THE Safety Chic

DIGITAL SAFETY AND CYBERSECURITY FOR CHILDREN

July 2025

THE Safety Chic

Website: www.thesafetychic.com
Email: info@thesafetychic.com

Contributors

Amarachi Iheagwam, Mercy John, Joshua Mze,
Elizabeth Kalu, and Ugochi Obidiegwu

Acknowledgments

Digital safety and security for children remain a burning issue today more than ever. We have a responsibility to create a safer world for our children. I would like to thank all staff, interns, and partners at The Safety Chic who supported the delivery of this paper. Thank you for your generous expertise and time throughout the writing process. I also extend our sincere gratitude to all the individuals and organisations whose insights, research, and feedback contributed to the development of this white paper. I hope these insights help in ensuring digital safety for our children.

Ugochi Obidiegwu
Founder, The Safety Chic

TABLE OF CONTENT

EXECUTIVE SUMMARY 05

INTRODUCTION 06

UNDERSTANDING DIGITAL RISKS 07

STRATEGIES FOR DIGITAL SAFETY EDUCATION 09

THE ROLE OF STAKEHOLDERS 15

CASE STUDIES AND SUCCESS STORIES 20

RECOMMENDATIONS 24

CONCLUSION 26

REFERENCES 27

LIST OF ACRONYMS

AAP	American Academy of Paediatrics
AI	Artificial Intelligence
COP	Child Online Protection
DCO	Digital Cooperation Organisation
EC	European Commission
ECPAT	End Child Prostitution and Trafficking
ESET	Essential Security against Evolving Threats
EU	European Union
GPS	Global Positioning System
ITU	International Telecommunication Union
KCSO	Keeping Children Safe Online
NARC	Nigerian Army Resource Centre
NGO	Non Governmental Organisation
OECD	Organisation for Economic Co-operation and Development
OFCOM	Office of Communication
SOS	Save Our Soul
UNICEF	United Nations Children's Fund

EXECUTIVE SUMMARY

Children today are immersed in a digital world that offers vast opportunities for learning and connection, yet also presents significant risks such as cyberbullying, exposure to inappropriate content, and data breaches. Their inherent trusting nature and limited awareness of online threats make them particularly vulnerable. This white paper addresses the critical need for comprehensive digital safety and cybersecurity measures, exploring prevalent online dangers, existing protective mechanisms, and the essential roles of various stakeholders in fostering a secure digital environment for children.

The primary digital risks identified include online privacy violations and data breaches, where children often share personal information without fully understanding its permanence or potential misuse. Cyberbullying and harassment are also key concerns, as they can occur at any time and may lead to severe psychological effects on children. Furthermore, unrestricted internet access exposes children to inappropriate content, impacting their emotional and cognitive development. Effective strategies for digital safety education involve teaching children about privacy protection, emphasising strong passwords, enabling privacy settings, and promoting cautious sharing habits. Parental control and monitoring, including screen time boundaries and open communication, are crucial for mitigating risks and building trust. Collaboration with schools to integrate digital literacy programs, foster critical thinking, and facilitate early intervention is also vital.

Ensuring children's digital safety requires a collective effort from all stakeholders. Parents and guardians are the first line of defence for educating children and modelling responsible online behaviour. Educators and schools must implement comprehensive curricula and robust cybersecurity protocols. Tech companies are responsible for designing child-centred platforms with safety features like age verification, content filtering, and strict privacy defaults. Governments, policymakers, and law enforcement agencies are essential for establishing legal frameworks, raising awareness, providing reporting mechanisms, and enforcing compliance. Lastly, healthcare and social service providers should offer crucial counselling, risk assessment, and collaboration with law enforcement to support affected children and families. Successful initiatives like UNICEF's Online Safety, Common Sense Media's Digital Citizenship program, and innovations in kid-safe devices and educational apps demonstrate the effectiveness of these multifaceted approaches.

ABSTRACT

As children navigate an increasingly connected digital world, they face a range of online risks including cyberbullying, privacy breaches, and exposure to harmful content that threaten their well-being and development. This white paper explores the urgent need for comprehensive digital safety and cybersecurity measures tailored to children's unique vulnerabilities. It examines key threats such as online harassment, data misuse, and unrestricted internet access while highlighting practical prevention strategies including privacy education, parental monitoring, and digital literacy programs in schools. The paper emphasises that safeguarding children online requires a coordinated, multi-stakeholder approach. It calls on parents, educators, tech companies, and policymakers to implement protective frameworks from user-centric platform design to legal safeguards and community-based interventions. Through case studies and proven initiatives like UNICEF's Online Safety guidance and Common Sense Media's Digital Citizenship program, the paper illustrates how collaborative, rights-based solutions can foster a safer digital environment where children can thrive.

INTRODUCTION

Children in the digital age are often surrounded by technology and use the internet for education, entertainment, and social contact. While the digital realm provides countless learning and development opportunities, it also exposes children to many online hazards, such as cyberbullying, identity theft, inappropriate content, and online predators. As technology evolves, so do the risks associated with its use, making digital safety and cybersecurity a top priority for parents, educators, and governments as well. Children are particularly vulnerable online due to their limited awareness of potential threats and their trusting nature. As digital technology becomes more integrated into their daily lives through smartphones, social media, online games, and virtual classrooms, the challenge of keeping them safe in cyberspace grows more complex. This situation calls for a well-coordinated effort involving parents, educators, technology providers, and policymakers to promote digital literacy and establish protective measures.

This white paper explores the concept of digital safety and cybersecurity for children by examining digital risks, examining the present challenges and available protection mechanisms, and the various roles of stakeholders in ensuring a secure digital environment. By understanding the nature of online risks and the best practices for mitigating them, this paper aims to contribute to the ongoing discourse on digital safety and cybersecurity for children in the digital space.

UNDERSTANDING DIGITAL RISKS

The world today is highly interconnected and children's engagement with digital technology has expanded exponentially. Despite the internet offering rich opportunities for education, creativity, and social interaction, it also exposes young users to a myriad of digital risks. Three significant areas of concern are online privacy and data breaches, cyberbullying and harassment, and exposure to inappropriate content. Understanding these risks is crucial for parents, educators, policymakers, and technology solution providers looking to create safer digital environments for children.

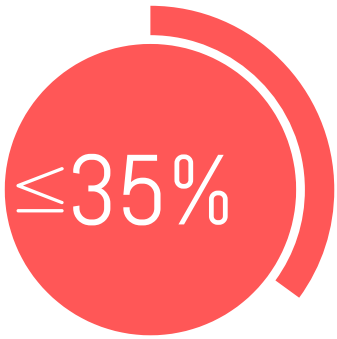
Online Privacy and Data Breaches

Children's data is particularly vulnerable in the digital world. Unlike adults, children may lack the cognitive maturity to fully understand the consequences of sharing information online. Children often share personal information on social media platforms without understanding the potential permanence and reach of such data. This behaviour can expose them to identity theft, targeted advertising, and exploitation (Livingstone et al., 2019).

Furthermore, data breaches involving children's information are rising. Educational platforms, gaming apps, and social networks often collect vast amounts of children's data, sometimes without adequate security measures (Auxier et al., 2020). In some cases, children's profiles are built long before they can consent, a phenomenon known as "datafication" of childhood (Lupton & Williamson, 2017). A breach in these systems can result in the exposure of sensitive information, such as location, school enrollment, and family details, to malicious actors.

Cyberbullying and Harassment

Cyberbullying is one of the most damaging forms of online harassment that children face. It encompasses a wide range of behaviours, including sending threatening messages, spreading rumours online, and posting humiliating content. Research by Hinduja and Patchin (2020) highlights that approximately 15% to 35% of youth report experiencing cyberbullying at some point. Unlike traditional bullying, cyberbullying can occur 24/7 and invade the perceived safety of a child's home. The anonymity afforded by the internet emboldens perpetrators and complicates detection and intervention (Kowalski et al., 2014). Victims of cyberbullying often experience severe psychological effects, such as depression, anxiety, low self-esteem, and even suicidal ideation (John et al., 2018).



15 to 35% of youth reportedly experiencing cyberbullying (Hinduja and Patchin, 2020)

children between 8 to 15 in the UK who have potentially encountered harmful content online. (Ofcom, 2023)

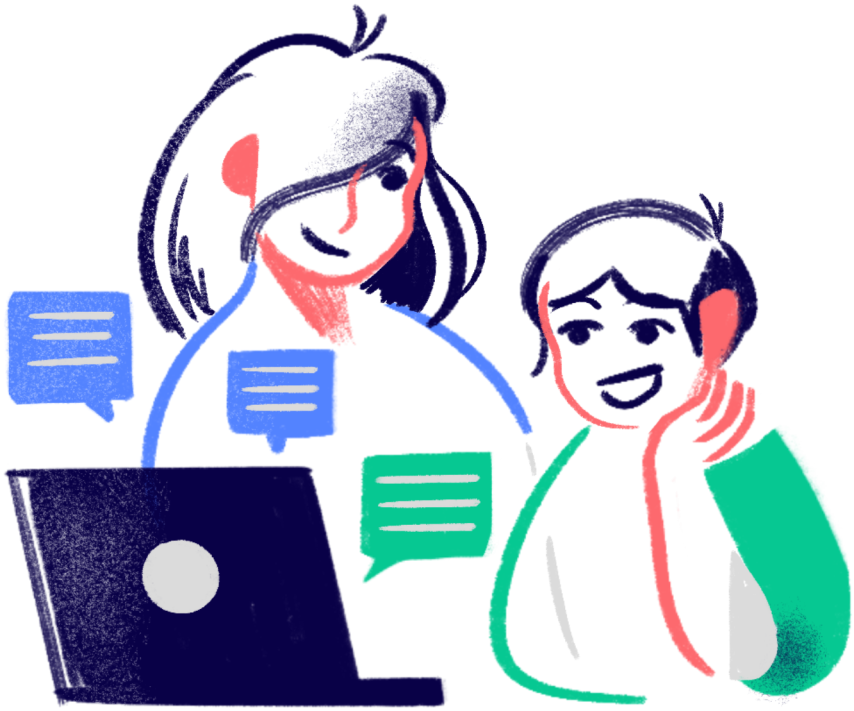
Effective prevention and response strategies include digital literacy education, promoting positive online behaviour, and fostering open communication between children and trusted adults. Anti-cyberbullying policies by social media companies and schools are also pivotal but require rigorous enforcement and child-centred approaches (UNICEF, 2019).

Exposure to Inappropriate Content

Another major concern is children's exposure to inappropriate content, including violence, pornography, extremism, and hate speech. The unrestricted nature of the internet means that even innocuous searches or interactions can lead to harmful material. A study by Ofcom (2023) found that nearly 60% of children between the ages of 8 to 15 in the UK encountered potentially harmful content online in the past year. Exposure to such material can negatively affect children's emotional, cognitive, and social development. For instance, early exposure to violent content can desensitise children to aggression, while exposure to sexual content can distort their understanding of relationships and sexuality (Livingstone & Smith, 2014). Parental controls, content filtering, and age-appropriate online environments are critical tools for mitigating these risks.

From the foregoing, we see that the digital age has transformed childhood, offered tremendous benefits, but also introduced significant risks. Understanding and addressing issues related to online privacy and data breaches, cyberbullying and harassment, and exposure to inappropriate content are paramount to ensuring children's digital safety. A multi-stakeholder collaboration involving families, schools, governments, and technology companies is needed to create a safer, more empowering online environment for children. Furthermore, building children's resilience and digital literacy is equally important so they can thrive amidst both the opportunities and the dangers of the online world.

STRATEGIES FOR DIGITAL SAFETY EDUCATION



Today's children are digital natives. They are skilled at navigating online spaces and frequently outsmart older generations in technology use. However, this ability does not always translate into critical thinking or digital literacy, leaving them open to false information, online predators, and cyberbullying. The long-term impact of digital immersion on children's well-being arising from excessive screen time is negative and can affect physical health and interfere with social connections (Nikolopoulou, 2024).

As individuals embrace digital solutions that facilitate anywhere/anytime access, cybercriminals and bullies are also constantly looking for methods to capitalise on this trend. They take advantage of unprotected wireless networks and vulnerable children, leading to cyber insecurity. This makes the digital space unsafe, especially for children. Digital safety is learning how to protect privacy and stay safe from predators while interacting in this new digital era. Digital safety is sometimes referred to as media safety, online safety, e-safety, cyber safety, or Internet safety (Sadiku et al., 2021).

Strategies for Digital Safety Education

Digital safety by design for children is an emerging concept that should guide innovation to be beneficial and responsible, placing children's safety and well-being at the forefront. The digital environment offers valuable opportunities for self-expression, learning, socialisation, cultural engagement, and the exercise of their rights. However, this same environment also exposes children to a broad range of risks to which they are more vulnerable than adults. These include harmful or illegal content, cyberbullying, breaches of privacy, commercial exploitation, and abhorrent crimes such as sexual exploitation and abuse (Organisation for Economic Co-operation and Development, 2024).

Protecting children in the digital space is challenging due to the complex, fast-evolving, and often insufficiently regulated nature of online platforms. A major concern is the fact that many digital products and services are developed without adequate safety features for children. For example, numerous platforms lack default protective settings for underage users, while design priorities often favour user engagement or data collection over child safety. Due to these challenges, digital safety education strategies are essential to protect children who are not only active participants in the digital world today but also future leaders.

The following are key strategies for promoting digital safety among children:

1. **Education on Privacy Protection**

Understanding the importance of personal information and its value is a crucial aspect of digital safety education for children. Children must be taught that the information they share in the digital space can have long-lasting implications. Teaching children to recognise what constitutes personal information is the first step in helping them protect their privacy. Parents and guardians should emphasise the permanence of digital sharing because once information is posted, it can be difficult or impossible to remove, and an unintended audience may access it. Educating children about the potential misuse of personal information can help them understand why it is important to keep certain details private. For instance, explaining that sharing personal information can lead to identity theft, online scams, and unwanted contact from strangers can bring the concept home to children (Wellspring Centre for Prevention, 2024).

Some guidelines for privacy protection and secure browsing are:

- **Use Strong Passwords:** Encourage children to use strong, one-of-a-kind passwords for their accounts on the internet. Passwords should not contain information that can be easily guessed, like pet names or birthdays, and should instead be a combination of letters, numbers, and symbols (Canavan, 2024; Wellspring Centre for Prevention, 2024).
- **Enable Privacy Settings:** Teach children how to use privacy settings on social media and other online platforms. These settings can help control who sees their information and posts. This protection can significantly affect children's digital safety, self-esteem, and long-term online behaviour positively. Also, parents and guardians should ensure they understand the

importance of regularly reviewing and updating these settings (Cappello, 2025; Wellspring Centre for Prevention, 2024).

- **Think Before Sharing:** It is important to teach kids to exercise caution when sharing any personal information online. They should be able to ask themselves, given the potential consequences, "Is what I am sharing true, kind, appropriate, necessary, and, finally, helpful?" (Ben-Joseph, 2023; Wellspring Centre for Prevention, 2024).
- **Limit Public Profiles and Prevent Oversharing:** Tell children to limit, or if possible, avoid sharing personal information such as photos and videos online in public forums or with individuals they do not know. This is important because sharing personal details can put them at risk of being contacted by strangers with bad intentions. Explain to children that once something is shared online, copies may still exist even if deleted and can be shared without their permission (Hertog, 2025; Tomkova, 2023; U.S. Department of Justice, 2025).
- **Avoid Sharing Location:** Remind children not to share their location online, whether through social media check-ins, geotagged photos, or location-sharing apps. This can help prevent unwanted attention and potential danger (Wellspring Centre for Prevention, 2024). Children need to understand that anything they share online can have lasting repercussions. Recognising the importance of protecting their personal information is a vital part of digital safety education. Parents and guardians play a crucial role in helping children understand why their privacy matters. By following the guidelines for secure browsing and privacy protection, families can further strengthen children's safety in the digital world.

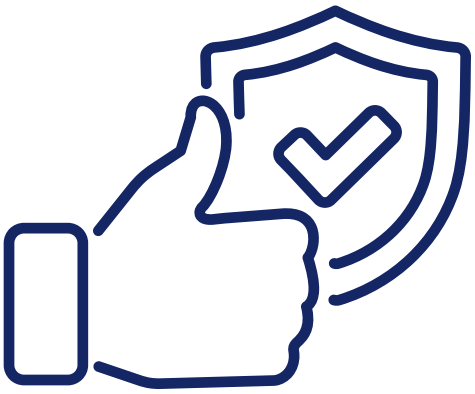
2. **Parental Control and Monitoring**

Effective communication between parents and children is crucial to support healthy development. A key aspect of this involves teaching children to think critically and make informed decisions online. However, the growing preference for digital devices over outdoor activities and face-to-face interactions has raised concerns about reduced environmental awareness and increasing individualism among children. Parental involvement is vital to ensuring that children can enjoy the benefits of digital technology while being protected from its potential risks. Engaging and equipping parents with knowledge of digital safety is important in creating a safe online environment for children. (UNICEF, 2024).

Parental control and monitoring are important for the following reasons:

- **Continuous Learning and Guidance:** Privacy policies and settings change regularly. Awareness of updates ensures optimal privacy protection. This provides an opportunity to have discussions within the family in an informal setup we recommend called the family safety meeting. This meeting is a scheduled time in a family's calendar to engage in fun activities together. During this fun time, an aspect of a child safety topic can be taught leveraging diverse techniques. It creates a core memory for children and teenagers during this bonding time and also demonstrates to them that digital safety requires an ongoing practice of learning.

- **Clear Screen Time Boundaries:** Ensuring clear screen time boundaries is a key strategy for enhancing children's digital safety. Parental control apps, such as Google Family Link and Qustodio, allow caregivers to set daily usage limits and monitor device activity, reducing the risks associated with prolonged and unsupervised online engagement. This helps to maintain a balanced routine between screen use and offline activities. By extension, these tools support children's physical and mental well-being and also reduce their exposure to online threats such as digital fatigue, addictive behaviours, and harmful content. Research shows that excessive screen time is linked to sleep disturbances, reduced physical activity, and heightened levels of anxiety and depression in children (Twenge & Campbell, 2018). This is why screen-time regulation as part of a broader digital safety framework is important.



- **Building Trust and Open Communication:** When parents and caregivers are present, actively engaged in their child's life, and involved during their online activities, they create valuable opportunities for open dialogue that fosters trust. This trust encourages children to share their thoughts, experiences, and concerns, making it more likely that they will seek guidance when encountering challenges online. Open communication also provides a platform for parents to educate their children about digital safety, teach critical thinking skills, and ask important questions about their online experiences. Families can use tools such as the Family Media Plan provided by the American Academy of Paediatrics (AAP). This customizable tool helps parents and children set shared expectations about screen time, online activities, and digital boundaries, encouraging a collaborative approach to digital safety through regular, open conversations.
- **Mitigating Risks Associated with Cyberbullying and Online Predators:** To keep children safe from cyberbullying and internet predators, parents must combine early instruction, supervision, and open communication. It is critical to teach children how to respect their privacy, notice suspicious activity, and report harmful encounters. Tools like Bark, for example, can help parents monitor their children's online behaviour and warn them of potential threats, creating a trustworthy environment that helps children discuss negative experiences without fear. According to research, proactive parental involvement minimises children's exposure to internet risks while also strengthening their resilience (Livingstone, Stoilova, & Nandagiri, 2019).

For children to be secure in the digital environment, open communication, defined boundaries, and ongoing education are necessary. Children can be helped to navigate online places safely by parents and caregivers who remain up to date on privacy upgrades, set screen time restrictions, and cultivate trust. By working together and taking preventive measures, they can further increase their resilience to threats like cyberbullying and online predators, guaranteeing a better digital future.

3. Collaborations with Schools for a Digital Literacy Program

Children's digital safety requires the joint efforts of parents, teachers, and schools. As schools progressively incorporate digital tools into their programs, students must be equipped with the skills and awareness needed for safe and responsible online participation. Through collaboration between parents, teachers, civil society, and educational institutions, comprehensive digital literacy programs can be developed and integrated into the curriculum.

Below are some key reasons to collaborate with schools on digital literacy:

- **Early Intervention and Risk Prevention:** As more individuals utilise the internet for social, professional, and educational purposes, more people are using it as an outlet for their anger and aggravation. Children online can be exposed to this. Therefore collaboration programs on digital safety with educators and parents can help in identifying early signs of risky digital behaviour, such as cyberbullying, sexting, or exposure to inappropriate content. Intervention in school settings helps prevent long-term damage (Kowalski et al., 2014).
- **Structured and Consistent Digital Education:** Schools provide a structured environment where digital literacy is systematically taught as part of the curriculum. Providing a detailed syllabus to the students (and parents, if necessary) helps them know what to expect from the class and allows them to tick off work as they complete it. Encouraging students to participate, personalising course plans, creating a consistent timetable, and tracking student engagement are also essential. Collaborations ensure that students receive consistent messaging about online safety, digital etiquette, and responsible technology use (Livingstone & Helsper, 2007).
- **Promoting Critical Thinking and Media Literacy -** To promote critical thinking and media literacy, teachers and parents need to collaborate and share updates on students' progress, and promote media literacy. Schools should offer parenting classes to help parents support their children's development of critical thinking and media literacy at home. Both teachers and parents play a crucial role in fostering these skills, contributing to a positive digital culture. While training sessions help enhance teachers' media literacy competencies, further support from the Ministry of Education is needed to equip early childhood educators. In today's digital age, schools, with the support of the government, lead in promoting media literacy and critical thinking across all age groups, ensuring children engage with digital content responsibly (Hasibuan et al., 2024).

- **Collaboration with Parents and Communities:** For digital safety education to be effective, educators must work in tandem with parents and communities. Children spend a lot of time in their communities, at school, and home; therefore, this collaboration guarantees a comprehensive approach to their digital well-being. Educators, parents, and communities must work closely together to implement structured digital education and provide early intervention to ensure children's digital safety. By empowering families and communities to collaborate, this shared knowledge helps kids securely navigate the digital world and develop a deeper awareness of the risks and responsibilities associated with their online activity. This will develop their media literacy and critical thinking skills.

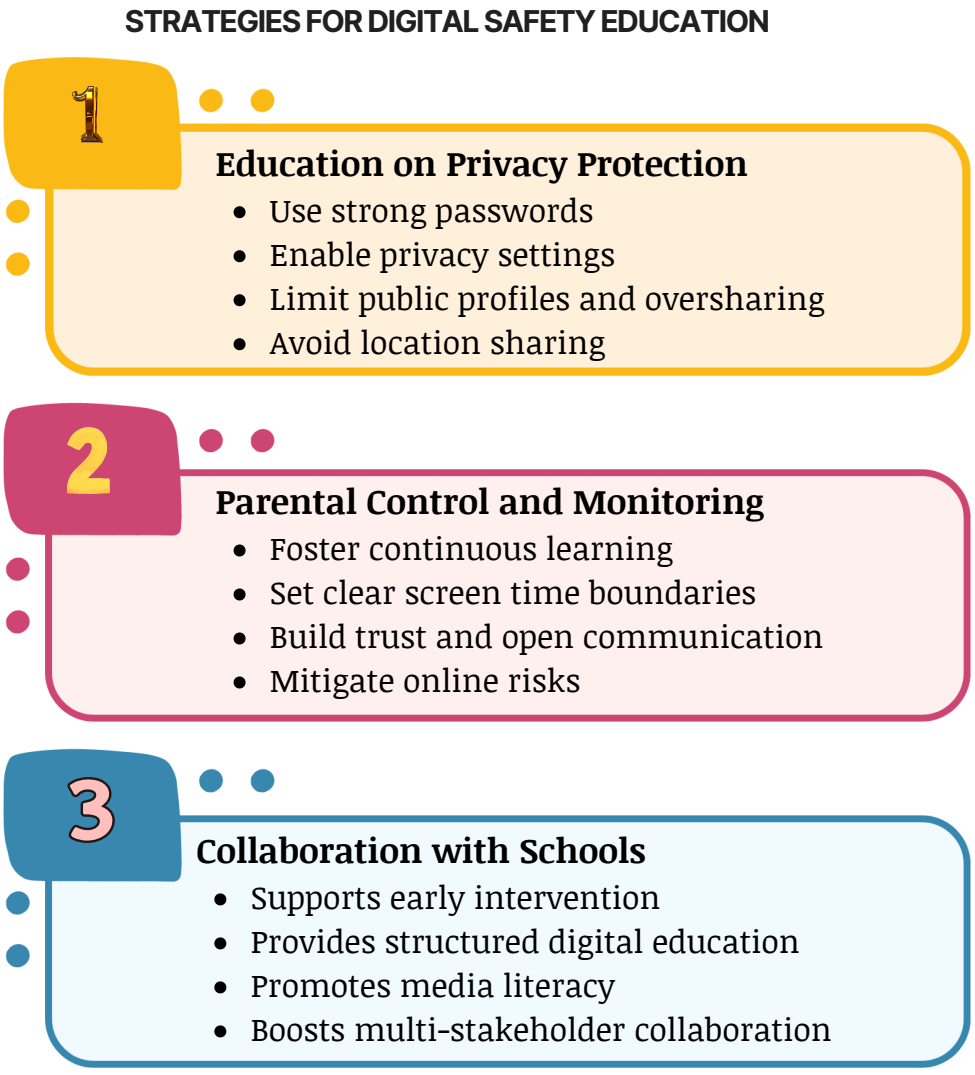


Figure 1: Strategies for Digital Safety Education

THE ROLE OF STAKEHOLDERS

Children are not usually involved in the process/dialogue. But they should be. It is crucial to actively engage them by gaining a clear understanding of their motivations, concerns, and vulnerabilities (Digital Cooperation Organisation, 2024). Stakeholders play a key role in ensuring children's digital safety. However a concerted multi-stakeholder approach including parents, educators, policymakers, technology companies, health care, and social service providers is what makes the difference. By working together, stakeholders can create a safer digital environment that effectively addresses children's needs and protects their rights.

CATEGORIES OF STAKEHOLDERS

1. Parents and Guardians

Parents and guardians play a critical role in ensuring children's digital safety. They are the first line of defence in protecting children from the wide range of risks present in the digital world. Young children use technology during after-school hours to explore the internet, as such, it is vital for parents and caregivers to actively guide and supervise their online experiences. Parents and guardians are responsible for educating children about online risks, setting appropriate boundaries, using digital tools to monitor activity, and modelling responsible online behaviour.

To do this effectively, parents must be equipped with adaptable strategies to manage their children's exposure to digital risks and to respond quickly to online safety incidents. However, many caregivers lack sufficient awareness of the threats their children face and are not adequately trained in the skills necessary to protect them. Sometimes, it's not their fault because with rapid technological advancements, new information keeps coming up. In addition, many parents find it difficult to initiate open conversations about sensitive online issues, even though open dialogue is key to building trust and encouraging children to seek help when needed (Digital Cooperation Organisation, 2024). By embracing their roles as educators, protectors, and communicators, parents and guardians can significantly enhance children's resilience and safety in the digital environment.

2. Educators and Schools

The role of educators in ensuring children's digital safety is equally important as children spend a significant amount of time at school. Research shows that higher levels of education, both nationally and individually, are closely linked to increased internet usage. Therefore, it is reasonable to expect that as educational attainment grows, so does the volume and complexity of internet engagement. This underscores the need for media education to be recognised and integrated as a core element of school curricula and infrastructure to support safe and

responsible online engagement (Livingstone & Haddon, 2009). Educational institutions have several strategies at their disposal to promote digital safety. Implementing comprehensive curricula that cover topics like digital citizenship, online safety, privacy protection, cyberbullying prevention, and responsible social media usage is crucial. Additionally, schools should establish robust cybersecurity protocols for their online platforms to protect against cyber threats. Clear regulations regarding safe internet use on school property should be set, including guidelines for sharing personal information, accessing appropriate websites, and reporting harmful online activities. Teachers, support staff, and school administrators must be well-equipped to identify and address online safety concerns, ensuring they can properly protect and guide their students in the digital realm (Digital Cooperation Organisation, 2024).

3. Tech Companies

Tech companies have a responsibility to make the internet a safer space for children. Given the increasing presence of young users online, companies must move beyond minimum legal compliance and proactively design digital programs and tools with children's safety and well-being in mind.

This can be accomplished by:

- Integrating safe features like strict age verification, content control, and features like "trusted adult" notifications into messaging and social media platforms to guarantee that interactions stay age-appropriate and that any risky activity is promptly identified and dealt with (Brennen & Perault, 2023).
- Development of technological platforms that provide educational resources to teach children about digital safety, safe communication applications, content filtering and monitoring software, and effective privacy protection measures (ECPAT International, 2023; Russell, 2024).
- Content filtering, monitoring, and privacy protection for children. Tools should screen appropriate material, allow parental controls, and encourage children's self-regulation. Privacy measures must default to strong protections, limit data collection, use child-friendly language, and avoid manipulative designs (Goldstein, 2023; Hertog, 2025).

4. Government, Policymakers, and Law Enforcement Agencies

In addition to parental involvement, protecting children's digital safety needs collaboration from the public and private sectors. Policymakers and legislators are responsible for developing comprehensive legal frameworks that define harmful digital actions and impose penalties to dissuade potential offenders. They must also monitor the formulation, implementation, and ongoing amendment of laws to ensure that they adapt to the changing digital landscape and properly protect children's rights online (Digital Cooperation Organisation, 2024). Law enforcement agencies are crucial for investigating and prosecuting cyber crimes such as online predation, child exploitation, and cyberbullying. Their work not only addresses criminal behaviour but also ensures that victims receive appropriate support and protection.

In 2009, the International Telecommunication Union's Child Online Protection (COP) Guidelines was introduced and it was updated in 2020. It provides a comprehensive framework to help countries develop national strategies for child online safety. These guidelines encourage governments to establish legal frameworks, promote cooperation, and empower children with digital skills to navigate online risks. Many countries worldwide have adopted the COP Guidelines to create safer digital environments and protect children from online harm (Moses, 2023).

The COP guidelines emphasise the following roles and responsibilities of the government:

- **Legislation and Regulation:** Governments should create and enforce laws to protect children online. This includes obligating online platforms to implement safety features, restrict access to age-inappropriate content, and address threats like cyberbullying, child exploitation, and online grooming. Governments can also work to ensure laws align with emerging technologies and risks.
- **Awareness and Education:** Governments should create educational programs and campaigns to inform children, parents, teachers, and the public about online risks and promote responsible digital behaviour. These efforts help build safer online environments through education and community engagement.
- **Reporting Mechanisms and Helplines for Digital Safety:** The government can set up and support safe and better ways for children to report problems they encounter online. These services may include hotlines, websites, or help centres where children, parents, and teachers can ask for help, report online threats and abuse, and also get advice on staying safe online. These services are to be made free and available.
- **Research and Data Collection:** The government should support ongoing research to understand how the internet is used and what puts children at risk. This helps them make appropriate tools and rules to ensure children's online safety.

- **Industry Collaboration:** Governments should partner with tech companies, social media platforms, internet providers, and international organisations to set safety standards and best practices, encourage the analysis and filtering of content and reporting tools, and ensure compliance with safety rules.

Finally, when governments, legislators, and law enforcement agencies work together on integrated training programs, public outreach campaigns, and community participation, they create a comprehensive ecosystem that promotes safer online environments for all children.

5. Healthcare and Social Service Providers

Healthcare and social service professionals are also important in promoting digital safety for children. Given their expertise in child development, mental health, and family dynamics, they are uniquely positioned to intervene, educate, and support children and families navigating the challenges of the online world. Their contributions can be outlined as follows:

- **Counselling and treatment:** Providing early intervention and therapy for children impacted by digital harm such as cyberbullying, online exploitation, and exposure to inappropriate content. This support helps children process their experiences, rebuild trust in online spaces, and strengthen emotional resilience to navigate the digital world safely.
- **Collaboration with law enforcement:** Reporting incidents of online abuse, such as cyberbullying, exploitation, and grooming, and working closely with authorities to protect children, support victims, and hold offenders accountable in the digital environment.
- **Risk assessment**: Identifying early signs of problematic internet use, exposure to predators, or risky behaviours during routine health checks or social evaluations.

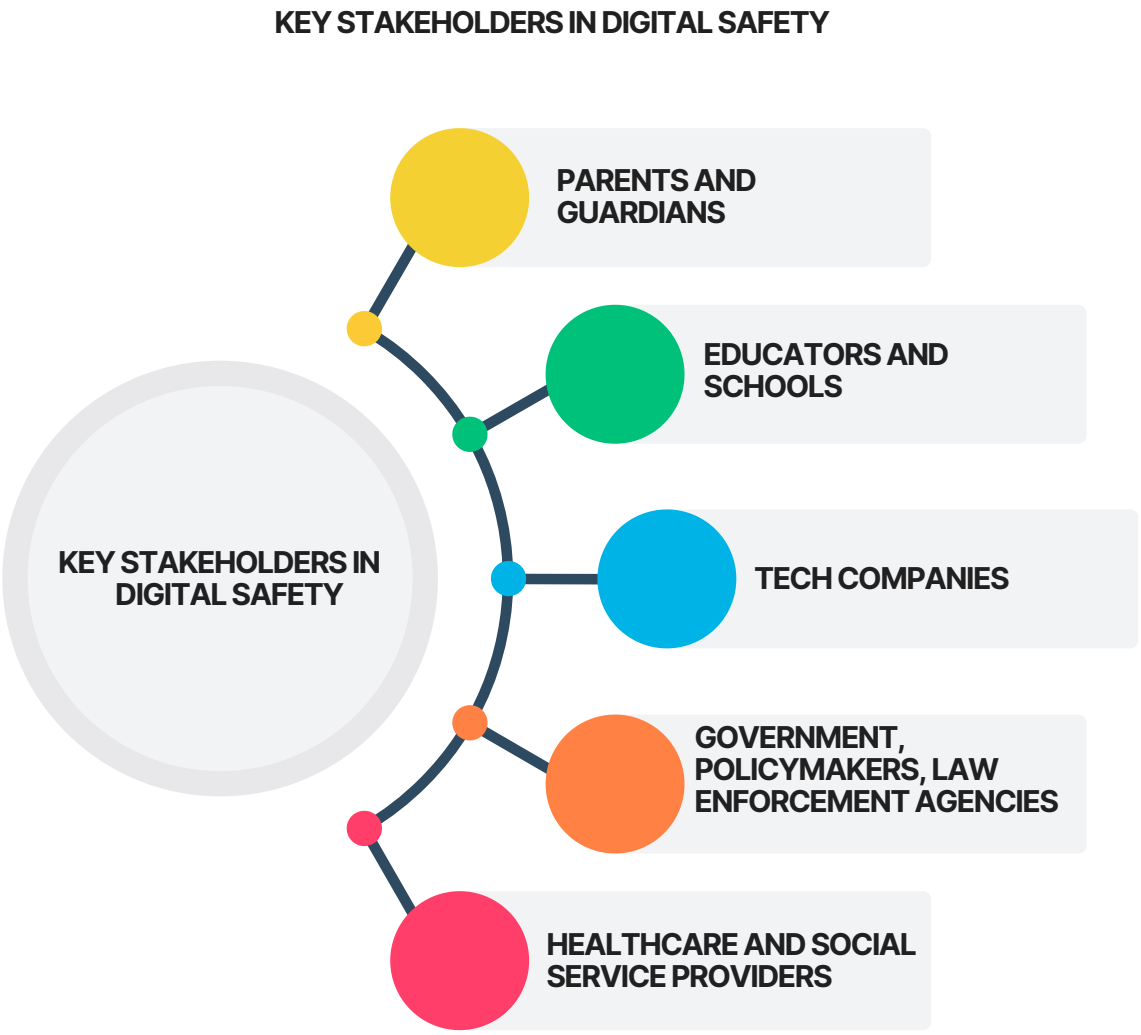


Figure 2: Key Stakeholders in Digital Safety for Children

CASE STUDIES AND SUCCESS STORIES

SUCCESSFUL DIGITAL SAFETY PROGRAMS

Despite the challenges, good examples abound on how to ensure the effective protection of children online. They buttress the importance of working together to adopt smart strategies, implement evidence-based programs, and use innovative tools that reduce risks while empowering young users. Some examples of successfully enhanced digital safety programs and tools for children are:

1. UNICEF's Online Safety Initiatives

To strengthen international efforts to protect children's online experiences through holistic tactics, UNICEF has been advocating for measures to guarantee children's safety online, such as policy lobbying, education, and parental participation (UNICEF South Asia, 2023).

2. Digital Citizenship Program

This dynamic educational resource by Common Sense Media promotes equity, safety, and digital citizenship through six interactive games designed to engage students while reinforcing key online safety concepts. The program integrates seamlessly with Google Classroom and includes:

- Password Protect (online security)
- Twalkers (multitasking, media balance, and digital well-being)
- Share Jumper (privacy awareness)
- E-volve (cyberbullying, hate speech, and being an upstander)
- Search Shark (news and media literacy)
- Mix-n-Match (understanding creative credit)

Additionally, the Educator Guide provides comprehensive lesson plans, including scope and sequence, to support effective classroom implementation (Caukin, 2023).

3. Keeping Children Safe Online (KCSO) Program

This initiative by World Vision International was implemented in six countries in the Middle East and Eastern Europe to reduce the risks of online violence through education, policymaking, and community involvement. Apart from engaging parents and educators and integrating online safety into school curricula, the effort centres on enacting laws to protect children from cybercrime and training children to be peer educators. Because of the initiative, 50% of parents and 80% of Armenian children have swiftly implemented safety precautions.

5. Qustudio

Qustodio is a parental control software designed to help parents monitor and manage their children's online activity, promoting safer and more responsible digital habits. It offers features such as screen time management, location tracking, app blocking, and detailed activity reports, giving parents greater visibility and control over how their children use connected devices. Some key benefits of using Qustodio parental control software:

- Comprehensive parental controls across devices
- Real-time location tracking and geofencing
- Ability to manage multiple devices from a single dashboard
- Detailed reports on a child's online activity and screen time habits

Its availability across major platforms and flexible pricing options make it an accessible solution for modern digital parenting (Qustodio, 2025).

INNOVATIONS IN CHILD SAFETY TECHNOLOGY

Since children begin using smart devices, the internet, and social media from an early age, there is a growing need for advanced tools and systems that can ensure their digital safety. These innovations would not only protect children but also promote healthy online habits and support parents and caregivers in guiding their children's development.

Some examples that help curtail the problems children encounter are:

1. Tablets and Kid-Safe Devices

They provide controlled digital experiences for children. Tablets and kid-specific smart devices have been developed with safety and age-appropriate features in mind. These devices often include curated app stores that offer only safe, educational, and parent-approved applications, providing a controlled digital experience tailored to a child's developmental stage. Many of these devices also have robust parental control features, allowing parents to set screen time limits, monitor usage, and even set learning goals. This level of control helps ensure that the time children spend on these devices is productive and aligned with their educational needs. Additionally, these tablets often come with durable designs and protective cases, making them resilient to the wear and tear typical of young users. Some kid-safe tablets are equipped with ad-free environments, ensuring that children are not exposed to advertising content that may not be suitable for their age. By eliminating ads and in-app purchases, these devices offer a distraction-free space where kids can engage in learning and entertainment without being subjected to external influences (The Cyber Data Bank, 2024)

2. Wearables and Smartwatches

Wearable technology, particularly smartwatches designed for kids, has become one of the most popular forms of child-friendly tech. These devices are more than just miniaturised smartphones on the wrist; they offer a range of safety features that keep kids connected to their parents while promoting independence. Smartwatches for kids often include GPS tracking, allowing parents to monitor their child's location in real-time through an app on their own devices. This feature is particularly useful when kids are on their way to school, playing outside, or attending activities independently. The ability to set geofences, virtual boundaries that alert parents when their child enters or exits a designated area, adds an extra layer of security, providing a sense of safety without needing constant supervision. In addition to location tracking, many of these wearables are equipped with SOS buttons that kids can press in emergencies. This one-touch alert system sends an immediate notification to parents, along with the child's current location, enabling a quick response. For children, wearing a smartwatch offers a sense of security and empowerment, knowing they can easily reach out for help if needed. These devices also include features such as restricted contact lists, ensuring that only approved numbers can communicate with the child, thereby reducing the risk of unwanted or unsafe interactions. For parents, smartwatches provide a balanced approach to child safety, keeping kids connected and protected while allowing them the freedom to explore their world (The Cyber Data Bank, 2024).

3. Educational Apps with Built-In Safety Features

Educational apps designed for children prioritise safety by integrating features like parental controls (content filtering, age restrictions, and limited user interactions) and offline modes to reduce online risks. They also enforce strict privacy settings to protect kids' data from collection or third-party sharing, complying with data protection standards. Advanced tools, such as AI-driven moderation, monitor chats and

block harmful content, language, or suspicious behaviour. These safeguards ensure a secure digital environment for learning while addressing concerns about inappropriate content, predators, and data privacy (The Cyber Data Bank, 2024).

4. The Evolution of Child-Friendly Tech

Child-friendly tech is rapidly evolving to address the unique safety needs of today's young users. From wearables and smartwatches to smart home sensors and secure educational apps, these technologies are revolutionising how parents protect their children in both the physical and digital worlds. By integrating safety features that go beyond basic controls, these innovations offer children the freedom to explore, learn, and connect while maintaining a secure environment. As technology continues to advance, the future of child safety tech promises even more sophisticated solutions that empower kids and provide parents with peace of mind (The Cyber Data Bank, 2024).

The integration of child-friendly tablets, safety-focused wearables, and secure educational apps reflects a transformative shift in technology designed to protect young users while fostering their growth. These innovations, equipped with parental controls, real-time GPS tracking, AI-driven content moderation, and ad-free environments, empower parents to manage screen time, monitor interactions, and safeguard data privacy. Simultaneously, they offer children age-appropriate independence through features like SOS alerts, geofencing, and curated learning tools. As these technologies evolve, they strike a critical balance between safety and exploration, ensuring children can learn, play, and connect within a secure digital and physical framework. This approach not only addresses modern risks but also paves the way for future advancements that prioritise both protection and developmental freedom.

RECOMMENDATIONS

Based on the key issues addressed in this white paper on digital safety and cybersecurity for children, implementing the following recommendations will guide educators, parents, policymakers, and technology developers toward more effective strategies for protecting children in digital environments.

INTEGRATE DIGITAL LITERACY INTO THE SCHOOL CURRICULUM

Schools should incorporate digital literacy and online safety into the curriculum from an early age. These lessons should be age-appropriate and interactive, allowing children to understand the real-life implications of online behaviour.

PROMOTE CHILD-CENTRED DESIGN IN TECHNOLOGY

Tech companies should adopt child-centred design principles, which include age-appropriate privacy settings, minimal data collection, content filtering, and easy-to-use reporting tools. These measures can create safer digital spaces without limiting the positive potential of technology.

STRENGTHEN LEGAL AND POLICY FRAMEWORKS

Governments should review and revise existing cyber laws regularly to address new and emerging risks and also develop new policies to address cyberbullying, exploitation, and data protection for children where necessary.

ENCOURAGE HEALTHY USE OF SOCIAL MEDIA

Schools and parents should work together to promote digital empathy and responsible behaviour online. At the same time, platforms should implement better age verification tools, clearer content moderation guidelines, and quicker response systems for reports of abuse or harmful content.

PROVISION OF SUPPORT SYSTEMS AND SAFE REPORTING CHANNELS

Governments and NGOs should invest in child-friendly support services, including anonymous helplines and counselling platforms. These services should be widely promoted and easily accessible to children and their parents/guardians.

SUPPORT ONGOING RESEARCH AND ADAPTATION

Continued research is essential to monitor trends, understand children's online behaviours, and develop evidence-based interventions. Policymakers and educators should embrace flexible, adaptive strategies as new threats and opportunities continue to emerge in cyberspace.

SANCTIONS FOR DEVELOPERS AND TECH COMPANIES

Governments should enforce appropriate sanctions for tech companies that fail to follow ethical policies and principles put in place to safeguard children in the digital space. This will encourage more compliance from tech companies and developers.

CONCLUSION

The digital transformation of childhood presents both immense opportunities and significant challenges, making the comprehensive protection of children online an imperative shared responsibility. As this white paper has highlighted, effectively safeguarding children in the digital realm necessitates a concerted, multi-stakeholder approach that addresses the evolving nature of online risks, ranging from privacy breaches and cyberbullying to exposure to harmful content.

The cornerstone of this protection lies in empowering children through robust digital literacy education, enabling them to critically assess online interactions, understand the permanence of their digital footprint, and responsibly manage their personal information. Concurrently, parents and guardians must remain actively engaged, utilising parental controls, fostering open communication, and modelling safe online behaviours to build trust and resilience in their children.

Furthermore, systemic changes are crucial; technology companies must prioritise child-centred design, integrating safety features by default rather than as an afterthought, with a strong emphasis on privacy and age-appropriate content moderation. Governments and policymakers are tasked with developing and enforcing adaptable legal frameworks, establishing accessible reporting mechanisms, and investing in ongoing research to stay ahead of emerging threats. Healthcare and social service providers complete this ecosystem by offering essential support, counselling, and early intervention for children impacted by digital harms.

Ultimately, ensuring a secure and empowering digital future for children is not merely about mitigating risks; it is about cultivating an environment where they can safely explore, learn, and connect without compromising their well-being. By integrating digital literacy into education, promoting responsible technology design, strengthening legal safeguards, and fostering collaborative partnerships across all sectors, we can collectively build a digital space where children are protected, respected, and empowered to thrive.

REFERENCES

Auxier, B., Anderson, M., Perrin, A., & Turner, E. (2020, July 28). Parenting children in the age of screens. Pew Research Centre. https://www.pewresearch.org/internet/2020/07/28/parenting-children-in-the-age-of-screens/

Ben-Joseph, E. P. (2023). Teaching kids to be smart about social media. KidsHealth. https://kidshealth.org/en/parents/social-media-smarts.html

Brennen, S., & Perault, M. (2023, June 21). Keeping kids safe online: How should policymakers approach age verification? Centre for Growth & Opportunity. https://www.thecgo.org/research/keeping-kids-safe-online-how-should-policymakers-approach-age-verification/

Canavan, P. (2024). How to teach children about online safety. SafeWise. https://www.safewise.com/blog/how-to-teach-children-about-online-safety-and-privacy/

Cappello, L. (2025). How to teach kids the importance of digital privacy. TIME. https://time.com/7282041/teach-kids-digital-privacy/

Caukin, N. (2023). Tech talk cyber safety effort for children: Are they working? What can we do? International Journal of the Whole Child, 8(1). Retrieved from https://libjournals.mtsu.edu/index.php/ijwc/article/view/2394/1417

Childnet. (2025). What we do. https://www.childnet.com/what-we-do/

Digital Cooperation Organisation. (2024). Safe digital space for children: Policy paper. https://dco.org/wp-content/uploads/2024/10/Digital-Safe-Space-for-Children.pdf

ECPAT International. (2023). Achieving child safety online through technology. ECPAT. https://ecpat.org/story/achieving-child-safety-online-through-technology/

Goldstein, K. (2023, May 31). I'm a parent and a privacy lawyer: Here's what I will and won't post about my kid online. Parents. https://www.parents.com/kids/safety/internet/im-a-mom-and-childrens-privacy-lawyer-what-i-do-and-dont-post-online/

REFERENCES

Hasibuan, S., Humaizi, H., Lubis, L. A., & Pohan, S. (2024). Promoting media literacy among early childhood education: A case study in Deli Serdang Regency, Indonesia. Revista de Gestão Social e Ambiental, 18(5), e06961. https://doi.org/10.24857/rgsa.v18n5-136

Hinduja, S., & Patchin, J. W. (2020). Cyberbullying: Identification, Prevention and Response (2020 Edition). Cyberbullying Research Centre. https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2020.pdf

Hertog, E. (2025, March 16). How tech experts keep their children safe online. The Guardian. https://www.theguardian.com/lifeandstyle/2025/mar/16/how-tech-experts-keep-their-children-safe-online

International Telecommunication Union & UNICEF. (2015). Guidelines for industry on child online protection [PDF]. https://www.unicef.org/media/66616/file/industry-guidelines-for-online-childprotection.pdf

International Telecommunication Union. (2020, June 23). *ITU 2020 Guidelines on child online protection: Responding to new challenges and significant shifts in the digital landscape* [Press release]. International Telecommunication Union. https://www.itu.int/en/mediacentre/Pages/pr10-2020-Guidelines-Child-Online-Protecion.aspx

John, A., Glendenning, A. C., Marchant, A., Montgomery, P., Stewart, A., Wood, S., Lloyd, K., & Hawton, K. (2018). *Self-harm, suicidal behaviours, and cyberbullying in children and Young People: Systematic Review*. *Journal of Medical Internet Research, 20*(4). https://doi.org/10.2196/jmir.9044

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). *Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth*. *Psychological Bulletin, 140*(4), 1073–1137. https://doi.org/10.1037/a0035618

Livingstone, S., & Haddon, L. (2009). *EU Kids Online: Final report 2009* (EC Safer Internet Plus Programme Deliverable D6.5). EU Kids Online, London School of Economics and Political Science. http://eprints.lse.ac.uk/24372/

REFERENCES

Livingstone, S., & Helsper, E. (2007). Gradations in digital inclusion: Children, young people and the digital divide. New Media & Society, 9(4), 671–696. http://eprints.lse.ac.uk/2768/

Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. Journal of Child Psychology and Psychiatry, 55(6), 635-654. https://doi.org/10.1111/jcpp.12197

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). Children's data and privacy online: Growing up in a digital age. An evidence review. London School of Economics and Political Science. https://eprints.lse.ac.uk/101283/

Lupton, D., & Williamson, B. (2017). The datafied child: The data surveillance of children and implications for their rights. New Media & Society, 19(5), 780–794. https://doi.org/10.1177/1461444816686328

Moses, J. (2023, July 11–12). Evaluating government strategies for child online protection [Conference paper]. Proceedings of the Cyber Secure Nigeria Conference, Nigerian Army Resource Centre (NARC), Abuja, Nigeria. https://doi.org/10.22624/AIMS/CSEAN-SMART2023P115

Nikolopoulou, K. (2024). Children in the digital space: Issues, researches, and suggestions for future research. Creative Education, 15, 815–827. https://doi.org/10.4236/ce.2024.155049.

Ofcom. (2023). Children and parents: Media use and attitudes report. https://www.ofcom.org.uk/__data/assets/pdf_file/0027/255852/childrens-media-use-and-attitudes-report-2023.pdf

Organisation for Economic Co-operation and Development (OECD). (2020). Design for children (OECD Digital Economy Papers No. 363). OECD Publishing. https://doi.org/10.1787/c167b650-en

Qustodio. (2025). The all-in-one parental control and digital wellbeing solution. https://www.qustodio.com/en/

REFERENCES

Rayhan, A. (2023). How technology is harming our children: Understanding and overcoming the negative effects of screen time [ResearchGate post]. https://doi.org/10.13140/RG.2.2.34234.57288

Russell, I. (2024, April 30). For children to be safe online, it's not they who need to change – it's the tech companies. The Guardian. https://www.theguardian.com/commentisfree/2024/apr/30/children-safe-online-change-tech-companies-social-media

Sadiku, M., Ashaolu, T. J., Ajayi-Majebi, A., & Musa, S. (2021). Digital safety. International Journal of Scientific Advances, 2(5), Article 21. https://doi.org/10.51542/ijscia.v2i5.21

The Cyber Research Data Bank. (2024). Revolutionising child safety: The latest innovations in child-friendly tech. https://www.cyberdb.co/revolutionizing-child-safety-the-latest-innovations-in-child-friendly-tech/

Tomkova, J. (2023, September 23). Oversharing is not caring: Basic principles to teach your children. ESET. https://www.eset.com/blog/en/oversharing-is-not-caring-basic-principles-to-teach-your-children/

Twenge, J. M., & Campbell, W. K. (2018). Associations between screen time and lower psychological well-being among children and adolescents: Evidence from a population-based study. Preventive Medicine Reports, 12, 271–283. https://doi.org/10.1016/j.pmedr.2018.10.003

UNICEF. (2019). Child online protection: Guidelines for industry on child online protection. https://www.unicef.org

UNICEF South Asia. (2023, July 3). 5 ways to protect your young child online: Tips to help parents support their young children to stay safe online. UNICEF. https://www.unicef.org/rosa/stories/5-ways-protect-your-young-child-online

UNICEF. (2024). *Protecting children in the digital world.* https://www.unicef.org/nigeria/protecting-children-digital-world

REFERENCES

U.S. Department of Justice. (2025). Keeping children safe online.Child Exploitation and Obscenity Section, Criminal Division. https://www.justice.gov/criminal/criminal-ceos/keeping-children-safe-online

Wellspring Centre for Prevention. (2024). Strategies for teaching kids about online safety. Wellspring Center for Prevention https://wellspringprevention.org/blog/strategies-teaching-kids-online-safety/

World Vision International. (2015). Keeping children safe online [PDF]. https://www.wvi.org/sites/default/files/KCSO%20case%20study%20FINAL.pdf

www.thesafetychic.com