adapt training for staff/students with disabilities or from rural areas with limited access (e.g., offline modules)?
- Do you exchange case studies with other schools, such as how addressing peer pressure reduced addictive tech use?
- Do you foster collective improvement through networks or forums for sharing successful practices?

Collaborative Safety Measures and Advocacy

- Have you collaborated with parents, teachers, librarians, and community organizations?
- Do you provide referrals, advice, and support (e.g., for victims of online issues) through these partnerships?
- Do you host joint sessions on help-seeking strategies and guidance resources?
- Have you integrated digital citizenship into the curriculum, covering responsible online behavior?
- Does the curriculum include media literacy for critical thinking (e.g., evaluating sources)?
- Does the curriculum build social-emotional skills, focusing on managing relationships and resilience?
- Have you explained the impacts of cyberbullying on wellbeing (e.g., mental health effects)?
- Have you discussed how weak accounts lead to identity theft?
- Do you promote positive approaches, emphasizing opportunities like online civic engagement?
- Have you promoted national helplines (e.g., 116 for child protection) to the community?

- Do you teach international tools, such as using report abuse buttons on platforms?
- Have you instructed on blocking offenders and preserving evidence (e.g., screenshots without sharing explicit material)?
- Have you advocated for government investments, such as expanding ICT labs to 80% coverage in high schools by 2028/29?
- Does your advocacy focus on equitable access and built-in safety features?
- Do you empower students to design safety programmes reflecting their experiences?
- Do you promote meaningful student participation (e.g., student-led campaigns or feedback surveys)?