Digital Cooperation Organization

SAFE DIGITAL SPACE FOR CHILDREN

POLICY PAPER

2024

DOCUMENT DISCLAIMER

The following legal disclaimer ("Disclaimer") applies to this document ("Document") and by accessing or using the Document, you ("User" or "Reader") acknowledge and agree to be bound by this Disclaimer. If you do not agree to this Disclaimer, please refrain from using the Document.

This Document, prepared by the Digital Cooperation Organization (DCO). While reasonable efforts have been made to ensure accuracy and relevance of the information provided, the DCO makes no representation or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained in this Document.

The information provided in this Document is intended for general informational purposes only and should not be considered as professional advice. The DCO disclaims any liability for any actions taken or not taken based on the information provided in this Document.

The DCO reserves the right to update, modify or remove content from this Document without prior notice. The publication of this Document does not create a consultant-client relationship between the DCO and the User.

The designations employed in this Document of the material on any map do not imply the expression of any opinion whatsoever on the part of the DCO concerning the legal status of any country, territory, city, or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The use of this Document is solely at the User's own risk. Under no circumstances shall the DCO be liable for any loss, damage, including but not limited to, direct or indirect or consequential loss or damage, or any loss whatsoever arising from the use of this Document.

Unless expressly stated otherwise, the findings, interpretations and conclusions expressed in this Document do not necessarily represent the views of the DCO. The User shall not reproduce any content of this Document without obtaining the DCO's consent or shall provide a reference to the DCO's information in all cases.

By accessing and using this Document, the Reader acknowledges and agrees to the terms of this Disclaimer, which is subject to change without notice, and any updates will be effective upon posting.

TABLE OF CONTENTS

1

EXECUTIVE **SUMMARY**

EXECUTIVE SUMMARY

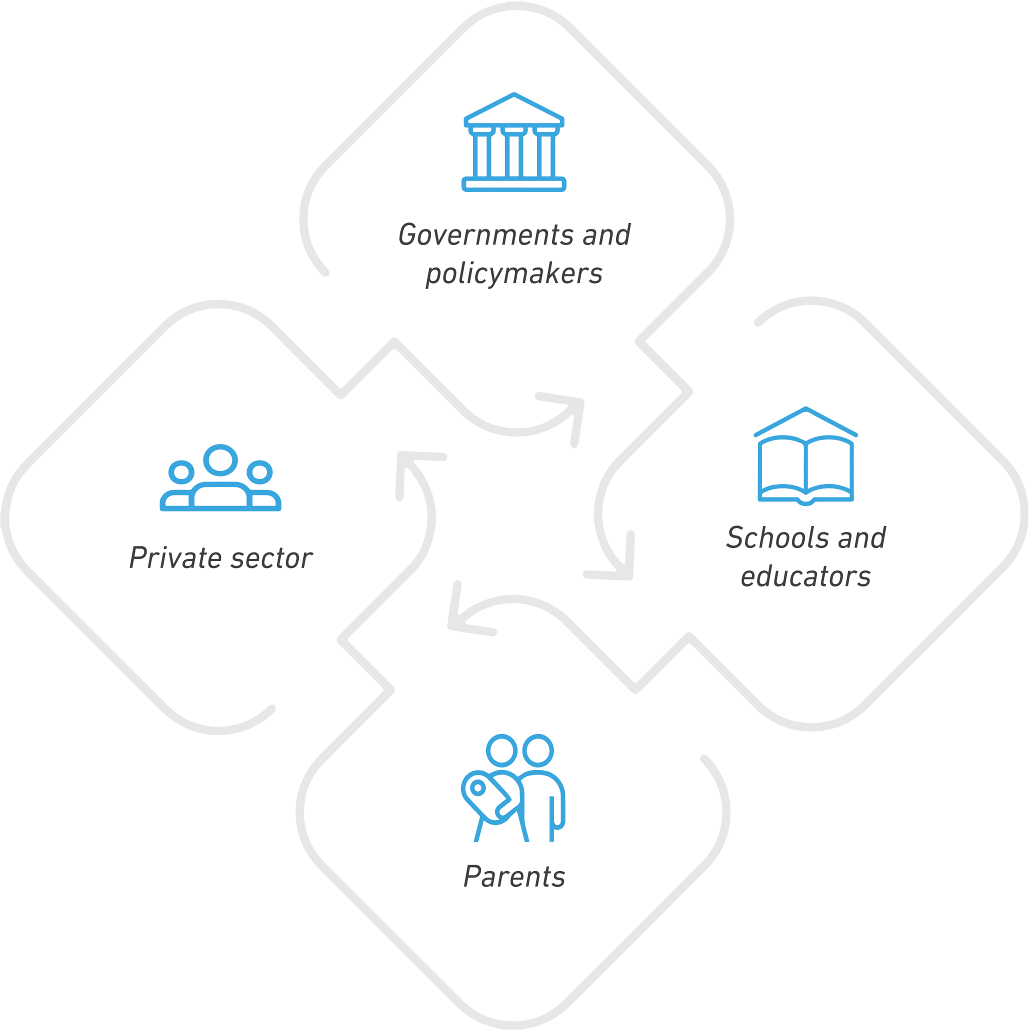
The challenges facing children in the digital world are escalating. With this concern, the Digital Cooperation Organization's (DCO) has developed this policy paper, which is based on extensive analysis, research, and discussion with experts that participated in the DCO's Digital Space Accelerator (DSA) global roundtable in:

- **Riyadh – September 19, 2023**
- **Cape Town – November 15, 2023**
- **Geneva – December 7, 2023**

In this policy paper, the reasons that make children especially vulnerable users of new technologies are presented, the main challenges to be addressed are outlined, and the most relevant stakeholders are identified.

Subsequently, some of the key initiatives carried out by various countries worldwide are analyzed, with a special focus on the DCO Member States. The policy paper culminates in presenting actionable policy recommendations to address the most pressing challenges and risks facing children in the online world.

Considering the analysis and research conducted, as well as the prospectives collected through the DSA roundtables, key policy recommendations, to be championed by different stakeholders are summarized as follows:



Governments and Policymakers should

Develop informational campaigns and resources, including guidelines for parents, teachers, and children around children's online safety.

Establish a minimum age limit for the use of AI tools in classrooms and emphasize the importance of teacher training in this field.

Regulate how advertisers target children and implement strict enforcement measures in case of non-compliance.

Mandate transparency from advertisers on their targeting practices and data collection.

Encourage and promote research, development and implementation of privacy-conscious, interoperable, and user-friendly technologies that can limit contact and access to content unsuitable for children.

Invest in public awareness campaigns on the risks of manipulative advertisements that are harmful for children.

Collaborate with technology advertising companies to jointly develop industry standards and best practices for children's online safety.

Join forces with other governments to enhance cybersecurity capabilities across DCO Member States, and encourage information sharing mechanisms at national and international levels.

Support targeted research projects to monitor and analyze long-term consequences on child victims.

Roll-out digital literacy programs to empower children and provide guidance on how to navigate digital spaces and showcase where to seek support.

Adapt film and broadcasting laws to the digital realm: leverage existing film and broadcasting laws and adapt them to the digital landscape to protect children in the online world.

Create holistic national child online safety strategies:

- Develop forward-looking and comprehensive national child online safety strategies, which include creating new, and streamlining existing policies, regulations, and enforcement/accountability mechanisms to ensure children's online safety.
- Create a national multi-stakeholder platform including legislators, policymakers and regulators, parents and guardians, children (especially the ones with vulnerabilities), educators and schools, private sector, healthcare and social services, non-governmental organizations (NGOs), and law enforcement and other agencies, responsible for guiding the formulation, execution, and oversight of the national or regional child online safety strategies.

Schools and Educators should

Integrate online safety modules into school curricula.

Establish school support programs, providing resources and pedagogical tools, and offer training to teachers so they can promptly identify and respond to the online risks facing their pupils.

Create helplines and forums within schools to ensure children can receive proactive support and advice on their online safety concerns.

Roll-out broad digital literacy programs informing children on wide-range of online threats they might be vulnerable towards.

Execute awareness campaigns focused on cyberbullying.

Provide educational materials and organize training sessions to equip parents with knowledge of new technologies and the risks associated.

Parents should

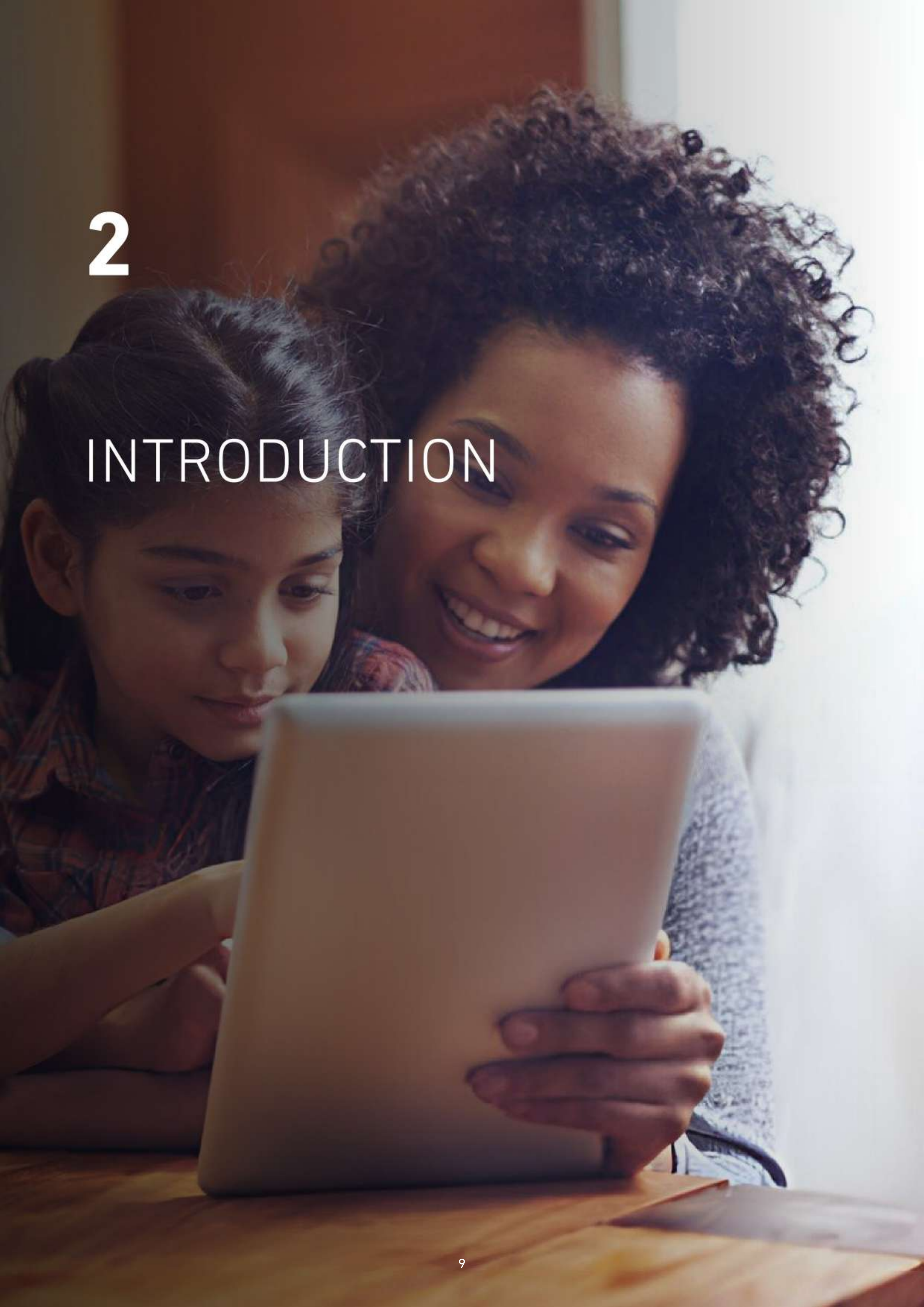
- Set clear guidelines and boundaries for internet usage, including time limits and approved websites or apps.
- Use parental control software to filter content, monitor online activities, and block inappropriate websites.
- Educate children about online risks such as cyberbullying, phishing, and identity theft, and encourage open communication about their online experiences.
- Encourage responsible online behavior by teaching children about privacy settings, the importance of not sharing personal information online, and the consequences of online actions.

Private sector should

- Create child-friendly mobile packages that limit exposure to harmful content.
- Adopt mechanisms and procedures to safeguard children online in the service offerings.
- Ensure transparency about existing products and services.
- Ensure the adoption of security-by-design principles in the provisions of new technologies and services.
- Develop assessment tools to verify how well safety and security-by-design practices are incorporated throughout the product development lifecycle, and undertake risk and impact assessments of the products and services with a focus to ensuring children's online safety.
- Incorporate children's inputs and prospectives while designing and planning new products and services to promote their children-friendliness.

2

INTRODUCTION



INTRODUCTION

In the era of rapid technological advancements, the concern of children's digital rights and protection is growing. As children increasingly start using web spaces from an early age, the need to safeguard their rights within these environments has become urgent to help maintain a social and prosperous society. This paper seeks to examine the multifaceted dimensions of children's digital rights, addressing key challenges such as privacy, cyberbullying, online harassment, inappropriate content, cybersecurity, and online safety. By exploring these issues through a human rights lens, this paper seeks to propose   policy recommendations aimed at fostering an online environment that nurtures the rights and well-being of children and creates a 'digital safe space' for them.

With this concern in mind, within the framework of various digital rights explored by the Digital Cooperation Organization (DCO) as a part of its digital policy advocacy, and aligned with the DCO Strategic Roadmap 2030, safe digital space for children was selected as a digital right for in-depth exploration. The goal of this exploration is to identify impactful and actionable policy recommendations, that upon their adoption, would strengthen the safety of children in the online world, especially across the DCO Member States.

This policy paper is based on extensive primary and secondary research conducted by the DCO through its innovative Digital Space Accelerator (DSA) mechanism that is aimed at engaging diverse global experts to garner ideas around nurturing an inclusive, safe, and sustainable digital economy.

The first question to address is what should be understood by the term 'child,'? Even the definition of adulthood varies from country to country due to cultural and political factors that precede the law. Moreover, within the definition of a child, there is a potential differentiation based on the child's age, which is rooted in the maturity and developmental stages that differ between a 10-year-old and a 16-year-old child. For the purposes of our paper, we use the United Nations Convention on the Rights of the Child (UNCRC)'s [1] definition of a child as any person under the age of 18. We have adopted this age for defining a child for the purposes of presenting our recommendations in this policy paper.

3

THE NEED FOR **SAFE DIGITAL SPACE FOR CHILDREN**

THE NEED FOR SAFE DIGITAL SPACE FOR CHILDREN

1. What is safe digital space and how can it be enhanced to ensure children's safety?

The concept of a safe digital space encompasses various dimensions concerning how individuals should be protected in the online world whilst mitigating online risks that can lead to real world harm. Overall, a 'safe digital space' refers to an online environment where individuals, especially children and vulnerable users, can interact, communicate, and engage in various digital activities without the risk of experiencing harm, exploitation, or abuse.

Some of the components and established measures aimed at ensuring the online safety and well-being of users, are:

Privacy Controls: Providing users with the ability to both understand and manage their privacy settings, ensuring that they have control over their personal information.

Cybersecurity measures: Implementing robust encryption and secure connections to protect user data from cyber threats and hacking activities.

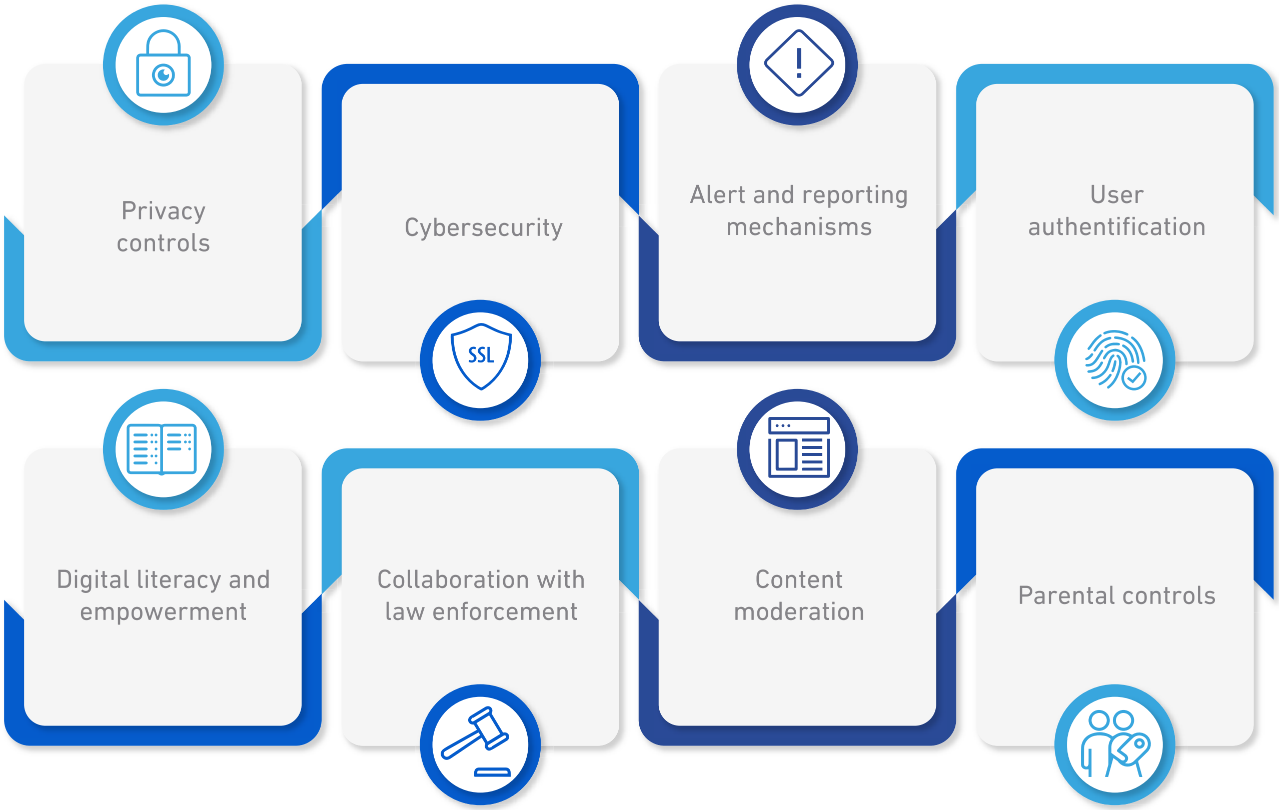
Reporting Mechanisms: Enabling users' easy access to report inappropriate content, cyberbullying, or any suspicious or illegal activities.

Collaboration with Law Enforcement: Establishing strong collaborations with law enforcement agencies and relevant authorities to address illegal or inappropriate activities such as online harassment, child exploitation, and cybercrimes in correlation with local laws and legislations.

Digital Literacy and Empowerment: Promoting digital literacy and empowering users with the knowledge and tools needed to protect themselves online.

Content Moderation: Enforcing effective content moderation tools and policies to prevent the spread of harmful or inappropriate content, including hate speech, violence, explicit materials, and frauds and scams.

Parental Controls: Offering parental control features that allow parents or guardians to monitor and restrict their children's online activities.



Privacy controls
Cybersecurity
SSL
Alert and reporting mechanisms
User authentification
Digital literacy and empowerment
Collaboration with law enforcement
Content moderation
Parental controls

Figure 1: Essential components of a Safe Digital Space

By integrating these components into holistic strategies, digital spaces can be enhanced, making it safer for those using them, and protecting them from online risks and threats.

2. Digital Security: What is Digital Security and how can it be enhanced?

Digital security has been identified by governments globally as one of their highest priority public policy areas. The foundation of data-intensive economic and social activities lies in an open, interconnected digital environment that facilitates the smooth and economical flow of data among diverse partners, spanning various organizations and jurisdictions. With increased dependency on data flow, comes the risk of its theft and misuse.

In recent years, digital security incidents have surged both in frequency and magnitude. Organizations find themselves increasingly vulnerable to these incidents. From an economic and social standpoint, these security breaches can severely impact an organization's reputation, financial stability, and operations. They jeopardize competitiveness, impede innovation efforts, and erode market positions. Such incidents can disrupt the availability, integrity, or confidentiality of crucial information and information systems that underpin economic and social activities. These incidents can result from deliberate malicious actions or unintentional factors such as natural disasters, human errors, or system malfunctions.

Particularly concerning are incidents involving personal data, often termed 'data breaches,' which have become alarmingly commonplace, compromising the confidentiality of individuals' personal information.

There are numerous reports and forecasts detailing the costs associated with security breaches in the digital economy. For instance, the IBM Cost of a Data Breach 2023 Report [2] reveals that the global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.

On the other hand, the United Nations Capital Development Fund (UNCDF)[3] reported that the economic impact of information and technology asset security breaches in 2020 reached a staggering USD 4-6 trillion, equivalent to approximately 4-6% of the global GDP. This translates into a significant $4.5 trillion impact in 2020.

In this context, security is regarded as a cornerstone for digitization, as it can either enhance or jeopardize trust in the digital economy. While security is undeniably critical for the whole digital economy, certain individuals, especially children, due to their developing maturity levels and increased exposure, are especially vulnerable to the security risks associated with new technologies of the digital world.

3. Why are children especially vulnerable?

Indeed, the first question to address is why children are particularly vulnerable in the digital realm and, why they deserve special care and protection. The answer begins with the extent of technology and digital penetration in the lives of children and youth today.

Globally, approximately one-third[4] of the internet's user base comprises children under the age of 18 (as of 2019/2020), highlighting the significant presence of young individuals in the digital realm. An increasing amount of evidence suggests that children are gaining access to the internet at progressively younger ages.

In certain nations[5], children under the age of 15 are just as likely to use the internet as adults over the age of 25. Smartphones are contributing to a 'bedroom culture'[6], where online access for many children is becoming more personal, private, and less supervised.

The recent COVID-19 pandemic serves as a significant example that accelerated the role of technology in children's education. To contain the spread of the virus, school doors worldwide remained closed for several months. The United Nations Educational, Scientific and Cultural Organization (UNESCO)'s data[7] on school closures due to COVID-19 vividly illustrates the pandemic's profound impact on global education. At its peak in early April 2020, educational institutions were closed in over 91% of countries, refraining nearly 1.6 billion students worldwide to physically attend schools. During this crisis, we witnessed widespread efforts to utilize technology for remote learning. But just as it increased children and young people's interaction with technology, it also heightened the exposure to online risks they are already susceptible to.

Moreover, the proliferation and abundance of online information sources has especially affected the younger generations. Understanding what is right or wrong, or recognizing a threat or risk, are aspects that children, and sometimes even adults struggle with. This concern has been highlighted by UNICEF[8], which warns that children may be especially susceptible to misinformation and disinformation due to their evolving maturity and cognitive capacities, including the development of diverse psychological and physiological motivations.

Excessive exposure to technology in the early ages can adversely affect the mental health of children[9] with depression being one of the big concerns. The impacts extend to other fundamental health and social issues, such as the impact on vision[10], and the development of interpersonal skills.

Regarding interpersonal skills, excessive dependence on technology can lead to increased isolation and hinder the positive personality development of a child. Since children are still in the process of forming their identity, the negative impacts can have a much more pronounced effect on them compared to adults.

The Organization for Economic Co-operation and Development (OECD) has mapped out [11] the following risks that the internet poses to children:

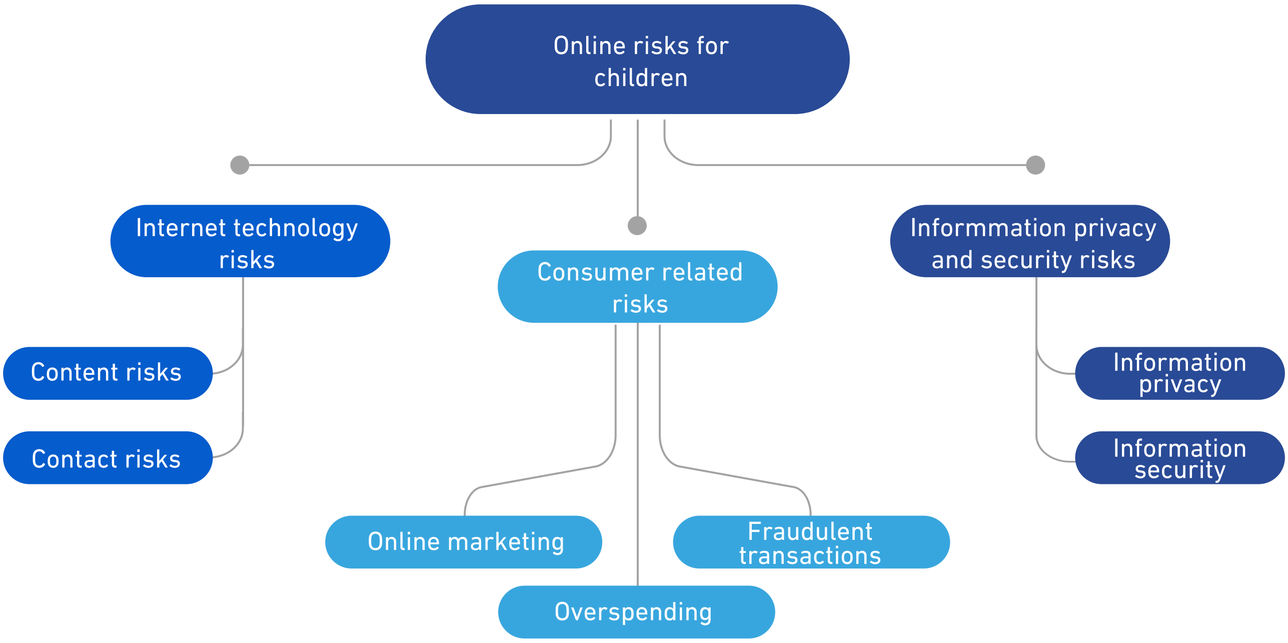


Figure 2: Risks posed by internet to children (OECD)

Since 2012, when the OECD conducted this mapping, additional risks such as **gambling** have been added to the list of reasons of children's vulnerability in the digital world.

More recently, experts have raised alarm about a new category of risks: '**lost in digital space**.' This expression refers to the vulnerable children of the current day who are growing up without adequate **internet safety education**. A recent study [12] highlighting this reality defines vulnerable children as those who are in care, have special educational needs, or face mental health, physical, or communication difficulties, making them more susceptible to online harms such as cyberbullying.

While it's not possible to list all the **threats** posed by the digital world for children, based on our primary and secondary research, below is a list of **key threats that we consider most relevant**.

To conclude, children are particularly vulnerable in the online world due to their evolving cognitive and emotional development, coupled with their inherent curiosity and lack of experience in discerning potential risks. The rapid advancement of technology has outpaced regulatory measures, leaving children exposed to various threats as mentioned above. Addressing these vulnerabilities requires a multifaceted approach that encompasses robust legal frameworks, comprehensive digital literacy programs, and collaborative efforts among stakeholders.

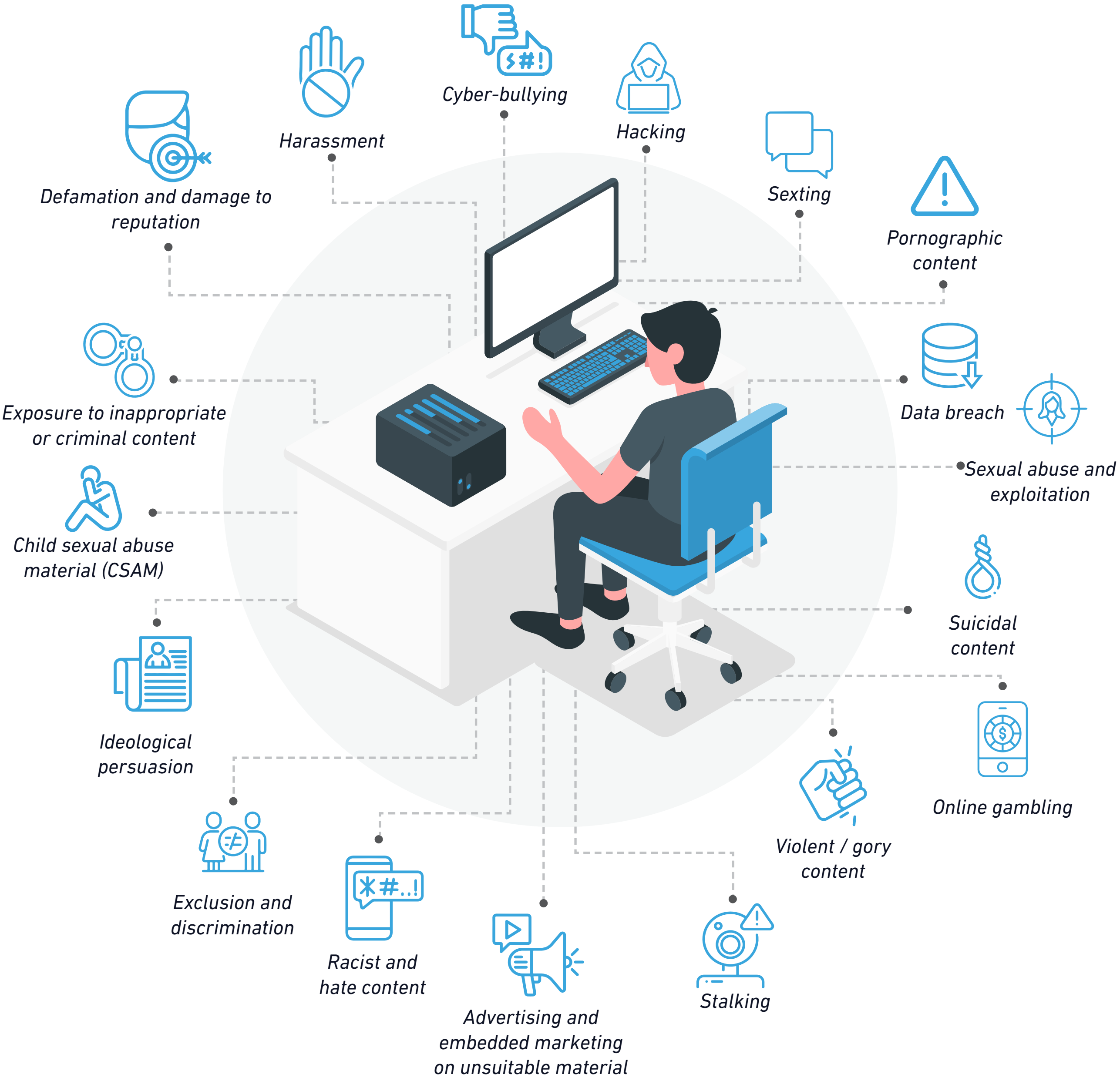

Cyber-bullying
Harassment
Hacking
Defamation and damage to reputation
Sexting
Pornographic content
Data breach
Exposure to inappropriate or criminal content
Sexual abuse and exploitation
Child sexual abuse material (CSAM)
Suicidal content
Ideological persuasion
Online gambling
Violent / gory content
Exclusion and discrimination
Racist and hate content
Advertising and embedded marketing on unsuitable material
Stalking

Figure 3: Threats posed to children in the digital world

4

KEY CHALLENGES **TO THE SAFETY OF CHILDREN ONLINE**

KEY CHALLENGES TO THE SAFETY OF CHILDREN ONLINE

a. What are the key challenges facing children's safety?

The internet has created entirely new social spaces globally, reshaping the way individuals interact. While these spaces can be incredibly creative, they also pose challenges, especially for children, that adults may not fully comprehend. As previously mentioned, children tend to embrace the internet early, often becoming pioneers and innovators in online spaces. They possess advanced skills and understanding, surpassing many adults in their use of the internet, especially in interactive and social networking platforms.

The ease of interaction among children, the threat of online abuse, rapidly evolving technology, and adults' limited awareness of the internet in some cases create a breeding ground for societal challenges related to children's wellbeing. This situation can lead to sensationalism, the creation of myths, and potentially misguided policy responses.

Some of the key challenges to the safety of children online are described below:

i) The addictive effects of social media networks

When it comes to social media networks, a primary concern [13] amongst online child safety advocates is how addictive social networks can become amongst children. Social media networks are designed to keep users active and engaged with some having an endless scrolling feature, a technique used to induce a sense of addiction. The act of endless scrolling immerses users, preventing them from naturally stopping. Consequently, it hinders them from considering the option of quitting or switching to alternatives. This aspect should be taken into consideration to understand the relationship between the use of these platforms and children's behavior [14].

One growing concern is that the social media platforms may have been contributing to exacerbating anxiety and depression, disrupting sleep patterns, promoting cyberbullying, and distorting body perception (which could lead to body shaming [15]).

Prolonged exposure to the social media has been linked to mental health issues [16]. Some reports [15] suggest that the crux of the matter lies in the duration and manner of online exposure. Numerous studies have demonstrated that teenagers [17] who extensively use social media platforms exhibit significantly higher rates of reported depression, ranging from 13 to 66 percent, compared to those who use these platforms sparingly.

Another potential contributor to depression amongst children could be the activities that teenagers are neglecting while spending time on social media, such as physical activities and pursuits that foster a sense of achievement, such as acquiring new skills and honing talents.

Speaking of other harmful effects of social media addiction, excessive use of social media can also contribute to low self-esteem, and feelings of loneliness among children. The constant comparison to others' lives and the pressure to maintain a certain image online can lead to negative psychological effects. Excessive use of social media can distract children from their studies, affecting their academic performance and productivity. Social media addiction can lead to a dependency on online interactions, causing children to prioritize virtual relationships over real-life interactions and activities.

In other words, moderate use of digital technologies can have a positive impact, whereas excessive use can adversely affect mental well-being. This is described as the "Goldilocks Effect": "moderate engagement in online and digital activities is beneficial in terms of subjective mental well-being and adolescent connectedness, whereas too much or too little might prove detrimental" [18].

ii) The impact of emerging technologies

Alongside social media networks, Children are usually the first category of users to be exposed to new and emerging technologies, including artificial intelligence, augmented reality, virtual reality, machine learning, and more. These new technologies hold an immense potential to positively influence children's cognitive development. Educational apps, games, and interactive tools can improve problem-solving, critical thinking, and information processing skills in an engaging manner. These technologies also empower young minds to explore independently. Learning STEM concepts like coding and programming enables children to dissect large, complex problems into manageable steps. Another crucial advantage of utilizing emerging technologies is that an early exposure to these technologies through hands-on experiential learning is vital for preparing children to meet future digital demands, and develop the right skills needed to prosper in the digital economy. As children learn and master these technologies, they are better equipped to explore diverse career opportunities in the evolving digital landscape. Indeed, this perspective is enshrined in UNESCO's Strategy for Technological Innovation in Education [19].

On the flipside, however, these technologies pose various risks to children's wellbeing. Concerns regarding the negative impact of emerging technologies are escalating as developments in these areas unfold rapidly.

In 2023, UNESCO released the world's inaugural comprehensive Guidance on Generative AI in Education and Research [20] that promotes a human centered approach to the use the Generative AI, and aims to mitigating harm that may accompany the development and use of this technology. This Guidance outlines seven essential steps that governments should follow to regulate Generative AI and establish policy frameworks for ensuring its ethical use in education and research. These steps, amongst others, include the adoption of global, regional, or national data protection and privacy standards. Additionally, it establishes an age limit of 13 for the use of AI tools in classrooms and emphasizes the importance of teacher training in this field.

UNESCO's recommendations stem from the concern that most GenAI applications are primarily designed for adult users, which raises substantial concerns for children. These applications can expose children to inappropriate content and risk of potential manipulation. Considering these risks and the persistent uncertainties associated with iterative GenAI applications, the implementation of age restrictions is strongly advocated by UNESCO as a precautionary measure to protect the well-being of children.

Besides the GenAI, immersive technologies have the transformative potential to reshape education fundamentally. However, our understanding of the effects of exposing children to multisensory experiences replicating the physical world in digital spaces is still in its infancy — and the limited research available raises some concerns on children's safety and wellbeing. For instance, a 2021 study [21] highlighted that immersive virtual reality could hinder the development of coordination necessary for children to maintain balance. Additionally, a 2021 review [22] of 85 studies on the impact of virtual reality on children identified evidence of cognitive challenges, difficulty distinguishing between real and virtual worlds, and potential addictive behavior. Perhaps the most significant concern revolves around how frequent and prolonged exposure to virtual environments affects mental health.

In summary, the impact of emerging technologies on children is undeniable, presenting both opportunities and challenges. While these innovations have the potential to enhance learning, creativity, and connectivity, they also raise concerns regarding privacy, mental health, and social development. As children navigate an increasingly digital world, it is imperative to adopt proactive measures that prioritize their well-being.

iii) Cyberbullying

Cyberbullying refers to the use of technology, platforms, and devices such as smartphones, computers, tablets, and gaming systems, to harass, threaten, embarrass, or target another person. Cyberbullying [23] stands out from traditional bullying due to two distinct features: anonymity and accessibility.

It can take various forms, ranging from obvious acts like harsh texts or comments to more subtle actions like posting someone's personal information, using hurtful photos or videos, or creating fake accounts to harass and bully others. Cyberbullying is harmful [24] and, in some cases, illegal. Severe or persistent cyberbullying can lead to serious consequences, including anxiety, depression, and other stress-related disorders in both victims and perpetrators. Tragically, in rare instances, some young individuals have also lost their lives to suicide due to cyberbullying.

A survey [25] conducted by Pew Research Center reveals that teenagers in the USA commonly experience various forms of cyberbullying, including:

- Offensive name-calling (32 percent)
- Spreading false rumors (22 percent)
- Receiving unsolicited explicit images (17 percent)
- Repeated requests for their location or whereabouts (15 percent)
- Physical threats (10 percent)
- Non-consensual sharing of explicit images (7 percent)

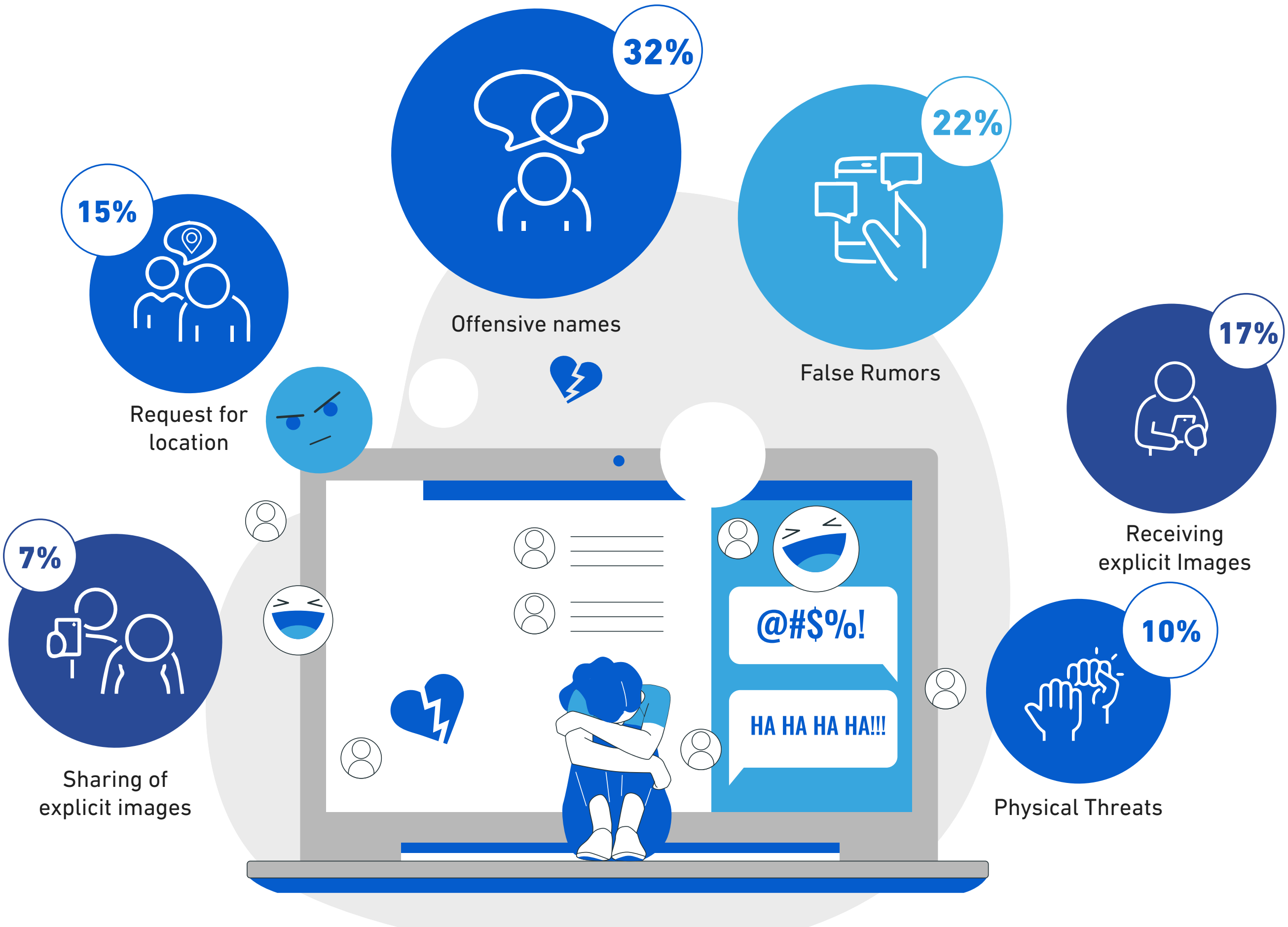


Figure 4: Various forms of Cyberbullying

Cyberbullying can be categorized into 5 groups

- Impersonating and account forgery
- Verbal violence
- Group violence
- Other Behaviors
- Visual violence

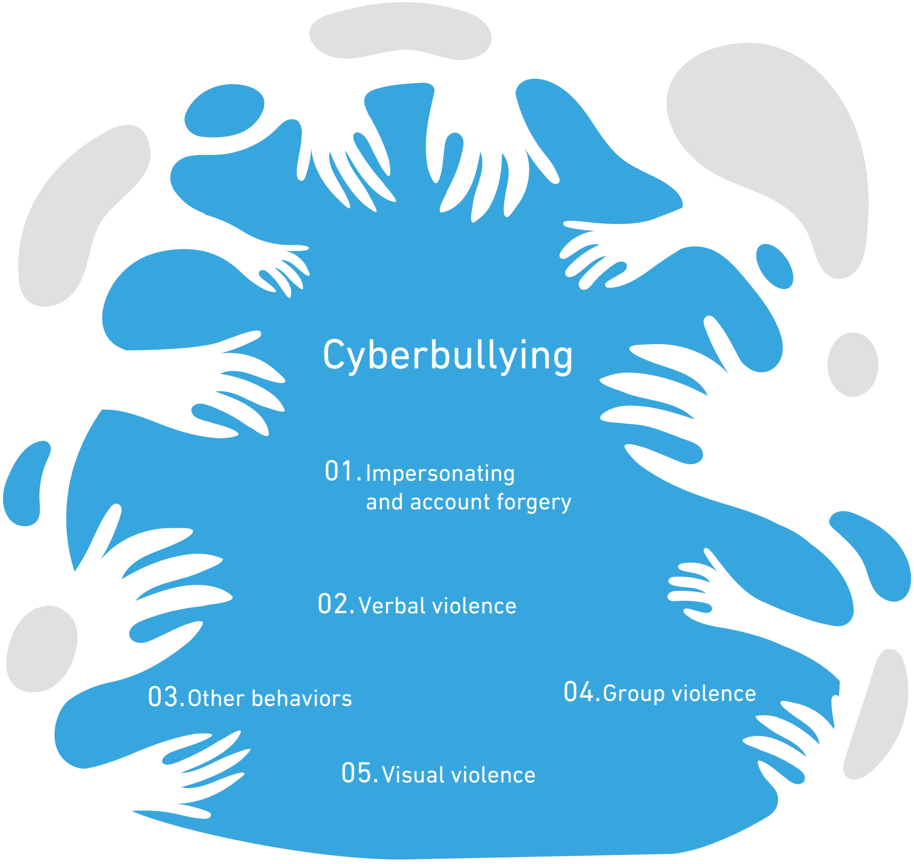


Figure 5: categories of cyberbullying

In 2019, UNICEF [27] highlighted the dangers presented by online violence, cyberbullying, and digital harassment for the 70.6 percent of young people aged 15 to 24 years old who were online globally. UNICEF called for concerted action to address and prevent violence against children and young people online.

Comparitech [28], a cybersecurity and privacy research firm conducted a survey involving over 1,000 parents of children aged 5 and above. Analyzing the trend from 2018 to 2022, it was reported that an increasing number of parents were reporting instances of bullying affecting their children, both at school and online. 10.5% of the parents reported that they witnessed their children being cyberbullied. While most of the bullying occurred in physical locations, bullying on digital platforms occurred in a wider variety of outlets. Nineteen percent of bullying was through social media, and eleven percent was through text messages.

The COVID-19 pandemic further exacerbated the issue significantly. The increase in cyberbullying during this time can be attributed, at least in part, to the additional leisure time and increased online presence of children during lockdowns and online schooling. Researchers from the

Universities of Florida and Denver conducted a study [29] indicating a notable rise in cyberbullying levels on Twitter due to the global pandemic. Their analysis of 454,046 publicly available tweets related to cyberbullying demonstrated a clear link between the pandemic and the surge in cyberbullying incidents.

On the legislative front, specific laws addressing cyberbullying are relatively recent and not commonly adopted. As a result, many countries utilize existing laws against harassment to penalize cyberbullies. In jurisdictions that have enacted specific cyberbullying laws, deliberate online actions causing significant emotional distress are considered criminal offenses. Victims in these countries have the legal right to seek protection, block communication from specific individuals, and impose restrictions on the use of electronic devices by the perpetrators of cyberbullying, either temporarily or permanently.

Recently, the OECD [30] released the first benchmarking report examining the policies and procedures related to child sexual exploitation and abuse (CSEA) of the world's top 50 global online content-sharing services, a clear indication that these issues are at the forefront of the global agenda.

iv) Frauds and scams

Children lack the necessary experience and skills to navigate the internet securely. Their personal information, coupled with access to devices, makes them vulnerable targets for scammers. The scammers' goal is typically to use the acquired information for fraudulent schemes. Scammers often target payment information and gain access to computers through malicious software. The goal is typically to use the acquired information for fraudulent purchases or to sell it on the dark web. Some of the challenges that children face related to frauds and scams when they are online include:

- **Online Predators:** Predators may use fraudulent tactics to gain the trust of children online, posing as peers or authority figures to manipulate them into sharing personal information or engaging in inappropriate activities.
- **Phishing Scams:** Children may fall victim to phishing scams where they receive fraudulent emails, messages, or links that appear to be from legitimate sources but are designed to steal personal information such as passwords or financial details.
- **Fake Websites and Apps:** Children may encounter fake websites or apps that mimic legitimate ones but are created to deceive them into providing personal information or downloading malware onto their devices.
- **In-app Purchases and Microtransactions:** Some online games and apps target children with deceptive tactics to encourage them to make in-app purchases or microtransactions without fully understanding the costs involved, leading to unauthorized charges on their parents' accounts.
- **Identity Theft:** Children's personal information, such as their name, address, or Social Security number, may be stolen and used for identity theft purposes, including opening fraudulent accounts or applying for loans or credit cards in their name.
- **Online Scams and Schemes:** Children may be lured into various online scams and schemes, such as fake charity fundraisers, get-rich-quick schemes, or work-from-home opportunities, which can result in financial loss or other negative consequences.
- **Lack of Digital Literacy:** Many children lack the necessary digital literacy skills to recognize and respond appropriately to online frauds and scams, making them more vulnerable to exploitation and manipulation.

In summary, the risks of online fraud and scams are pressing concerns with far-reaching implications. From fostering addictive behaviors to exposing children to financial risks and potential exploitation, the impact on children's well-being cannot be overstated. Urgent action is needed to implement stringent regulations, enhance parental controls, and bolster educational efforts to effectively mitigate these risks. By addressing these challenges directly, we can strive to create a safer digital environment where children are shielded from the harmful effects of frauds and scams and empowered to make informed decisions about their online activities.

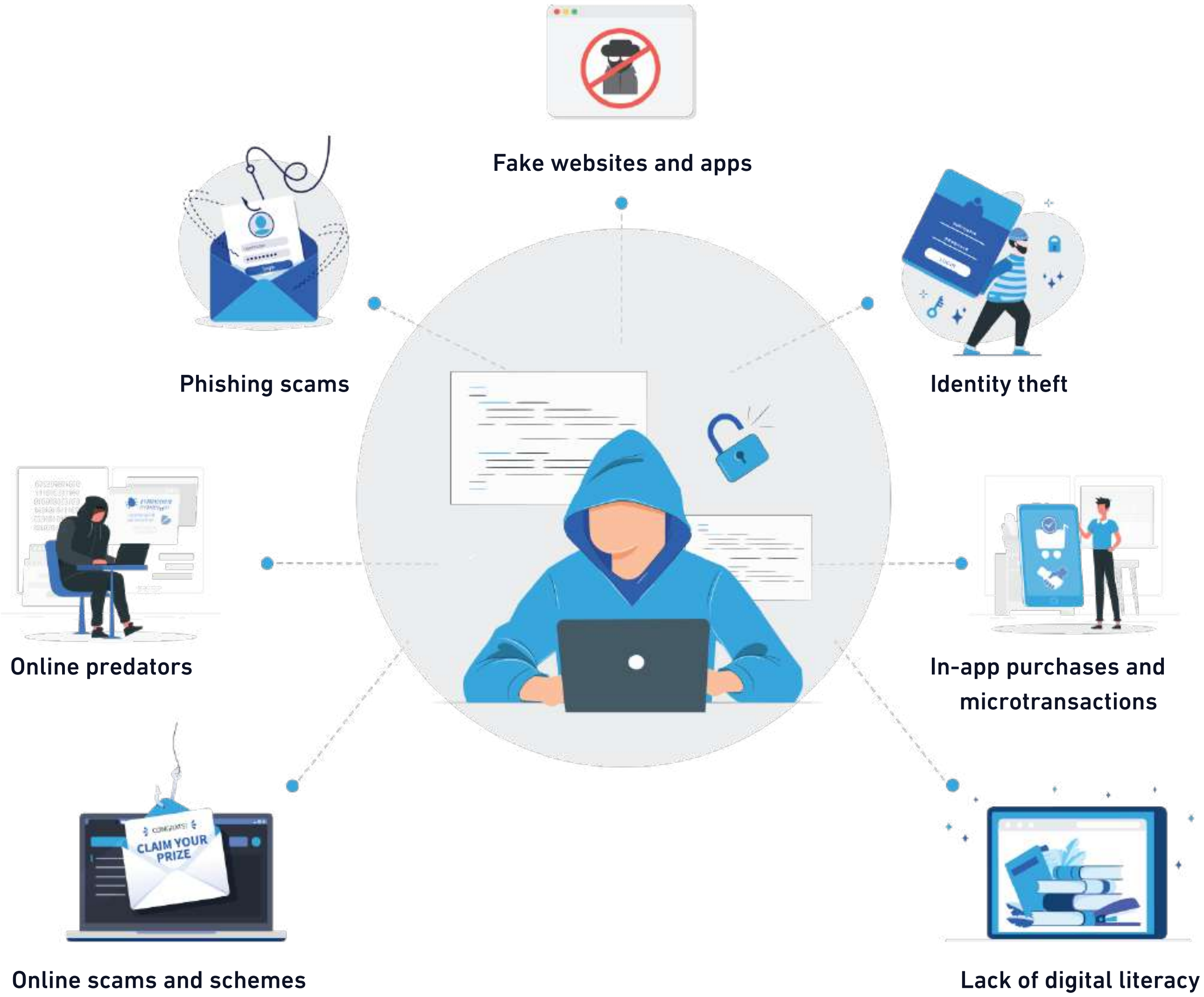


Figure 6: Frauds and scams

v) Data privacy

Traditionally, privacy has been understood as an individual's ability to control the information they consciously shared with others. However, in our increasingly interconnected world, where communication and information technologies are becoming more advanced and commercially significant, the concept of privacy is shifting away from being purely 'personal.' It is now embedded within a complex and evolving data ecosystem that encompasses various types of data. This environment goes beyond individual control or awareness, redefining privacy not only as 'the personal' but also challenging the traditional boundaries of 'the private' [31].

The connection between online privacy and data has grown increasingly intricate. Consequently, this presents a considerable challenge in media literacy for children, as well as their parents and teachers, as they strive to comprehend and critically engage with the digital landscape.

Experts [32] categorize the complexity of children's online privacy into three levels:

- **Interpersonal privacy:** pertaining to how their 'data self' is generated, accessed, and shared through online social connections.
- **Institutional privacy:** related to how public agencies such as government, educational, and health institutions collect and manage data about them; and
- **Commercial privacy:** concerning how their personal data is collected and utilized for business and marketing endeavors.

Figure 7: Levels of children's privacy

It is essential to understand why the issue of online privacy is so urgent concerning children. Firstly, because it is often children who pioneer the experimentation and use of new digital devices and content, navigating the risks associated with these uses without adult awareness.

Secondly, the growth of the data economy makes the collection of data profitable, especially from more vulnerable targets such as children, who lack the necessary literacy to comprehend the dangers of data access or the significance of privacy. Children's data is frequently gathered and processed without true informed consent, encompassing details like geolocation, biometrics, and other sensitive information. This practice can potentially result in misuse, identity theft, privacy invasion, exposure to inappropriate advertising and spam, and incurring undisclosed costs.

One of the most recent examples highlighting the relevance of children's privacy is the recent incident involving TikTok. Irish regulators fined TikTok €345 million (£296 million) for violating children's privacy. The investigation by Ireland's Data Protection Commission (DPC) began in September 2021, focusing on TikTok's compliance with EU data protection laws during the period from July 31, 2020, to December 31, 2020. This case underscored the increasing scrutiny and penalties faced by social media platforms for lapses in data protection, especially concerning children and young users. The DPC's investigation revealed that TikTok had violated EU data protection rules by setting the default profiles of users aged 13-17 to public settings, allowing anyone, both on and off TikTok, to view their content and contact them. TikTok also failed to provide adequate transparency to child users regarding the handling of their data, steering them towards more privacy-intrusive options. Family pairing settings lacked verification mechanisms to confirm that the adult linked to a child's account was indeed the parent or guardian, enabling over-16s to access direct messaging features. This penalty reflected a broader trend of regulatory actions against social media platforms for privacy shortcomings. Meta, the owner of Facebook, received a €1.2 billion fine in 2023 and was ordered to halt data transfers to the US. Instagram, owned by Meta, faced a €405 million fine for failing to protect children's data in September 2022.

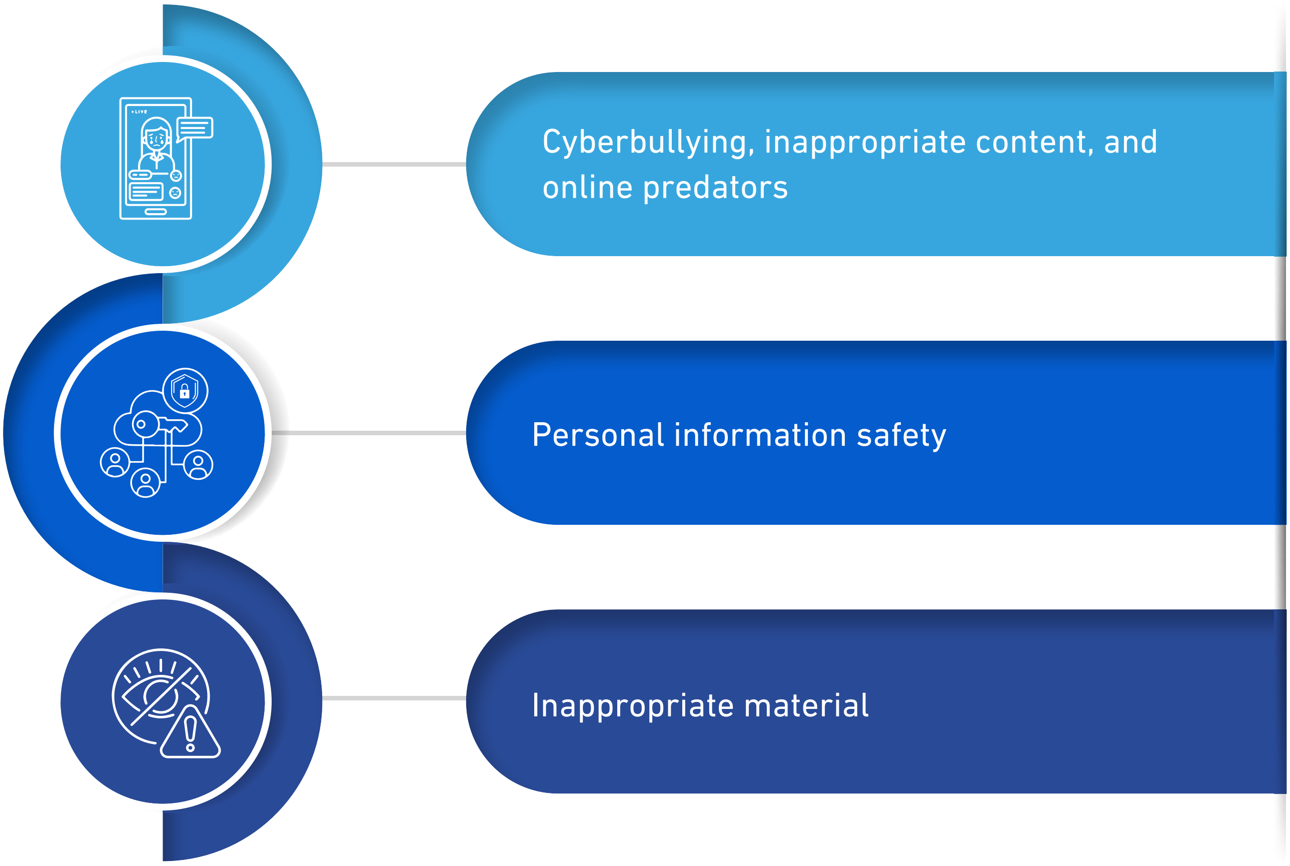
To conclude, the challenge of data privacy poses a significant threat to children's online safety and digital rights. By prioritizing data privacy as a fundamental aspect of children's digital rights, we can create a more secure online environment where their rights are respected, and their well-being is preserved.

vi) Cybersecurity

The significance of the challenge of children's cybersecurity is underscored by their increasing internet connectivity. Young people serve as the primary driving force behind global connectivity, with 75% of individuals aged 15 to 24 being online in 2022, a notable increase [33] compared to the 65% observed in the rest of the world's population.

Cybersecurity is crucial for children for several reasons:

- The first reason is related to protection from online threats such as cyberbullying, inappropriate content, and online predators. Cybersecurity measures help create a secure online environment, shielding them from potential harm.
- Secondly, it is important to mention personal information safety, as children often share personal information online, and cybersecurity safeguards prevent unauthorized access to this information. Protecting their data helps prevent identity theft and other malicious activities.
- Thirdly, robust cybersecurity measures include content filtering to prevent children from accessing inappropriate material. This helps maintain a positive and age-appropriate online experience.



Cyberbullying, inappropriate content, and online predators

Personal information safety

Inappropriate material

Although it extends beyond the realm of cybersecurity, the Better Internet for Kids initiative developed by the European Union stands out as one of the most prominent projects in this domain. Notably, the Better Internet for Kids (BIK) Policy Map serves as a valuable tool for comparing and sharing insights on policy development and implementation across EU Member States. It focuses on the themes and recommendations outlined in the European Strategy for a Better Internet for Children, initially introduced by the European Commission in May 2012. In fact, In May 2022, a new strategy for a better internet for kids (BIK+) [34] was launched, aiming to ensure that children are protected, respected, and empowered online in the new Digital Decade, in alignment with the European Digital Principles.

b. What are some of the ethical considerations around children's online safety that warrant attention?

The safety of children in the digital space raises several questions encompassing ethical, political, and moral dimensions. Addressing these questions shape the choices policymakers must make while devising public policies and legal frameworks around children's digital rights.

The first question concerns the level of autonomy and choices available to children while accessing digital technologies and online platforms: Should the access be limited, and under what circumstances should these limits occur? Additionally, there is the issue related to the age up to which parents and guardians should play an active role in making choices on behalf of their children. In other words, how to reconcile children's independence with the need of overseeing their safety and security, both offline and online. The manner and balance in which these dimensions should be reconciled are ethical, political, moral, and even ontological questions that must be addressed while shaping policies and legal solutions to promote children's digital rights.

The second question is related to the role we envision for schools. While the family should be the central unit for a child, determining the boundaries of the school's and teachers' field of action is another question that needs to be answered thoughtfully. Similarly, what role should be assumed by public authorities and entities, with governments at the forefront? It is essential to assess the responsibility they should bear concerning children and in defending and protecting their safety.

These questions cannot be answered in isolation. While answering these questions, it is crucial to understand the context and legal framework of countries, as well as their social, economic, political, cultural, and religious realities. These dimensions are fundamental in shaping the perspective that should be adopted when promoting digital rights of children, especially their safety online.

In conclusion, the multifaceted challenges confronting children's digital rights and online safety demand urgent attention and concerted action from all stakeholders. From the pervasive influence of social media and the rapid advancement of technology to the insidious threats of cyberbullying, online harassment, and exposure to inappropriate content, children face a complex landscape fraught with risks. Furthermore, the emergence of online gambling, data privacy breaches, cybersecurity vulnerabilities, and the integration of technology in schools present additional concerns that must be addressed. These challenges not only impact children's immediate well-being but also raise profound ethical, policy, and moral questions about their rights in the digital age.

Considering the above, it is important to emphasize that the solutions devised to enhance the protection of children in the digital world must involve the engagement of the most relevant stakeholders. Only through this approach will it be possible to address the challenges listed earlier, seeking to ensure the well-being of children, the ultimate goal to which all societies should be committed.

5

CHAMPIONS OF CHANGE: RELEVANT STAKEHOLDERS OF **CHILDREN'S DIGITAL RIGHTS AND THEIR ROLE**

CHAMPIONS OF CHANGE: RELEVANT STAKEHOLDERS OF CHILDREN'S DIGITAL RIGHTS AND THEIR ROLE

To effectively navigate the complexities and challenges discussed in the earlier section, collaborative efforts are essential, spanning across a diverse set of stakeholders including governments, educators, technology companies, parents, and civil society. Only by prioritizing children's digital rights and online safety, and implementing collective and proactive measures by all the relevant stakeholders to address these challenges, can we pave the way for a safer, more empowering digital future for all children.

Unfortunately, efforts [35] to protect children in the digital world have not borne significant results due to the lack of collective engagement from all stakeholders. Identifying the right stakeholders [35] is crucial, not only from a conceptual standpoint but also to ensure that everyone knows their responsibilities towards the collective cause of protecting our children [36].

To start with, children themselves are the key stakeholders in the process of protecting their rights. One of the issues has been the lack of engagement with children themselves. It is essential to involve them, starting by understanding their motivations, concerns, and vulnerabilities adequately.

Parents are also crucial in providing their children with the necessary information, and are key players in adopting preventive and vigilant behaviors to protect children's digital rights [37]. Alongside parents, educators are entrusted with the task of guiding and supporting young individuals, particularly younger children, in utilizing services that encourage positive behaviors. Their pivotal role in education and awareness is recognized as a fundamental frontline defense in minimizing risks.

Government and industry's role in devising and implementing strategies to empower children to protect themselves is crucial. This encompasses promoting awareness and education among children to help them navigate online risks. Investment in welfare measures is imperative to address the needs of children who have suffered harm due to sexual exploitation and abuse on the Internet. Additionally, building the capacity of professionals who work with these affected children is essential for effective support and intervention.

Every stakeholder bears the responsibility of ensuring children's safety in the online realm. The role and importance of each key stakeholder in protecting children's digital rights is elaborated further below.

1. Parents and Guardians

Hardly any child protection strategy can succeed without the involvement of parents and families. The protection of children's online safety starts primarily at the home, and with the family. As younger children explore the internet and use technology beyond school hours, parents and caregivers assume a crucial role in educating their children about technology. They need to be equipped with adaptable ways to respond to safety incidents and effectively manage their child's online exposure to risks.

Parents often lack awareness about the online threats their children face, and many are not equipped with the knowledge, training, and skills needed to effectively protect their kids. Keeping pace with the rapid advancements in technology, much like law enforcement, proves to be a challenge for parents. Additionally, discussing sensitive topics openly with their children can be daunting for many parents.

A significant percentage of parents do not closely monitor their children's online activities [38], and incidents often go unreported to authorities. Addressing this gap in parental understanding and involvement is essential for fostering a safer online environment for children.

Therefore, empowering and educating parents to recognize the risks and challenges facing their children is paramount. Strengthening parents' abilities to guide and safeguard their children is a fundamental aspect of online safety.

Furthermore, technology can act as a valuable bridge in parent-teacher communication, ensuring parents are kept abreast of their children's school activities and engaging them in meaningful discussions and activities.

2. Governments, Policymakers and Law Enforcement Agencies

In addition to parental involvement, a greater comprehensive response for protection requires collaborative efforts from both public and private institutions. This involves establishing robust legislative frameworks to define harmful digital activities thereby creating the foundation to deter and prosecute potential abusers. It also requires fostering collaboration between justice and social welfare sectors, enhancing awareness about child protection services, and educating professionals working with children.

Governments and policymakers also collaborate with other relevant stakeholders, including schools, parents, NGOs, and industry partners, to raise awareness about online safety issues. They support educational programs, campaigns, and resources that empower children, parents, and educators with the knowledge, skills, and tools needed to navigate the online world safely.

Legislators and policymakers establish the rules and measures for the protection of children in the digital world, especially where state intervention is paramount. The drafting of laws, their implementation, as well as their modification when the results obtained are not in line with the intended objectives, necessitate that these stakeholders play a central role in promoting a safe digital space for children.

Policymakers play a leading role in co-creating and co-developing comprehensive policies, guidelines, and frameworks that address the unique challenges and vulnerabilities faced by children in the digital age. These policies, amongst others, could cover areas such as online education, digital literacy, parental controls, safe online gaming, social media usage, and protection against online exploitation and abuse.

Finally, law enforcement agencies play a vital role in enforcing laws related to online child protection, investigating cybercrimes, and apprehending offenders who target children online. It is their responsibility to work proactively to identify and disrupt online predators, trafficking networks, and illegal activities involving children, while also providing support and protection to victims and their families.

3. Schools and Educators

Schools, teachers, and education systems are pivotal in promoting safe and responsible internet usage. The dilemma for schools lies in mitigating the potential negative aspects of the internet and digital devices while preserving their educational and social benefits. To achieve this balance, it is essential for the schools to train children, as well as the educators, on managing online risks.

For this, amongst other things, schools and education systems can employ various strategies including implementing comprehensive educational programs that teach students about online safety, digital citizenship, privacy protection, cyberbullying prevention, and responsible use of social media and the internet. Schools should enforce robust cybersecurity policies within their online educational portals to reduce the risk of cyberattacks. They should establish clear guidelines for safe internet use within the school premises, including rules on accessing appropriate websites, avoiding sharing personal information online, and reporting any suspicious or harmful online activities.

Schools, teachers, and support staff need to be aware of how to recognize and respond to online safety issues. This awareness is essential for effectively protecting and supporting their students online.

4. Private Sector and Technology Firms

Big Tech and the private sector have started to initiate youth trust and safety programs. For example, TikTok has developed the TikTok for Younger Users which is aimed at providing additional privacy and safety features for children under 13, including restrictions on commenting and content posting. Facebook and Instagram also offer various anti-bullying tools.

However, there is growing pressure on these companies, whose hardware and software serve as primary access points for children online, to intensify their efforts in child protection. To achieve meaningful results in enhancing children's safety in the digital world, there must be a deeper commitment and collaboration among tech giants. This includes establishing industry standards and developing innovative solutions to effectively address children's online safety risks.

Safety features should be seamlessly integrated into products and services commonly used by children to ensure the strategies and initiatives therein are truly effective. It would also be pertinent for the private sector to establish systems for monitoring and publicly reporting cyber threats and incidents. This enhanced transparency regarding the challenges faced by children can pave the way for more targeted and impactful solutions.

5. Children and Youth

Children and youth play a crucial role in promoting a safe digital space, and their involvement is vital for creating a positive online environment. In fact, as children are the intended recipients and beneficiaries of any policy recommendations, strategies and initiatives aimed at protecting them online, their insights and feedback are essential for designing effective protection measures that address their specific needs, challenges, and preferences. This ensures that the policies, strategies, and initiatives implemented are relevant and impactful.

Engaging children as stakeholders raises their awareness about online safety issues and encourages them to become more conscious and responsible digital citizens. It helps them understand potential risks, learn how to protect themselves online, and develop critical thinking skills to navigate the digital world safely.

Furthermore, children and youth often have innovative ideas and creative solutions to address online safety challenges. By involving them in the process, we can tap into their creativity, imagination, and digital skills to develop innovative tools, resources, and campaigns that resonate with their peers and promote positive online behaviors.

Finaly, engaging children as stakeholders in their online protection initiatives can have a long-term impact by instilling lifelong habits of responsible digital citizenship, ethical online behavior, and proactive risk management. It lays the foundation for a safer and more inclusive digital environment for future generations.

In the engagement process, it is important to consider children based on their age group, paying special attention to children with vulnerabilities.

6. Non-Governmental Organizations, International Organizations and other Agencies

Any kind of private organizations that operate independently from government control, multilateral organizations that are governed by the international law, and/or other autonomous organizations/agencies that focus their endeavors on protecting children's digital rights, should be considered as key stakeholders in ensuring safe digital space for children.

These entities can advocate for global awareness and action on the issues related to children's online safety and contribute to the development of national, regional, and global policies and guidelines related to children's online protection. These organizations engage in research endeavors aimed at comprehending the dynamic nature of online threats to children. Through the collection of data and the generation of insights, they actively contribute to the formulation of evidence-based policies and the crafting of effective strategies.

7. Healthcare and Social Service Providers

Healthcare and social services providers play important roles as stakeholders in protecting children's online safety through their support mechanisms, initiatives, and interventions. Their specialized services to give support to children and young people who are victims of online or offline abuses or illicit behaviors are vital to children's online safety ecosystem.

Healthcare professionals and social workers are trained to assess children's vulnerabilities and risks related to online safety. They can identify signs of online abuse, cyberbullying, grooming, and other online threats, and provide preventive measures and interventions to mitigate these risks. They offer counseling, therapy, and support services to children who have experienced online harm or trauma while providing a safe and confidential space for children to express their concerns, process their emotions, and develop coping strategies for dealing with online safety issues.

Healthcare and social services providers also collaborate with law enforcement, child protection agencies, mental health services, and other stakeholders to coordinate responses, share information, and provide holistic support to children at risk of online harm.

These stakeholders contribute to the holistic well-being of children, addressing mental health, physical health, and social aspects impacted by digital experiences. Their involvement in the ecosystem ensures a comprehensive and coordinated approach to safeguarding children in the digital age.

In conclusion, ensuring a safe digital space for children requires a concerted effort from a wide range of stakeholders. Parents and guardians play a crucial role in guiding and supervising children's online activities. Governments, policymakers, and law enforcement agencies are responsible for enacting and enforcing laws, policies, and regulations that protect children online and hold perpetrators accountable. Schools and educators are instrumental in promoting digital literacy and teaching children how to navigate the online world responsibly. The private sector and technology firms have a responsibility to develop and implement tools, platforms, and policies that prioritize children's safety and privacy. Children and youth themselves should be empowered as active participants in creating safer online environments through education and awareness. Non-governmental organizations, international organizations, and other agencies provide support, resources, and advocacy for child online safety initiatives. Finally, healthcare, and social service providers play a vital role in identifying risks, providing counseling and support, and collaborating with other stakeholders to protect and ensure the well-being of children in the digital age.

By working together collaboratively, these stakeholders can contribute to the development of comprehensive strategies and solutions that safeguard children's online experiences and promote their healthy development.

6

GLOBAL POLICY AND LEGAL ENDEAVORS FOR **CHILDREN'S ONLINE PROTECTION**

GLOBAL POLICY AND LEGAL ENDEAVORS FOR CHILDREN'S ONLINE PROTECTION

The quest towards safeguarding children's digital rights and cultivating a safe online environment for their growth and development has sparked a global movement of advocacy, policy-making, and collaborative action. From establishing legal frameworks and policy guidelines to fostering digital literacy and promoting responsible online behavior, a myriad of efforts is underway globally to ensure that children can navigate the digital landscape securely and confidently. In this section, we delve into a diverse array of global policy endeavors that are aimed at safeguarding children's digital rights and creating a safe digital space where they can thrive.

The **United Kingdom** has implemented the Children's Code [39], also known as the Age-Appropriate Design Code, which outlines 15 standards that online services must adhere to. These standards ensure compliance with data protection laws, specifically safeguarding children's online data. The code applies to various online services, including Apps; Games; Connected toys and devices; and News services.

The UK government is also actively engaged in a comprehensive review to comprehend the impact of social media on children's well-being and establish guidelines for healthy screen time limits. In October 2023, in the UK, the Online Safety Bill [40] was officially enacted into law as the Online Safety Act, following the granting of Royal Assent. This legislation aims to shield users from harmful online content, compelling social media companies to promptly remove any illegal material posted on their platforms. The bill also introduces new offenses addressing image-based sexual abuse, including cyberflashing and the sharing of 'deepfake' pornography. Notably, while the act prohibits the dissemination of such content, the creation of deepfake pornography itself remains legal.

The **Swedish** Authority for Privacy Protection, The Ombudsman for Children in Sweden, and the Swedish Media Council, have released a guide with several principles [41]. This guide outlines specific aspects of the General Data Protection Regulation (GDPR) concerning the processing of personal data related to children and young people. These principles mandate that those handling data related to children can only collect personal information for explicit and legitimate purposes. They should not collect more data than necessary for these purposes, must ensure data accuracy, delete information when it's no longer needed, and protect the data from unauthorized access. This guide is primarily intended for stakeholders involved in creating and managing digital environments where children and young people frequently engage.

The **Netherlands** introduced 'The Code for Children's Rights,'[42] designed to assist developers and designers in prioritizing children's rights during the development of digital services. This Code comprises ten principles, supported by practical implementation examples. While the principles themselves are not legally binding, they are rooted in existing laws and regulations, such as the UN Convention on the Rights of the Child (1989) [43], which holds legal weight. This Code has 10 principles:

- **Principle 1:** Make the best interests of the child the primary consideration when designing.
- **Principle 2:** Involve children and their expectations in the design process.
- **Principle 3:** Ensure the legitimate processing of personal data of children.
- **Principle 4:** Provide transparency in a way that is understandable and accessible to children.
- **Principle 5:** Carry out a privacy impact assessment based on children's rights.
- **Principle 6:** Provide a child-friendly privacy design.
- **Principle 7:** Prevent the profiling of children.
- **Principle 8:** Avoid the economic exploitation of children at all times.
- **Principle 9:** Always avoid a harmful design for children.
- **Principle 10:** Develop industry guidelines which are geared to protecting the interests and rights of children.

In 2021, in **France,** the Paris Peace Forum [44] hosted the launch of an international Call to stand up for children's rights in the digital environment. French President Emmanuel Macron and UNICEF, along with seven other states, a dozen non-governmental organizations, and most of the major digital platforms (including Amazon, Google, YouTube, Meta, Microsoft, Dailymotion, Qwant, Snap, X, and TikTok) signed this Call and committed to enabling children to use digital tools safely and benefit from their full potential without being exposed to abuse through a series of actions. The French government has announced creation of a Children Online Protection Laboratory (COPL) [45] with the goal of improving kids' online safety globally. The COPL is aimed to explore, promote, develop and evaluate solutions to improve safety in the digital environment, and it will respect the fundamental rights that are enshrined in the UN Convention on the Rights of the Child [46]. It brings together leaders from social organizations, governments, and businesses as well as researchers to identify strategies and develop frameworks and best practices to evolve policies that can best support children.

On June 9, 2021, the French Supervisory Authority ("CNIL")[47] published recommendations to help strengthen the protection of minors online. The CNIL's eight recommendations aimed at enhancing the protection of minors online are as follows:

- Regulate the ability of minors to act online.
- Encourage minors to exercise their rights.
- Support parents in digital education.
- Seek the consent of a parent for minors under the age of 15.
- Promote parental tools that respect the privacy and interests of the minor.
- Adapt terms and disclosures and reinforce the rights of minors by design.
- Verify the age of minors and obtain parental consent while respecting privacy.
- Provide specific safeguards to protect the interests of minors.

In **Ireland,** the Fundamentals for a Child-Oriented Approach to Data Processing (the Fundamentals) [48] was launched in 2021 and have been drawn up by the Irish Data Protection Commission (DPC). The Fundamentals aim to provide guidance for organizations handling children's data, outlining the key principles derived from the GDPR's overarching obligations. These principles serve as a framework that the DPC expects such organizations to follow diligently. In line with these guidelines [49], online service providers are required to identify their users and implement specific data protection measures for services designed for or likely to be accessed by children.

Australia [50] released the Enhancing Online Safety for Children Act in 2015 that stated that if content was deemed to be cyber-bullying targeting children, it was required to be taken down. A children's e-safety commissioner is appointed to administer a complaints system for cyber-bullying material targeted at an Australian child. The commissioner is responsible for:

- Promoting online safety for children
- Coordinating activities of Commonwealth Departments, authorities and agencies relating to online safety for children
- Administering the online content scheme that was previously administered by the Australian Communications and Media Authority

An updated version of the Act, the Online Safety Act [51] was released in 2021. The regulation around children was not updated, but the act was expanded to included cyberbullying of adults. In September 2023, the eSafety Commissioner of Australia has released a statement that mentions that search engines like Google, Bing, Yahoo and DuckDuckGo will have to take steps to reduce the risk of child abuse and similar material being returned in search results. The new regulation comes under the 'Search Engine Code' [52].

To counter the concerns about excessive usage of digital spaces by children, **South Korea** has enacted a legislation to prevent children from playing online games that require a resident registration number between midnight and 6 am without parental consent. According to the 2016 Smartphone and Internet Addiction Survey conducted by the Korean Government, 1.2% of children aged 3 to 9 and 3.5% of teenagers were identified as high-risk individuals for smartphone or internet addiction. It was observed that children and teenagers with addicted parents faced a significantly higher risk of addiction themselves, with rates standing at 23.5% and 36.0% respectively. To address this issue, the Korea Youth Counselling and Welfare Institute offered a range of prevention and counseling services for young individuals dealing with depression, anxiety, adjustment difficulties, and family conflicts. Counseling is provided on an individual basis, in group settings, over the phone, and even at home for those who have isolated themselves from real-world social interactions. In severe cases, the National Center for Youth Internet Addiction Treatment organizes internet abstinence rehabilitation camps, providing intensive 12-day programs that involve outdoor sports and activities as part of the therapeutic approach[15].

Many guidelines have been put into place to help protect children's digital safety in **Canada,** while a concrete bill setting rules to protect children's digital safety is still missing. Protect Kids Online[53] in Canada is a platform with information about the ever-changing online interests of young people, the potential risks they face and proactive strategies to help keep your child/adolescent safe while online. During Covid-19 the Public Health Department of Canada specifically released guidelines[54] on children's safety online emphasizing the key priorities and recommendations on how to mitigate children's exposure to online risks and promote positive online experiences for children.

Finally, the **United States** is deliberating changes to the Children's Online Privacy Protection Rule (COPPA)[55]. Since 1998, COPPA has imposed specific requirements on operators of websites or online services aimed at children under 13 years of age, as well as on operators of other websites or online services that are aware they are collecting personal information online from a child under 13 years of age. The proposed changes involve updates[56] to the Children's Online Privacy Protection Act and separate legislative proposals introducing targeted privacy protections for teenagers and children. One possibility being discussed is the creation of a COPPA 2.0 that would raise the age limit of COPPA. Several states, including Minnesota and Nevada, are introducing legislation modeled after the California Age-Appropriate Design Code Act, effective from July 1, 2024. California passed the Age-Appropriate Design Code Act (A.B. 2273) [57] on August 30, 2022. This legislation compels online platforms to proactively evaluate the privacy and safety of children in the design of any digital product or service they offer. States like Maryland, New Mexico, and Oregon are following suit. Other states are concentrating on parental supervision for children's online access. Utah implemented a law requiring social media companies to grant parents or guardians access to the content and interactions of accounts held by Utah residents under 18 years of age. Additionally, Arkansas passed legislation prohibiting minors under 18 from using social media platforms without parental consent. The California Age-Appropriate Design Code Act is currently facing a legal challenge from the technology trade association NetChoice, which alleges that the legislation forces companies to act as internet speech censors. Meanwhile, advocates have expressed concerns, particularly regarding surveillance, related to the legislation in Arkansas and Utah.

7

DCO MEMBER STATES: PRESENT INITIATIVES AND **PROSPECTS FOR ENHANCEMENT**

DCO MEMBER STATES: PRESENT INITIATIVES AND PROSPECTS FOR ENHANCEMENT

Aligned with the global trend, the DCO Member States have introduced several initiatives for advancing children's digital rights and protecting their online safety. This section delves into the landscape of efforts and opportunities within the DCO Member States aimed at advancing the protection of children's digital rights and cultivating safer digital environments. With a focus on current initiatives and potential avenues for improvement, this section aims to provide insight into the actions undertaken by various DCO Member States to address the multifaceted challenges surrounding children's online safety and well-being. The section also outlines, in a non-exhaustive way, certain gaps and opportunities that have been identified in various studies on how each Member State can improve on their efforts towards enhancing children's online safety. By examining both existing endeavors and emerging opportunities, this exploration seeks to offer an understanding of the progress made and the pathways forward in ensuring that children can navigate the digital world securely and responsibly within the DCO Member States.

Member States	Initiatives
Bahrain	Telecommunications Regulatory Authority offers resources for child online protection through its Safe Surf initiative
Bangladesh	Cyber Security Strategy 2021-2025, addressing concerns about risks and threats faced by young people
Cyprus	Cyprus Safer Internet Centre (SIC) - CyberSafety, supported by European funding through the Better Internet for Kids (BIK) project
Djibouti	Initiatives and policies in this field can still be developed to further enhance children's safety online
The Gambia	Data Protection and Privacy Policy, with specific provisions regarding the protection of children
Ghana	Cybersecurity Act 2020 (Act 1038) criminalizes acts against children
Greece	Better Internet for Kids – Greece
Jordan	New Child Rights Bill
Kuwait	Data Privacy Protection Regulation 2021
Morocco	E-Himaya, a nationwide platform designed to inform and raise awareness among children

Nigeria	National Child Online Protection Policy and Strategy
Oman	Child Protection Committees and the Child Law of 2014
Pakistan	Prevention of Electronic Crimes Act
Qatar	Center dedicated to combating cybercrime
Rwanda	National Cybersecurity Authority and Data Protection Law
Saudi Arabia	Saudi Vision 2030 has spurred the development of e-learning initiatives catering to various education levels, from primary to tertiary.

In **Bahrain**, the Telecommunications Regulatory Authority offers resources for child online protection through its Safe Surf initiative [58]. They have released a comprehensive report on the state of internet safety and conduct lectures in schools to educate parents and teachers about online safety challenges faced by children.

Legislation in Bahrain [59] can further be enhanced to safeguard children online, particularly in areas such as online 'luring' (grooming) and the production and collection of indecent images of children.

Bangladesh has launched its Cyber Security Strategy 2021-2025 [60], addressing concerns about risks and threats faced by young people. While this document outlines some actions and areas for improvement, there is an opportunity to include specific details regarding concrete measures for children's online safety.

Going forward, particularly for Bangladesh [61], but potentially applicable to all DCO Member States, there is a need for a comprehensive assessment of the entire legal framework concerning technology and security issues.

Cyprus operates the Cyprus Safer Internet Centre (SIC) [62] - CyberSafety, supported by European funding through the Better Internet for Kids (BIK) project. The center is dedicated to enhancing efforts for the safe and creative use of the internet in Cyprus. With a focus on emerging internet technologies at both national and European levels, the center fosters collaboration among national stakeholders to cultivate a cybersecurity culture. Additionally, it has spearheaded the development and promotion of the National Strategy for Better Internet for Kids in Cyprus.

For Cyprus, the Better Internet for Kids strategy [63] emphasizes the need to involve and listen to children in aligning and defining public policies, considering they are the ones directly affected by these policies.

Despite **Djibouti's** recognized progress in improving children's rights, as acknowledged by the United Nations [64], there is further opportunity to design specific initiatives for the protection of children's digital rights and their protection online. Djibouti's efforts in enhancing child protection should continue and extend to the online world. There is currently a legislative gap in this area. The existing penal code [65] punishes crimes against minors of a sexual or abusive nature but it falls short of addressing the challenges posed in the online world. There is an opportunity to enhance the legislation needs to include both offline, and online abuses.

In 2019, **The Gambia** drafted the Data Protection and Privacy Policy (the Policy) [66], having specific provisions regarding the protection of children. The draft policy envisions creation of a National Supervisory Authority ('Supervisory Authority') appropriately empowered to oversee, monitor and enforce compliance and safeguarding of the data protection and privacy rights of individuals. The authority's mandate would include, among other things, the protection of privacy and data rights of children and other vulnerable individuals. There is an opportunity where The Gambia can focus on reforming its cybercrime laws. Given that children are especially vulnerable to this type of criminal activity, they stand to greatly benefit from a strong legal framework [67]. In fact, Gambia has laws related to cybercrime and online activities, although are not specifically aimed at children.

Ghana has made remarkable strides in cybersecurity. Ghana's readiness in cybersecurity has significantly improved, rising from a score of 32.60% in 2017 to 86.6% as of 2020 according to the ITU's Global Cybersecurity Index [68]. In Ghana, the Cybersecurity Act 2020 (Act 1038) [69] criminalizes child online abuses, including the production, viewing, and distribution of child sexual abuse materials, online grooming of children, cyberstalking of a child, and sextortion. Upon conviction, the Act penalizes these offenses with sentences of up to 25 years. Protecting children on the internet is one of the mandates of the Cyber Security Authority, established under Section 2 of the Cybersecurity Act, 2020 (Act 1038), to regulate cybersecurity activities and lead Ghana's cybersecurity development, among other related functions.

Going forward, Ghana could improve awareness, conducting research on child online protection, bolstering the criminal justice response to child online safety matters, which includes prosecuting offenders, and providing support services for victims, among other initiatives [70].

Similar to Cyprus within the framework of the European Union, **Greece** has undertaken numerous initiatives to promote the safety of children in the digital world. Under the umbrella of the Better Internet for Kids [71] program, in addition to awareness-raising actions, legislative initiatives in this area have been developed.

In 2022, **Jordan's** parliament, with support from UNICEF, enacted a new Child Rights Bill [72] to enhance protections for all children in the country, preventing economic exploitation and child labor while improving access to comprehensive child protection services including education, health, and legal aid. Additionally, Jordan has been a trailblazer, participating in a groundbreaking Safe to Learn Diagnostic Study [73]. Launched in 2021 by the Ministry of Education of Jordan, UNICEF, and Safe to Learn, this study [74], funded by the United Kingdom Foreign, Commonwealth, and Development Office, provides vital insights into accomplishments and remaining challenges within each component of the Call to Action. It establishes a baseline for tracking Jordan's progress nationally, regionally, and at the school level. The study delves into online safety for children and the challenges associated with their digital presence.

For Jordan, after recently ratifying the Personal Data Protection Law [75], a notable opportunity for improvement revolves around its implementation and creation of comprehensive supporting legal instruments to operationalize data protection [76]. Addressing this gap will have implications for the safeguarding of children's information as well. These supporting instruments could encompass precise guidelines and regulations on the collection, processing, and storage of personal data, along with stringent penalties for any breaches of these regulations. The Jordanian Personal Data Protection Law No. 24 of 2023 has officially been ratified and shall come into force six months from the date of its publication (17 September 2023) in the official gazette (i.e. enforceable starting 17 March 2024).

As previously mentioned, **Kuwait** released the Data Privacy Protection Regulation [77] in 2021, outlining detailed guidelines for data collection, storage, processing, and transfer, which includes specific provisions regarding information of individuals under 18 years of age.

In one of the recent studies [78] conducted in **Kuwait** regarding the use of smart devices by children, it was found that the prevalence of smart device usage among children aged five years or younger is high, despite parents' awareness of the potential harm it may cause. The study highlighted the need for campaigns to enhance understanding of the effects of smart devices on children and promote alternative activities that encourage children's engagement with parents and peers. Additionally, the study emphasized the importance of educating professionals working in fields involving interactions with parents and children, such as family doctors, pediatricians, teachers, and nannies. There is an opportunity for Kuwait develop specific laws focused solely on children's online protection.

The laws No. 09-08 [79] and Decree No. 2-09-165 [80], which govern the processing of personal data and individual protection, respectively, were passed by **Morocco** in 2009. These laws are collectively known as the DP Law. Notably innovative for its time, the legislation established the Commission Nationale de Protection des Données Personnelles (CNDP) [81] as an independent data regulator. Personal data is noted in the law as any information regardless of its nature and format, relating to an identified or identifiable person, which indicates applicability of the active law on children. In 2021, Morocco's Digital Development Agency (ADD) introduced E-Himaya [82], a nationwide platform designed to inform and raise awareness among children, young people, and parents about digital culture and responsible internet usage. E-Himaya offers assistance, awareness programs, and educational guides to help ICT users navigate the virtual world safely. The platform provides downloadable educational and entertaining videos, aiding children and young individuals in maximizing the advantages of secure ICT usage while encouraging responsible online behavior.

In a recent study [83] conducted in **Morocco,** digital security emerged as a vital tool for ensuring online privacy. However, a staggering 78% of Moroccan parents surveyed felt inadequately informed about protecting their children from online threats. Just over half of them believed they could respond effectively if their children fell victim to cyberbullying. Therefore, raising awareness about the dangers and implementing effective strategies to enable parents to discuss these issues with their children is likely to be a crucial focus in Morocco, and indeed, a global challenge.

In 2023, **Nigeria** approved the National Child Online Protection Policy and Strategy to protect children from harmful online materials. This strategy complements the Child Rights Act of 2003[84], which includes provisions for protecting and ensuring the safety of online content in other legislations. According to the International Telecommunication Union, in Nigeria, more than one billion children were online, especially during COVID-19, when most of them were out of schools were shut down and then switched to virtual learning. Data protection was governed by the Nigeria Data Protection Regulation, 2019 ("NDPR") [85], which was enforced up to 2022 by the country's ICT body, the National Information Technology Development Agency ("NITDA"). The president of Nigeria gave his approval for the Nigeria Data Protection Bureau ("NDPB") to be established in February 2022. The primary focus of the NDPB's work is privacy and data protection. Among other things, this includes building on the achievements of the NDPR and assisting in the creation and ratification of the first data protection act of parliament. The legitimacy of the NDPR has been called into question, with the main defense being that it was issued by a regulator, NITDA, rather than by the legislature. Later in the year, the NDPB went into existence and is currently a data protection authority. This legislation has provisions related to child's personal data.

One of the gaps identified in studies [86] conducted on the prevalence of online risks for children is the need to conduct further studies on child online risks in **Nigeria** to evaluate the extent of child online abuses. This need identified for Nigeria is applicable globally.

Oman's legal framework for child protection is robust [87], with Child Protection Committees (CPCs) established in all 11 governorates to prevent and address child abuse. The Child Law of 2014[88], along with the 2019 executive regulations, prohibits violence against children in all settings, including schools. This law mandates the reporting of all child abuse incidents and facilitates the swift removal of children from violent situations. It has been noted that a significant number of children and young people still continue to experience violence in their schools, communities, and families despite the legal framework in place. In 2021 alone, CPCs received reports [87] of 1,507 cases of child abuse, highlighting the ongoing challenges in ensuring the safety and well-being of children in Oman.

Going forward, Oman could develop a comprehensive and cross-cutting strategy dedicated to the protection of children and their online safety.

The Prevention of Electronic Crimes Act, 2016[89], was introduced to combat cybercrimes and unauthorized activities related to information systems in **Pakistan.** The Act applies to all Pakistani citizens, regardless of their location, and extends to anyone present in Pakistan at the time. Furthermore, it also encompasses acts committed outside Pakistan if they qualify as offenses under this legislation and impact individuals, property, information systems, or data within Pakistan.

The need for Pakistan to develop a national initiative [90] aimed at creating a safer internet environment for children and young people has been recognized by different stakeholder groups, including the government. Hence, the involvement of experts and international organizations in the discussions regarding these issues has recently become a notable aspect of Pakistan's efforts towards protecting children online.

Qatar has spearheaded several initiatives to safeguard children in the digital realm. Among these efforts is the establishment of a center [91] dedicated to combating cybercrime, the enhancement of legislation pertaining to such crimes, and the launch of a safe space website [92]. This platform is designed to educate children and adolescents about fundamental rules for preserving their safety and privacy while navigating the internet.

Qatar could further enhance[93] adequate reporting mechanisms to strengthen children's safety in the digital world.

The National Cybersecurity Authority ("NCSA") is the main regulator and enforcer of data protection in **Rwanda,** as per Law No. 058/2021 of 13 October 2021 [94] on the protection of personal data and privacy ("Rwanda DP Act"). The NCSA established its Data Protection Office on 31 March 2022. Its main functions are to protect personal data and ensure the privacy of individuals, as stipulated by the Rwanda DP Act, to provide opinions on personal data processing issues, to educate the data subject, the data controller, the data processor and third parties on their rights and duties, to maintain a register of data controllers and data processors, to handle complaints and appeals related to personal data processing, to give guidance on data protection and privacy matters, and to work with other authorities, organizations or entities involved in data protection and privacy. This legislation includes provisions related to child's personal data. Additionally, 5Rights, in partnership with the University of East London, the Government of Rwanda, and the University of Rwanda, created a Child Online Protection Policy [95] and Five-Year Implementation Plan for Rwanda [96]. The Government of Rwanda's cabinet officially approved the policy in June 2019. On April 28, 2022, the National Cyber Security Authority (NCSA) released a guide detailing how data protection and privacy laws safeguard children's data. The guide specifically highlights Article 9 of Law No. 058/2021 dated October 13, 2021, pertaining to the Protection of Personal Data and Privacy (the Data Protection Law), focusing on the protection of children's personal data. According to the guide, key points from Article 9 of the Data Protection Law include:

- Children's personal data includes any information belonging to individuals under the age of 16.
- Processing children's personal data requires obtaining consent from a person with parental responsibility for the child.
- Consent obtained on behalf of the child is valid only if it serves the child's best interests.
- Consent is not necessary if the processing is essential for safeguarding the child's vital interests.

One aspect highlighted as a potential area for improvement in Rwanda [95] concerns the responsibility of the industry to ensure that children are protected online. This includes the development of procedures and special considerations undertaken by the industry to guarantee child safety and uphold children's rights as they expand their online services into Rwanda.

In **Saudi Arabia**, one of the central tenets of Saudi Vision 2030 [97] revolves around the expansion of online learning platforms and digital resources. These platforms offer a multitude of advantages, including flexible learning schedules, access to diverse educational materials, and opportunities for self-paced learning. For instance, the HM the King Abdulaziz and his Companions Foundation for Giftedness and Creativity (Mawhiba) has introduced several online programs aimed at nurturing gifted students nationwide. Saudi Vision 2030 has spurred the development of e-learning initiatives catering to various education levels, from primary to tertiary. While the integration of the Internet into education brings numerous benefits, it also poses challenges. Promoting digital literacy is essential to ensure that students and educators can fully utilize online resources. Ofcom's recent study [98] focusing on Internet users aged 9 to 15 in Saudi Arabia highlighted the substantial presence of young individuals in digital domains. The report accentuates that a significant portion of children in this age group actively engage in online activities, exploring the digital landscape and its varied offerings. Particularly noteworthy is the finding that a substantial percentage of 9 to 15-year-olds in Saudi Arabia have access to the Internet through a range of devices, including smartphones, tablets, and computers. Acknowledging this reality, Saudi Arabia's National Cybersecurity Authority and UNICEF entered into an initial agreement to collaborate on child protection in cyberspace in 2022.

Despite the significance of Saudi Vision 2030 and its broad scope, there remains room for enhancing and advancing national policies that prioritize cybersecurity, particularly concerning the online safety of youth. Given the unique aspects of child protection, it is crucial for the government to incorporate cybersecurity measures and guidelines into comprehensive digital education and child protection policies. This integration will ensure that cybersecurity awareness and practices are seamlessly woven into the nation's digital agenda.

To conclude, governments, policymakers and other stakeholders around the world are actively working to address the unique challenges children face online. This ranges from the adoption of comprehensive data protection laws to the implementation of age-appropriate content regulations and the promotion of digital literacy programs. While progress has been made, significant gaps and challenges remain, underscoring the need for continued collaboration, innovation, and vigilance to ensure that children can fully enjoy their digital rights while staying safe and empowered in the online world.

8

POLICY RECOMMENDATIONS: HOW CAN WE MAKE THE **DIGITAL SPACE SAFER FOR CHILDREN?**

POLICY RECOMMENDATIONS: HOW CAN WE MAKE THE DIGITAL SPACE SAFER FOR CHILDREN?

Technology holds the promise to revolutionize education and equip students for an ever-evolving future. Yet, the potential risks to children are only beginning to surface. Establishing a policy and regulatory framework that centers on developing a comprehensive understanding of the advantages and threats posed by emerging technologies and safeguarding children where knowledge is limited is not an alarmist approach but a prudent and responsible course of action.

We began our paper by emphasizing the importance and necessity of strengthening protection for children in the online world. We then identified the main challenges to children's online safety and the role that diverse stakeholders can play in alleviating the challenges. We then discussed various best practice initiatives that have been taken globally, and across the DCO Member States to safeguard children online, as well as the opportunities for the DCO Member States for improvement.

Following that, and based on our primary and secondary reach through extensive benchmarking, and discussion with global experts at the DCO Digital Space Accelerator roundtables in Riyadh, Cape Town and Geneva, we present now present our policy recommendations that aim to create a safer digital space for children. To make the digital space safer for children the following actions are could be undertaken by DCO Member States, and beyond.

a. Refining existing laws and policies

The multitude and diversity of laws and regulations among DCO Member States makes a singular analysis challenging concerning refining existing policies. Consequently, while reshaping any the existing policies, laws or regulations concerning children's online safety, it is imperative to involve the key stakeholders mentioned throughout the document. These stakeholders include governments (policymakers and legislators), parents and guardians, children (paying special attention to children with vulnerabilities), educators and schools, industry, health care and social services, non-governmental organizations, and agencies, as well as law enforcement agencies. The identified stakeholders should be active participants in the process of ensuring children's online protection and build a safer and more secure digital environment. This was one of the main conclusions drawn from the roundtables held in September 2023 in Riyadh, in November 2023 in Cape Town, and in December 2023 in Geneva.

Furthermore, a **comprehensive assessment** of the DCO Member States' **entire legal framework** affecting technology and online security is crucial, with a special focus on protecting children in the digital world. This assessment should include the crucial intervention of policymakers and legislators, as well as other stakeholders including children and youth, and should support the choices made based on scientific evidence. The dispersion and autonomization of legal statutes pose a challenge that needs to be addressed. Mapping the key issues common to DCO Member States, and comparing them with each country's legal framework is a preliminary step. It is recommended to conduct a prior benchmarking of best practices, review existing child protection laws including personal data protection laws, and engaging in discussions about the implementation of new ones to create a comprehensive legal framework.

Specifically, there is a need to review the current legal framework to ensure the presence of all necessary legal powers enabling law enforcement and other relevant actors to protect individuals under the age of 18 from various online harms across all online platforms. One of the approaches could involve **Law Enforcement Training and Awareness**, providing law enforcement agencies with training and resources to effectively investigate and address online child protection issues. Financial resources need to be provided to empower law enforcement authorities to have the means to be able to enforce the laws and deal with and combat online/cyber-crimes against children. This aspect will encourage the full engagement of legal and the enforcement communities to contribute to the construction of a safer digital ecosystem for children.

It is recommended to focus on the **development of professional training programs and courses** specifically targeted for law enforcement communities and professionals to gain more knowledge about the risks and harms to which children and young people are exposed to and increase capabilities to detect and conduct investigations into internet related crimes against children.

Additionally, it is important to ensure that **any illegal act against a child in the physical world is also considered illegal online**. Online data protection and privacy regulations for children must be robust and effective. Furthermore, it is recommended to promote the adoption of systematic and **universal reporting and supporting mechanisms for instances of online child abuse.**

This evaluation should aim to **harmonize legal frameworks with established international standards,** laws, and conventions related to children's rights and cybersecurity. It should encourage **international collaboration through unified legal approaches.**

One of the most important aspects to consider will be promoting the **use of precise terminology in crafting legislation and policies** aimed at preventing and safeguarding against the sexual exploitation and abuse of children, particularly in areas such as online 'luring' (grooming) and the production and collection of indecent images of children.

This process should involve listening to and engaging with children to align and define public policies, considering they are the ones directly affected by these policies. **The lack of children and youth's involvement in shaping child protection policies and initiatives** has been identified as an important gap during our global roundtable discussions. Similarly, addressing the challenge where 'smart kids' that are able to bypass the online safety and protection measures was identified as crucial. To achieve this, any online child protections strategies should be developed keeping in view the ability of tech-savvy children to circumvent safety measures and access inappropriate content.

Criminalizing the harmful acts against the children committed in this digital domain is another area, as previously stated, that could be enhanced. Legislators and law enforcement agencies gave a vital role to play in this.

Additionally, enhancing international support is also relevant. **Fostering stronger international cooperation and rapid response mechanisms** to address online child protection issues should be a priority. Governments should lead efforts to operationalize this recommendation.

b. Developing new strategies, policies, and initiatives

i) Governments and Policymakers

1. Governments should partner with schools, educators, and the media to develop informational campaigns and resources, including guidelines for parents, teachers, and children, in collaboration with other stakeholders.

2. Policymakers should partner with experts in the fields of education and health to discuss and align on establishing a minimum age for having access to emerging technologies due to the severe impact emerging technologies can have on children. Additionally, individuals under 18 should require obtaining permission from their parent or legal guardian to use the services. This is one of the topics that was discussed in the roundtables, and is aligned with the UNESCO recommendations mentioned earlier.

3. As previously mentioned, some big Tech made decisions to stop allowing advertisers to target teens with interest-based ads. However, they continue to permit advertisers to target teens as a broad demographic group. To tackle the issue of targeted advertisements towards minors, the governments should:

- Consider, on priority, regulating how advertisers use children as target. Strict and effective regulations should be adopted to protect children from harmful advertisements e.g. by banning advertisers from targeting children under a certain age (13 years is recommended by UNESCO) with any form of targeted advertising, and penalties should be imposed for non-compliance.
- Mandate the advertisers to be transparent on their targeting practices and on the data they collect.
- Enforce stricter privacy regulations to protect children's personal information from being used for targeted advertising purposes without parental consent.
- Invest in public awareness campaigns to inform about the risks of targeted advertisement to children, and devise strategies to counter such measures.

- Collaborate closely with the technology companies that are responsible for these advertising approaches to jointly develop industry standards and best practices. This initiative was taken by the EU with TikTok (see earlier reference to the TikTok case) and the organization has since significantly improved the ways it targets children and processes their personal data.

4. Policymakers and legislators should partner with academia and especially experts in privacy and technology to promote the research, development, and implementation of privacy-conscious, interoperable, and user-friendly technologies that can limit contact and access to content unsuitable for children. These technologies should consider the child's age, maturity, and specific circumstances.

The studies conducted so far on the impact of technology on children are mostly inconclusive in several domains. As illustrated throughout this policy paper, the assessment of impact of technology, and prolonged online exposure on children's mental health, and cognitive and social development is not yet sufficiently robust. Public policies should be designed with the necessary scientific support and evidence to effectively address the issues at hand. It is advisable for the DCO Member States to promote in-depth research on the impacts of technologies on children, considering different age groups and developmental stages, counting on the impetus of governments and the expertise and knowledge of academia for this purpose.

This was one of the main recommendations made by the participants of our Geneva roundtable, where it was mentioned that scientific research and studies analyzing and evaluating the impact of technology on children have primarily focused on those aged 12 or older. Given that access to technology is occurring at increasingly younger ages, it is crucial to study the relationship between children under the age of 12 and technology. It is pertinent to encourage conducting focused studies involving younger children.

5. Policymakers should also embed policies and secure resources to enhance the Cyber capabilities across the DCO Member States to prevent, detect, protect, and mitigate against vulnerabilities and threats before they arise and be ready to respond to online/cyber-crimes against children.

6. Governments and policymakers should design and engage in meaningful awareness campaigns, and work on upskilling, and information sharing activities. As such, they should:

- Develop, coordinate, and implement national public awareness campaigns, with support of public institutions and social media to ensure a wider outreach, targeting, at least, children under 13 and children over 13 to acquire knowledge on the various online risks they may encounter and emphasizing the importance of a responsible behaviors.

- Develop, coordinate and implement national public awareness campaigns targeting children with vulnerabilities tailored to their specific needs to enhance the capabilities to identify and mitigate those risks to which children with vulnerabilities may be exposed to.

- Promote educational and training programs/initiatives to provide all stakeholders involved in child online protection activities with adequate knowledge and skills to deal with issues arising when children are online. These programs should be run on a periodic (e.g., bi-annual) basis.

- Encourage information sharing mechanisms at national and international levels to enhance relevant expertise, helpful practices, data on current and emerging threats, and meaningful insights to enable better decisions and facilitate more efficient prevention and effective response to any kind of threats to children in the digital space. Inspiration can be taken from the extensive collaboration that currently exists in the EU between the EU member states.

7. Governments, with support of the international organizations should also facilitate the development of bilateral and multilateral engagements with other countries or any other stakeholders to encourage the harmonization of laws, strategies and initiatives and implement a cross-border collaboration within and outside of DCO Member States to build a secure and global digital environment for children.

8. A Holistic National Child Online Safety Strategy

The need to develop holistic national strategies, for a concerted effort to protect children in the online world and the imperative involvement of all stakeholders were the key points highlighted in all three DCO roundtables (Riyadh, Cape Town, and Geneva).

Governments (policymakers and legislators) should partner with all the relevant key stakeholders identified in the sections above, to develop forward-looking and comprehensive **national child online safet**y strategy(s), which should include developing new laws, policies [99], and regulations, revising the current ones and devising robust enforcement/accountability mechanisms to protect children's safety and digital rights. This should be guided by the following cross-cutting principles:

- It is essential to have a holistic vision that incorporates families, governments, industry, and society, ensuring multi-sectoral action and accountability.
- Clearly define relevant roles and responsibilities, allocating sufficient human and financial resources for proposed actions.
- Ground the strategy in a thorough, evidence-based understanding of the digital environment while tailoring it to national/regional priorities.
- Show respect for and consistency with existing domestic laws and strategies, building upon the strengths of similar initiatives that are already in place. The child online safety strategy should be integrated into the broader governmental plans for economic and social development.
- Foster active participation of all stakeholders, including children and their families, addressing their needs and responsibilities, particularly focusing on vulnerable groups.
- Design the strategy in a way that it aligns with broader government/regional plans for economic and social development, including investment and resource mobilization for child online protection efforts.
- Utilize the most appropriate and robust policy instruments available to achieve objectives of the strategy.
- Provide guidance to empower and educate children, caregivers, and educators as digital citizens, emphasizing digital access, equity, and digital literacy.
- Contribute significantly to creating a trusted digital environment that ensures the safety of children on national, regional and global levels.

Why is it important to have a Child Online Protection Strategy?

- Due to the continuous increase of risks and vulnerabilities of children and young people in the cyberspace, we need to encourage the implementation of measures, initiatives, and solutions to support the achievement of a secure and safe digital environment for children and young people.
- Child Online Protection is a subject of valid international global interest, and it has been made a major priority of the global community's agenda in recent years.
- Dimensions such as safety, privacy, the impact of technologies, age of access, and the roles of parents and schools should be safeguarded.

Summary of a National/ Regional Child Online Protection Strategy

- Considering the growing significance of this topic, developing national Child Online Protection Strategy for DCO Member states is recommended.
- The purpose of this strategy will be to set the strategic direction and guide stakeholders towards the adoption of a common approach to deal with Child Online Protection issues, establishing both short and long-term objectives to:
  - Build a safer and more secure digital environment, tailored to children and young people's needs.
  - Create awareness among policymakers, industries, parents and educators as well as children and young people on the risks and threats they may encounter online.
  - Encourage the sharing of knowledge and experience

Governments should consider the following for development and implementation of the strategy:

- Co-create the strategy through a multi-stakeholder platform and task force, including representatives from all relevant stakeholders. This taskforce should be responsible for guiding the formulation, execution, and oversight of the child online safety strategy.
- Define clear, time-bound objectives and establish a transparent process for evaluating and tracking progress. Ensure the availability of essential human, technical, and financial resources to effectively implement the national child online safety strategy and its associated components.
- The key and fundamental step in enhancing safety and ensuring the success of the defined strategy is to create and implement the necessary regulations. Governments must obtain the necessary legislative approvals to achieve this goal. This could, for example, involve establishing safety entities such as the National Cyber Security Council. This organization should place particular emphasis on online safety for children.
- Technological solutions and tools to enhance children's online protection form a critical part of the strategy. Governments should encourage the adoption, promotion, and deployment of robust tools and mechanisms to mitigate risks, enhance safety, and promote responsible digital behavior. These tools and solutions include, content filtering and monitoring tools, parental control software, Privacy Enhancing Technologies (PETs) specially designed with children's privacy in mind, tools that can flag and identify cyberbullying, age-verification and safety features, digital literacy and educational tools, and last but not the least, law enforcement tools to investigate online crime against children. Integrating these tools into the strategy can enhance the overall safety of children in the digital age.

- The strategy should encourage the sharing of knowledge and experience among the relevant stakeholders to increase prevention and protection capabilities. A forum should be created for these stakeholders to meet on a bi-annual basis to discuss trends and developments and risk mitigation actions.
- Support targeted research projects, encouraging gathering of inputs from victims as well as from all stakeholders with an interest in child online protection and execution of in-depth analysis to monitor and analyze long-term consequences on child victims of online abuses or crimes.
- Ultimately, the strategy should empower children by providing them with guidance on how to navigate in the digital space and where to seek support. Rolling out digital literacy programs would be a main driver for achieving this goal.
- Through the process of developing policies, the relevant stakeholders should encourage the direct participation and review by children and young people to make sure it is relatable with their day-to-day lives and challenges making sure it addresses their needs.

ii) Schools and Educators

Schools and educational systems have made significant strides in adapting their programs and curricula to include digital skills and competencies. However, these efforts often fall short in providing practical training and solutions for online risks—what these risks entail, where they occur, how to respond, and how to prevent them.

Schools should encourage more online safety educational and awareness-raising initiatives providing all stakeholders with appropriate knowledge and capabilities for a safe and responsible use of the internet – especially children. Additionally, education systems frequently lack collaboration with parents and guardians to keep them informed about the latest threats. To address these gaps, online safety modules should be integrated into curricula. Schools and educational institutes should:

- Organize parental information sessions and conduct awareness campaigns focused on cyber threats and conduct cyber incident simulations to show the impacts of cyber attracts. Moreover, it is crucial for schools to offer digital literacy courses for educators, ensuring they stay updated on the latest technological developments and cyber-risk dynamics.
- Establish school support programs, providing resources and pedagogical tools, and offering training to teachers so that they can easily identify and respond to the online risks.

  This recommendation aligns with one of the suggestions put forward during the DCO's Riyadh roundtable.
- Create helplines to ensure children receive support and advise in case of any suspected or experienced illicit behaviors against children and their wellbeing.
- Promote children and young people's engagement on forums and/ or platforms for child online protection to provide them with adequate knowledge to manage online risks.
- Develop, coordinate, and promote activities and initiatives to raise awareness around privacy-related risks to foster children's consciousness on privacy and data protection issues as well as on good practices when engaging in online activities.
- Encourage and participate in the development of a broad digital literacy program that is age-appropriate and focuses on skills and competencies to ensure that children can fully benefit from the online environment while being aware on the wide-range of threats.

- Ensure that educators are well trained for preventative and responsive activities to online abuse, harms and/or crimes against children, thus enabling them to proactively help children, recognizing such illicit behaviors and providing specialized and long-term support and assistance to victims through both online and offline channels.
- Ensure educators and school administrators/professionals are well trained to identify and adequately respond to suspected or confirmed cases of illicit behaviors against children's online safety as well as to provide children with the required skills and knowledge on the positive and responsible forms of online behaviors.
- Execute awareness campaigns focusing on cyberbullying aimed at discouraging children from posting offensive information about someone, intentionally sharing privacy information, photos, or videos in an offensive way, sending threatening or insulting messages, spreading rumors and false information or any other cyberbullying-related behaviors.
- Provide children with vulnerabilities with the necessary tools, equipment, and adequate coaching to guarantee their secure inclusion within the digital environment.

For the operationalization of these recommendations, schools and educators, education policymakers, as well as parents and children, should be involved, as they would be the prime recipients of these measures.

It is important to note that schools and educators were identified in the surveys distributed amongst the roundtable participants as one of the most relevant stakeholders in the efforts to ensure online safety for children.

iii) Parents

Policymakers should partner with parents, and schools to provide educational materials and organize training sessions to empower parents with knowledge about the new technologies and platforms their children are accessing. These resources should cover online control mechanisms, the latest hardware and software features designed to protect young internet users, and effective ways to communicate with their children about online behavior and potential threats. Equipping parents with this understanding is pivotal for enhancing their ability to ensure their children's online safety.

The need to develop robust and meaningful tools for parent's upskilling was one of the aspects that was highlighted DCO's Riyadh roundtable.

Using these tools, and in their capacities, the parents should:

- Educate their children about online risks, safe internet usage, privacy settings, and the importance of responsible digital behavior. They should have open and ongoing communication about online experiences and safety concerns.
- Establish clear rules and guidelines for screen time, appropriate websites and apps, sharing personal information online, and interacting with strangers. They should use parental control tools and filters to enforce these boundaries.
- Regularly monitor children's online activities, including the social media accounts of young children, gaming interactions, and messaging platforms. For young children, they should supervise their online interactions, friends list, and content consumption to identify any potential risks or red flags.
- Encourage children to come to them with any online safety concerns or incidents of cyberbullying, harassment, or inappropriate content they encounter online.
- Be a positive role model for responsible digital behavior. They should show respect for privacy, avoid oversharing personal information, and demonstrate healthy online habits. They should engage in offline activities and family time to balance their children's online activities.

iv) Meaningful Collaboration and Partnerships with the Industry

Governments and regulators should partner with private sector organizations including technology players, connectivity and broadcasting service providers to establish meaningful collaboration on children's online safety protection. Especially:

- Governments should encourage the telecom service providers to create **child-friendly mobile packages** that limit children's exposure to harmful content. Given that children now have easier and widespread access to mobile phones with mobile data, it is important to design solutions that safeguard their safety. *This is in line with a recommendation made during the DCO roundtable in Cape Town where the participants emphasized the need for the governments to work with the technology firms and telecom service providers to create bespoke and safe products, packages and solutions for children.*

- Governments should collaborate with operators across the technology and telecom industry to establish mechanisms and procedures, especially using advanced technologies and shared platforms to prevent, detect, block, remove and most of all report illegal and exploitative contents that threaten children's online safety.

- Governments should encourage industry players to be transparent about how they secure products and services and contribute to minimizing online threats by anticipating, detecting, and removing harmful content and vulnerabilities before they occur.

- Policymakers and legislators should partner with the audiovisual industry and the media to adapt film and broadcasting rules and laws to the digital realm: leverage existing film and broadcasting laws and adapt them to the digital landscape to protect children in the online world.

  This was a recommendation discussed and presented at the Cape Town roundtable held in November 2023.

- Governments should mandate technology companies to adopt safety and security-by-design principles in the new products and services. There should be an enhanced adoption of proactive and preventative approaches that ensure user safety is embedded into the design, development and deployment of online services, platforms and products accessible to children. This is particularly relevant when adopting emerging technologies such as AI solutions.

- Governments should partner with academia and the private sector to support the development, adoption, and dissemination of **assessment tools** to verify how well safety and security-by-design practices are incorporated throughout the product development lifecycle and how to further improve them to support the building of a safer digital environment for children.

- Policymakers and regulators (especially the data protection authorities, if they exist) should work with the industry and domain experts for the continuous execution of risk and impact assessments investigating the nature, scope, context, lawful basis, associated risks and impacts of processing children's personal data. This will allow for proper identification and minimization of risks through appropriate mitigation strategies as well as technical and organizational measures. Mechanisms should be in place to report these risk assessments to the authorities and flag any high risks identified.

- Governments should encourage industry operators to embed the protection of children and young people's personal data into the development and deployment of new products, tools, platforms, and services.

- Governments should emphasize on the industry players to involve children during the design and planning phases of new products and services, to provide children-friendly tools that ensure their safety and security.
- Governments and international organizations should partner with specialized domain experts and academia to create awareness programs and initiatives for industry on how to make the internet a safer and more secure environment for children and young people. Thereby, enabling them to recognize risks and vulnerabilities of their products and services and adopting adequate prevention and protection measures.

The DCO member states should strive to play a leading role in creating a safe and secure online experience for children. This should be undertaken in collaboration with service providers that target children with their services.

CONCLUSION

DCO's policy paper on 'Safe Digital Space for Children' underscores the critical importance of addressing key safety challenges faced by children in the online world. Through an in-depth analysis of global best practices, policy measures adopted by various countries, including the DCO's Member States, and insights from experts and stakeholders, the paper highlights the urgent need for action towards protecting children's wellbeing and safety in the digital world. The need for comprehensive and holistic national child online protection strategies came out as key recommendation of the paper.

Throughout the paper, we have sought to identify the reasons why children are particularly vulnerable in the digital world. We began by recognizing children as increasingly early users and natives in the use of new technologies were exposed to significant risks. We considered it essential to understand the main challenges arising in the use of new technologies by minors through data derived from extensive secondary research.

The insights gained were enriched by the discussions held in the DCO roundtables conducted in Riyadh (September'23), Cape Town (November'23), and Geneva (December'23). This was further supplemented with the results of surveys distributed to participants of the roundtables as well as discussion with the DCO Member State representatives.

The paper emphasizes the pivotal roles of governments, schools and educators, parents, industry, and collaborative efforts among stakeholders in ensuring children's online safety. It acknowledges the progress made in promoting children's digital rights and online safety measures globally while recognizing the ongoing challenges and evolving nature of online threats.

Throughout the research, we analyzed key trends and the most relevant initiatives aiming to protect children in the online world. This included recommendations from international organizations and various countries across different regions, with a particular focus on the realities of the DCO Member states.

As an outcome from the above, a set of policy recommendations have been outlined focused on enhancing the children's online safety. The recommendations are aimed at enhancing current policies and regulations, fostering digital literacy among children and parents, implementing effective parental controls, and monitoring tools, enhancing law enforcement capabilities to combat online crimes against children, and promoting responsible digital citizenship.

As a key recommendation, the paper advocates for the creation of robust national child online protection strategies that encompass policy frameworks, educational initiatives, technological solutions, and collaborative partnerships. These strategies should prioritize children's rights, safety, and well-being in the digital age, integrating best practices and innovative approaches from around the world.

By implementing these recommendations and fostering meaningful collaboration among stakeholders, DCO aims to create a safer and more inclusive digital environment for children, where their rights are protected, and they can explore and thrive in the online world with confidence and security, enabling digital prosperity for all.

REFERENCES

1 United Nations Convention on the Rights of the Child (UNCRC)'s

2 IBM Cost of a Data Breach 2023 Report

3 United Nations Capital Development Fund (UNCDF)

4 Share of children with internet access in their household in 2020, by region, Statista

5 Children in a Digital World, UNICEF

6 The State of the World's Children 2017, UNICEF

7 Education: From COVID-19 school closures to recovery, UNESCO

8 Digital misinformation / disinformation and children, UNICEF

9 Impacts of technology use on children: exploring literature on the brain, cognition and well-being, OECD, 2019

10 Impact of computer use on children's vision, N. Kozeis, 2009

11 Educating 21st Century Children, OECD, 2019

12 Vulnerable Children in a Digital World, Internet matters

13 Addictive Features of Social Media/Messenger Platforms and Freemium Games against the Background of Psychological and Economic Theories, Christian Montag, Bernd Lachmann, Marc Herrlich, and Katharina Zweig, 2019

14 On Social Media Design, (Online-)Time Well-spent and Addictive Behaviors in the Age of Surveillance Capitalism, Christian Montag & Jon D. Elhai, 2023

15 Children & Young People's Mental Health in the Digital Age, OECD

16 Social Media and Depressive Symptoms in Childhood and Adolescence: A Systematic Review, Niall McCrae, Sheryl Gettings & Edward Purssell, 2017

17 Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time, Jean M. Twenge, Thomas E. Joiner, Megan Rogers, and Gabrielle N. Martin, 2017

18 What do we know about children and technology?, OECD

19 UNESCO Strategy on technological innovation in education (2021-2025)

20 Guidance for generative AI in education and research, UNESCO, 2023

21 Immersive virtual reality interferes with default head–trunk coordination strategies in young children, Jenifer Miehlbradt, Luigi F. Cuturi, Silvia Zanchi, Monica Gori & Silvestro Micera, 2021

22 Could virtual reality applications pose real risks to children and adolescents? A systematic review of ethical issues and concerns, Polyxeni Kaimara, Andreas Oikonomou & Ioannis Deliyannis, 2022

23 New technologies and 21st century children - Recent trends and outcomes, OECD

REFERENCES

24 Online aggressor/targets, aggressors, and targets: a comparison of associated youth characteristics, Michele L. Ybarra, Kimberly J. Mitchell, 2004

25 The state of online harassment, Pew Research Center, 2021

26 Cyberbullying Among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures, Chengyan Zhu, Shiqing Huang, Richard Evans, Wei Zhang, 2021

27 Safer Internet Day: UNICEF calls for concerted action to prevent bullying and harassment for the over 70 per cent of young people online worldwide, UNICEF

28 Almost 60 percent of parents with children aged 14 to 18 reported them being bullied, Comparithec

29 Understanding the Rise of Twitter-Based Cyberbullying Due to COVID-19 through Comprehensive Statistical Evaluation, Sayar Karmakar, and Sanchari Das, 2021

30 Transparency reporting on child sexual exploitation and abuse online, OECD

31 Children's data and privacy online, LSE

32 Children's data and privacy online - Growing up in a digital age, Sonia Livingstone, Mariya Stoilova, Rishita Nandagiri, LSE, 2018

33 Child and Youth Safety Online, United Nations

34 A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+), European Union, 2022

35 Child Safety Online Global challenges and strategies, UNICEF

36 Online technology and very young children: Stakeholder responsibilities and children's rights, Andy Phippen

37 "Prevention Alone Is Not Enough:" Stakeholders' Perspectives About School-based Child Sexual Abuse (CSA) Prevention Programs and CSA Research in China, Mengyao Lu, Jane Barlow, Franziska Meinck, and Yumeng Wu, 2022

38 The Role of Parents in Digital Safekeeping and Advice-Giving, Amanda Lenhart, Mary Madden, Aaron Smith, Kristen Purcell and Kathryn Zickuhr, 2011

39 Children's Code, United Kingdom

40 Online Safety Bill, United Kingdom

41 The rights of children and young people on digital platforms, Swedish Authority for Privacy Protection

42 Code for Children's Rights, Sweden

43 UN Convention on the Rights of the Child, 1989

44 Paris Peace Forum

45 Children Online Protection Laboratory

REFERENCES

46 Convention on the Rights of the Child

47 French Supervisory Authority

48 Child-Oriented Approach to Data Processing

49 Approaches to children's data protection, 5Rights Foundation, 2022

50 Enhancing Online Safety for Children Act, Australia, 2015

51 Enhancing Online Safety for Children Act, Australia, 2021

52 'Search Engine Code'

53 Protect Kids Online, Canada

54 Public Health Department of Canada guidelines

55 Children's Online Privacy Protection Rule (COPPA), United States

56 Proposed changes to COPPA

57 The Age-Appropriate Design Code Act (A.B. 2273), California

58 Safe Surf initiative

59 TRA Bahrain Role on Internet Safety and Child Protection Online

60 Cyber Security Strategy 2021-2025, Bangladesh

61 Cyber Security Awareness in Bangladesh: An Overview of Challenges and Strategies, Bangladesh

62 Cyprus Safer Internet Centre

63 Better Internet for Kids strategy

64 United Nations recognition of Djibouti's improvements

65 Djibouti's penal code

66 Data Protection and Privacy Policy, Gambia

67 Reform of cybercrime legislation: the Gambia

68 ITU's Global Cybersecurity Index

69 Cybersecurity Act 2020, Ghana

70 Ghana initiatives

71 Better Internet for Kids

72 Child Rights Bill, Jordan

73 Safe to Learn Diagnostic Study

REFERENCES

74 Diagnostic Study of National Efforts to Reduce and Respond to Violence in Ministry of Education Schools in the Hashemite Kingdom of Jordan, 2020-2021

75 Personal Data Protection Law, Jordan

76 Protecting privacy: A government guide to safeguarding personal data

77 Data Privacy Protection Regulation, Kuwait

78 Prevalence of Use of Smart Devices in Children Aged Five Years or Less and Associated Factors in Kuwait

79 Laws No. 09-08, Morocco

80 Decree No. 2-09-165, Morocco

81 Commission Nationale de Protection des Données Personnelles (CNDP)

82 E-Himaya

83 84% of parents are worried about their child's online safety, but aren't taking the time to talk about it, Kaspersky

84 Child Rights Act of 2003, Nigeria

85 Nigeria Data Protection Regulation, 2019

86 An Assessment of Internet Use and Cyber-risk Prevalence among Students in Selected Nigerian Secondary Schools, Adeola O. Opesade Dr and Abiodun O. Adetona Mr, 2021

87 Protection of Children from Violence, UNICEF

88 Child Law of 2014

89 Prevention of Electronic Crimes Act, Pakistan, 2016

90 Pakistan national initiative aimed at creating a safer internet environment for children and young people

91 Doha Declaration

92 Safe space website, Qatar

93 Addressing violence against children: A case review in the state of Qatar, Abdulla Saeed Al-Mohannadi, Sanaa Al-Harahsheh, Sajeda Atari, Nadeem Jilani, Ghalya Al-Hail, Kennedy Sigodo, 2022

94 Law No. 058/2021 of 13 October 2021, Rwanda

95 Child Online Protection Policy, Rwanda

96 Child Online Protection in Rwanda, Professor Julia Davidson Baroness, Beeban Kidron, Kirsty Phillips, 5Rights Foundation

97 Saudi Vision 2030

REFERENCES

98 Investigating How Parental Perceptions of Cybersecurity Influence Children’s Safety in the Cyber World: A Case Study of Saudi Arabia, Tariq Saeed Mian and Eman M. Alatawi, 2023

99 Keeping children safe in the digital environment: The importance of protection and empowerment, International, Communications Union

Digital
Cooperation
Organization

Follow us on

@dcorg | www.dco.org