Fountain University Law Journal Vol. 2 No. 4, 2025

THE CHILD RIGHTS ACT IN NIGERIA AND ONLINE CHILD SAFETY

By

Zaynab Omotoyosi Shittu-Adenuga*
&
Ibrahim Owolabi**

Abstract

The Child Rights Act (CRA) of 2003 fails to address online child safety amidst the evolving digital landscape. Anchored on the United Nations Convention on the Rights of the Child (CRC) and the African Charter on the Rights and Welfare of the Child (ACRWC), the CRA provides a comprehensive framework for protecting children's rights to survival, development, and protection. However, the Act's lack of specific provisions addressing digital threats such as cyberbullying, online grooming, sexual exploitation, and data privacy violations highlights significant legislative gaps. Through a doctrinal research methodology, this study analyses primary legal sources, including the CRA, Cybercrimes Act of 2015, and international instruments, alongside secondary sources like scholarly articles and reports from organizations such as UNICEF. The findings reveal uneven domestication of the CRA across Nigeria's 36 states, weak enforcement mechanisms, limited digital literacy, and inadequate institutional coordination as key barriers to ensuring online child safety. A comparative analysis with international best practices, such as the UK's Online Safety Act, the EU's General Data Protection Regulation (GDPR), and the US's Children's Online Privacy Protection Act (COPPA), underscores Nigeria's lag in adopting child-specific digital protection measures. The study proposes legislative reforms, including the passage of the Child Online Access Protection Bill, nationwide CRA domestication, enhanced institutional capacities, and public awareness campaigns to promote digital literacy. It also recommends integrating digital safety education into school curricula and fostering collaboration with international bodies to combat transnational online child exploitation. This research contributes to the discourse on child protection by advocating for a dynamic, technology-driven legal framework to safeguard Nigerian children in the digital age, while identifying areas for further studies, such as the role of artificial intelligence, gender dimensions, and child participation in online safety policy-making.

Keywords: **Childs Right, Online Safety, Reform, Sexual Exploitation.**

1.0 INTRODUCTION

Protecting and promoting the rights of children has become a cornerstone of modern legal systems, reflecting a global commitment to ensuring their well-being and development.[1]Given

*Lecturer, Department of Private and Business Law, College of Law, Fountain University, Osogbo, Osun State
*500 Level Law Students, College of Law, Fountain University, Osogbo, Osun State

that children are among the most vulnerable members of society, it is essential to establish intentional legal frameworks and procedures to ensure their protection and well-being.[2] International standards for protecting children's rights are set out in the 1989 United Nations Convention on the Rights of the Child (CRC) and the 1990 African Charter on the Rights and Welfare of the Child (ACRWC). In a bid to align its national laws with these global and regional frameworks, Nigeria ratified both treaties and took a significant step in 2003 by enacting the Child Rights Act (CRA), thereby domesticating their provisions.[3]The Child Rights Act (CRA) was enacted to safeguard children's rights to participation, survival, development, and protection. It outlines a wide range of entitlements, including protection from abuse, neglect, and exploitation. However, Nigeria's federal structure poses challenges to its effective implementation, as enforcement is left to individual states. To date, the CRA has not been domesticated in all 36 states, leaving many children vulnerable to rights violations in parts of the country.[4]

While the CRA focuses primarily on traditional forms of abuse, modern challengesparticularly those linked to the internet and digital technologieshave introduced new dimensions to child protection. With the widespread use of digital platforms, children are increasingly exposed to risks such as cyberbullying, online grooming, sexual exploitation, and access to harmful content. Reports from organizations like UNICEF continue to highlight the growing prevalence of online abuse, underscoring the urgent need for legal frameworks to evolve in response to the realities of the digital age.[5]Nigeria's legal instruments on cybercrimesuch as the Cybercrime Act of 2015tend to focus broadly on cybersecurity, with limited attention to the specific vulnerabilities faced by children online. This gap is compounded by the absence of explicit, child-focused provisions in the Child Rights Act (CRA) to address online risks. As a result, the current legal framework falls short in responding to the evolving nature of child exploitation in digital environments.

Given these shortcomings, there is a pressing need to critically review the CRA to determine its adequacy in tackling modern challenges related to online child safety. This study aims to assess how effectively the CRA protects children from digital threatsand propose legal and policy reforms to strengthen child protection in Nigeria's digital era.[6]

---

[1]OAgbede, "Nigeria Legal and Practical Position" SSRN(2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3639563> accessed 22 December 2024.

[2] ibid.

[3]Steve Anya, "FG: 34 States have domesticated Child Rights Act" Thisdaylive(2022) <https://www.thisdaylive.com/index.php/2022/11/29/fg-34-states-have-domesticated-childs-rights-act/> accessed 22 December 2024.

[4] ibid.

[5]UNICEF, "Cyberbullying: What is it and how to stop it?" UNICEF, (2024) <https://www.unicef.org/end-violence/how-to-stop-cyberbullying> accessed 23 December 2024.

[6]Ibid

2.0 DEFINITION OF TERMS

2.1 Who is a Child? In Nigeria, the definition of a child is primarily derived from the Child Rights Act (CRA) of 2003,[7] which was enacted to domesticate the United Nations Convention on the Rights of the Child (UNCRC).[8] The CRA defines a child as any person under the age of 18 years and guarantees various rights, including the right to survival, development and protection from abuse, neglect and exploitation.[9] This definition aligns with international standards and underscores the recognition of individuals below this age as requiring special protection and care.

2.2 What are Child Rights: Child rights are the fundamental entitlements and protections afforded to every individual below the age of 18, grounded in the principle that children require special safeguards due to their vulnerability and developmental needs.[10] At their core, these rights recognize children as independent rights holders whose well-being, survival, development, and participation in society must be actively protected and promoted.

2.3 What is Online Child Safety?: Online child safety refers to the measures and protocols established to protect children from online threats, including exposure to harmful content, cyber bullying, sexual exploitation, and data privacy violations.[11]

3.0 CHILDS RIGHT ACTAND ONLINE CHILD SAFETY

The Child Rights Act (CRA) of 2003 is a landmark piece of legislation in Nigeria that brings together and codifies the rights of children, aligning the country's legal framework with international standards such as the United Nations Convention on the Rights of the Child (CRC) and the African Charter on the Rights and Welfare of the Child (ACRWC). Enacted as Act No. 26 of 2003, the CRA establishes a comprehensive foundation for safeguarding the rights, protection, and overall welfare of children across Nigeria.[12]The Child Rights Act (CRA) contains 278 sections and 11 schedules, covering a broad range of issues related to children's rights and welfare. It includes detailed provisions aimed at ensuring child safety in various contexts. Below are specific sections of the Act that focus on child protection, outlining their implications and the degree of safeguard they provide.

[7]Child Rights Act (CRA) 2003.
[8] United Nations Convention on the Rights of the Child (UNCRC) 1989.
[9] Section 277 Child Rights Act (CRA) 2003.
[10]Child Rights Act (CRA) 2003.
[11]AFalode. "Cybersecurity Policy in Nigeria: A Tool for National Security and Advancement." In Routledge Companion to Global Cyber-Security Strategy (2021) <https://www.researchgate.net/publication/344862459_Cybersecurity_Policy_in_Nigeria_A_Tool_for_National_Security_and_Advancementaccessed 23 December 2024.
[12] Ibid.

i. Protection from Abuse and Neglect

Section 11 of the CRA explicitly prohibits subjecting a child to any form of torture, inhuman or degrading treatment or punishment.[13] It states that every child is entitled to respect for the dignity of their person and, accordingly, no child shall be:

- Subjected to physical, mental, or emotional injury, abuse, neglect, or maltreatment, including sexual abuse;
- Subjected to torture, inhuman or degrading treatment or punishment;
- Subjected to attacks upon their honor or reputation; or
- Held in slavery or servitude, while in the care of a parent, legal guardian, or school authority.

This provision reflects the state's commitment to protecting children from all forms of abuse while promoting their overall development in a safe and nurturing environment. Although it does not explicitly address digital threats, its broad language can be interpreted to cover emerging forms of abuse, including cyberbullying, online grooming, and digital exploitation. This interpretive flexibility provides an opportunity for courts and child protection agencies to apply the provision to the evolving landscape of online risks facing children.

ii. Right to Privacy

Section 8 of the CRA guarantees every child's right to privacy, covering their family life, home, correspondence, telephone conversations, and telegraphic communications. However, this right is balanced with parental or legal guardian supervision to ensure that children's safety and well-being are always prioritized. In today's digital world, this provision also extends to safeguarding children against unauthorized access to their personal information online, highlighting the critical need for data protection and cyber safety.[14]

This right to dignity and privacy implicitly supports the protection of children's personal data and digital footprints, particularly in online spaces. It aligns with international instruments such as Article 16 of the CRC, which guarantees the child's right to privacy. However, digital-specific expressions such as protection from unauthorized data collection, online surveillance, and invasion of privacy via social media are not outlined. While the CRA acknowledges personal dignity, it fails to extend that into 21st-century realities of digital data and surveillance.[15]

iii. Protection from Exploitative Labor

[13] Section 11 Child Rights Act (CRA) 2003. Child's Right Act 2003.
[14] Ibid.
[15] AO Olatunji. "Digital Rights and the Nigerian Child: Revisiting the Child Rights Act in a Digital Age." African Human Rights Law Journal, (2020) 20(1) 59–78,https://www.ahrlj.up.ac.za/olatunji-ao](https://www.ahrlj.up.ac.za/olatunji-ao) accessed on 6th May, 2025.

Section 28 of the CRA addresses child labor by prohibiting the employment of children in any capacity, except when a child is engaged in light work on a family member's farm or household, as approved by the Minister. It also criminalizes the use of children for begging, hawking, prostitution, or any activity harmful to their well-being, education, or development. This provision seeks to eliminate exploitative labor practices and protect children from conditions that threaten their safety and future.[16]

However, in the digital realm, challenges like online child sexual exploitation (OCSE), including grooming, pornography, and traffickingare rapidly evolving. While the CRA criminalizes these abuses offline, it does not explicitly address their online counterparts, which have become more widespread due to increased internet access and unsupervised digital interactions. Though the Act offers strong protections against physical exploitation, its silence on digital forms leaves children vulnerable in cyberspace.[17]

iv. Duty of Care by Parents, Guardians, and Institutions

Section 14 of the Act places a legal responsibility on parents, guardians, and institutions to ensure the well-being and safety of children. This duty could extend to supervising children's digital activities and managing their access to internet-enabled devices. However, the Act does not include specific guidelines or digital safety frameworks for schools, cybercafés, or online content providers. While Section 14 is important in principle, it remains vague and difficult to enforce in the digital context without additional legislation or a comprehensive national framework on digital child safety.[18]

v. Penalty Provisions

The CRA also provides for penalties where violations occur, particularly in sections relating to sexual offences, abduction, or trafficking (Sections 31–34). However, there are no direct penalties or regulatory oversight concerning cybercrimes targeting children, such as sextortion or cyberbullying.

Conclusively, while the Child Rights Act (2003) provides a broad legal basis for the protection of children from harm, it does not explicitly contemplate online safety, which is a growing area of concern in Nigeria and globally. Provisions related to privacy, exploitation, dignity, and abuse may be interpreted to include digital harms, but the absence of specificity weakens enforcement and legal clarity. This creates a compelling need for legislative reform or supplementary

[16] ibid

[17]KO Odeku. "Child Sexual Abuse in Nigeria: Current Legal and Institutional Frameworks." Journal of Social Sciences,(2014)41(1)85–94, https://doi.org/10.1080/09718923.2014.11893336](https://doi.org/10.1080/09718923.2014.11893336 accessed on 6th May, 2025.

[18]CO Eze "Reforming Child Online Safety Laws in Nigeria." Nigerian Law Journal, (2021) 24(1), 30–48, https://www.nigerianlawjournal.org/articles/eze2021](https://www.nigerianlawjournal.org/articles/eze2021 accessed on 6th May, 2025.

regulations that explicitly incorporate online safety measures into the framework of child protection.

3.1 The Cybercrimes (Prohibition, Prevention, etc.) Act 2015:

The Cybercrimes Act, passed in May 2015, is Nigeria's first legislation specifically addressing cybersecurity. It gives effect to the 2011 ECOWAS Directive on combating cybercrime and provides a legal framework for the prohibition, prevention, detection, investigation, prosecution, and response to cybercrimes. The Cybercrime (Prohibition, Prevention, etc.) Act, 2015 is a landmark legislation in Nigeria that specifically addresses online child sexual exploitation and abuse. It criminalizes various activities related to child pornography, aiming to protect children from the growing risks associated with digital platforms. The key Provisions of the Cybercrime Act Related to Child Protection includes the following:

a. Criminalization of Child Pornography:

The Act prohibits the production, distribution, offering, procurement, or possession of child pornography through computer systems or networks.[19]According to the Cybercrime Act, child pornography includes any pornographic material that visually depicts[20]:

- a minor engaged in sexually explicit conduct;
- a person who appears to be a minor engaged in such conduct; and
- realistic images that portray a minor involved in sexually explicit activities

Offenders convicted of producing, offering, or distributing child pornography face up to 10 years' imprisonment, a minimum fine of ₦20,000,000, or both. For procurement or possession, the punishment is at least 5 years in prison or a minimum fine of ₦10,000,000, or both.[21]

b. Grooming, Luring, or Online Solicitation: The Act criminalizes the use of computer systems to lure, groom, or solicit children for sexual purposes.[22]

The Act reflects Nigeria's commitment to global child protection standards, particularly the UN Convention on the Rights of the Child. The law extends its protection to cover non-physical forms of sexual abuse, such as the circulation of indecent images, grooming, and solicitation, recognizing that harm in the digital space can occur even without physical interaction.[23]

While the Cybercrime (Prohibition, Prevention, etc.) Act, 2015 marks an important step in Nigeria's efforts to safeguard children in the digital age, its scope remains narrow and largely

[19]Cybercrime Act 2015
[20] ibid
[21]Section 23 of the Cybercrime Act 2015
[22] Section 23(3)
[23]EB Obianuju, "Cybercrime: Legal Protection and Liabilities for Nigerian Internet Users" SSRN (2023)https://ssrn.com/abstract=4605510 or http://dx.doi.org/10.2139/ssrn.4605510

reactive, focusing primarily on online sexual offenses. However, the threats children face online today go far beyond sexual exploitation, revealing serious gaps in the Act's protective reach.[24]

One major limitation of the Act is the lack of a comprehensive framework for digital child safety. Although it criminalizes child pornography and online grooming, it does not account for other forms of harm that are equally damaging to a child's mental, emotional, and psychological development. For instance, cyberbullying, a growing issue among school-aged children is not addressed in the Act. Similarly, there are no provisions dealing with online radicalization, exposure to violent or inappropriate content, or the invasion of privacy on social media platforms.

In addition, the Act offers no preventive measures. There is a clear absence of child-specific content regulations, digital literacy programs for schools, or legal obligations placed on internet service providers, social media companies, and tech platforms to protect child users. This lack of a structured, preventive approach means that the law only comes into play after harm has occurred, rather than working to prevent it in the first place.In a digital age where children often spend unsupervised time online, ignorance can be dangerous. Without widespread education and sensitization efforts, even the best-intentioned laws will fail to protect those they are designed to serve.

4.0 GAPS AND LIMITATIONS IN EXISTING PROTECTIONS FOR ONLINE CHILD SAFETY IN NIGERIA

Despite Nigeria's commendable efforts in domesticating the Child Rights Act 2003 (CRA) and launching policies related to child welfare, significant gaps remain in the realm of online child safety, both in legislative content and implementation mechanisms. These gaps weaken Nigeria's ability to address emerging risks such as cyberbullying, online grooming, child sexual exploitation, and exposure to harmful content.

i. Lack of Explicit Provisions on Online Safety in the Child Rights Act (CRA): While the CRA comprehensively addresses children's rights to protection, survival, development, and participation, it does not contain explicit provisions addressing online or digital safety. For instance, sections 3 to 14 of the CRA affirm various rights, including protection from abuse and harmful practices (Sections 11–15), but they were enacted in 2003, before the explosion of digital technologies and internet penetration in Nigeria.The absence of specific terms like "cyberbullying", "online grooming", or "digital exploitation" renders the CRA less effective in today's digital landscape. Accordingly, the law "fails to reflect the reality of children's lives in the digital age," thereby leaving a protection vacuum in a highly dynamic online environment.[25]

[24] unicef.org/eca/media/22501/file/Child Online Protection in and through Digital Learning.pdf

[25] T Iyoha-Osagie"The Right to Online Data Protection of Children: Examining the Adequacy of the Legal Frameworks to Combat Child Online Data Breaches in Nigeria", ABUAD Private and Business Law Journal (2024) 3(1) 82-109 DOI: 10.53982/apblj.2019.0301.05-j accessed 6th May, 2025

ii. Weak Enforcement Mechanisms and Inter-Agency Collaboration: Even where laws such as the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 provide frameworks for some forms of digital safety for children, enforcement is hampered by poor coordination among institutions such as NAPTIP, NCC, Ministry of Women Affairs, and law enforcement agencies. There is no central or specialised body focusing exclusively on online child safety.[26]

iii. Limited Digital Literacy and Awareness: A major limitation in protecting children online is the low level of digital literacy among children, parents, and even law enforcement officers. Without proper knowledge of digital risks, many children fall prey to cyber predators, sextortion, and harmful content. According to the UNICEF Nigeria Digital Literacy Report, over 70% of Nigerian children do not receive formal education on digital safety, and parents are ill-equipped to guide them, especially in rural areas.[27]

iv. Outdated Policy Frameworks: Nigeria's policies on child protection, including the National Child Policy (2007) and National ICT Policy, do not sufficiently reflect current realities of online abuse and digital exposure. There is no standalone National Online Child Safety Strategy, which places Nigeria behind countries like South Africa and the UK, which have adopted integrated national frameworks.[28]

v. Inadequate Funding and Technical Infrastructure: "Combating online child abuse requires strong institutional infrastructure, including cyber-surveillance tools, dedicated reporting hotlines, and well-equipped digital forensic laboratories. However, many Nigerian institutions tasked with protecting children are hampered by chronic underfunding and limited technical capacity. These constraints significantly impair their ability to investigate digital crimes or provide adequate support to victims. According to the Internet Watch Foundation (IWF), Nigeria is listed among countries with limited capacity to detect and remove child sexual abuse material (CSAM) from the internet. Even specialized agencies such as the National Agency for the Prohibition of Trafficking in Persons (NAPTIP), which is responsible for handling cases of trafficking and exploitation, struggle to keep up with the technological demands of combating online abuse. The lack of advanced tools

[26]A Ojedokun. "Institutional Fragmentation and Child Protection in Nigeria: Bridging the Gaps", in African Journal of Law and Society, (2018) 6(1), 317, https://ajol.info/index.php/ajls/article/view/181279](https://ajol.info/index.php/ajls/article/view/181279 accessed on 6th May, 2025.

[27]UNICEF Nigeria. Report on Digital Literacy and Online Safety for Children in Nigeria, p. 9, (2021) https://www.unicef.org/nigeria/reports/children-online-nigeria](https://www.unicef.org/nigeria/reports/children-online-nigeria accessed on 7th June, 2025.

[28] U Okafor. & A Asobie. "Children and Digital Vulnerabilities in Africa: Challenges and Policy Responses", Journal of African Law, (2022) 66(2), 226,https://www.cambridge.org/core/journals/journal-of-african-law/article/children-and-digital-vulnerabilities-in-africa/ accessed on 7th June, 2025.

and specialized training further undermines their effectiveness in addressing digital threats to children.[29]

While Nigeria has made legislative strides with the Child Rights Act, the Cybercrime Act and other policy initiatives, the online safety dimension is largely neglected or insufficiently addressed.

5.0 Online Child Safety Measures/ International Best Practices

With the digitalization of society, online child safety has become a critical component of child protection. The United Kingdom's Online Safety Bill and the European Union's General Data Protection Regulation (GDPR) include provisions specifically aimed at protecting children online. These measures mandate age-appropriate design, parental controls, and stringent data protection standards.[30]Nigeria's legal framework lacks comprehensive provisions addressing online child safety. Incorporating international best practices into national legislation can safeguard Nigerian children in the digital space.[31]

Online child safety has become a paramount concern globally, prompting various jurisdictions to enact legislation aimed at protecting minors in the digital realm. Some of the legislations are:

i) United Kingdom- The Online Safety Act: The United Kingdom has enacted the Online Safety Act, which imposes clear duties on online platforms to safeguard children. The Act mandates the use of effective age assurance technologies to prevent children from accessing harmful content, including violent pornography and material promoting suicide. Platforms are required to implement measures that mitigate risks to children, ensuring a safer online experience.[32]The UK's Age-Appropriate Design Code (also known as the Children's Code), enforced by the Information Commissioner's Office (ICO) in 2021, is one of the most robust online child protection standards globally.[33]It is a set of regulations introduced in the UK to ensure online services prioritise the privacy and safety of children under 18. It provides 15 standards that tech companies must meet when designing digital services likely to be accessed by children. These include: data minimization, default privacy settings, profiling limitations, and age-appropriate information. No equivalent code exists in Nigeria, either in

[29]Internet Watch Foundation (IWF) "Annual Report on Global CSAM Detection" (2022)https://www.iwf.org.uk/report/2022-annual-report](https://www.iwf.org.uk/report/2022-annual-report accessed on 7th June, 2025.

[30]UNICEF. "Every child is protected from violence and exploitation: Global annual results report 2021". (2021) (https://www.unicef.org/media/121671/file/Global-annual-results-report-2021-goal-area-3.pdf accessed on 20th April, 2025.

[31] Ibid.

[32]U.S. Department of Commerce. U.S.-UK Joint Statement on Child Online Safety. (2024) https://www.commerce.gov/news/press-releases/2024/10/us-uk-joint-statement-child-online-safety accessed 19 April, 2025.

[33] ICO. "Age Appropriate Design Code: A code of practice for online services". Information Commissioner's Office, UK, p. 12, 2020 https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-serviceshttps://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services accessed on 7th June, 2025.

the CRA or in ICT regulatory frameworks. Nigerian digital platforms do not have enforceable standards for age-sensitive design or content moderation, thereby exposing children to digital exploitation and manipulation.[34]

ii) Australia: Social Media Restrictions for Minors: Australia has introduced stringent regulations banning children under 16 from accessing social media platforms such as Facebook, Instagram, Snapchat, Reddit, and X. Set to take effect in late 2025, the law includes fines up to $49.5 million for non-compliance. Exemptions exist for health and educational services. This move aligns with global concerns over children's online safety.[35]

iii) European Union: Parental Consent and Age Restrictions: The European Union mandates parental consent for the processing of personal data of children under 16, though some member states have lowered this age to 13. France requires parental consent for children under 15 to create social media accounts, while Germany enforces parental consent for 13-16-year-olds. Belgium mandates a minimum age of 13 for social media usage, and Italy requires parental consent for under 14s.[36]

iv) United States: Children's Online Privacy Protection Act (COPPA): Enacted in 1998, COPPA is a foundational U.S. federal law designed to protect the privacy of children under 13 years of age. It mandates that websites and online services obtain verifiable parental consent before collecting personal information from children. COPPA also requires clear privacy policies and restricts the collection of unnecessary data. The Federal Trade Commission (FTC) enforces COPPA, ensuring compliance and penalizing violations. This legislation has influenced global standards for children's online privacy.[37]

v) Canada-Canadian Centre for Child Protection Initiatives: Canada's approach involves a combination of legislative measures and public awareness campaigns. The Canadian Centre for Child Protection operates programs like Cybertip.ca, a national tipline for reporting online child exploitation. Additionally, educational initiatives aim to inform children, parents, and educators about online safety practices, emphasizing the importance of digital literacy and responsible internet use.[38]

vi) ITU and UNICEF Guidelines: International organizations like the International Telecommunication Union (ITU) and UNICEF have developed guidelines to assist

[34]https://ondato.com/blog/uk-age-appropriate-design-code/#:~:text=The%20Age-Appropriate%20Design%20Code%2C%20also%20known%20as%20the%20Children's,safety%20of%20children%20under%2018.accessed 19 April 2025

[35]The Guardian. "How Australia's tough social media ban compares to laws in other countries". (2024)https://www.theguardian.com/media/2024/nov/29/how-australias-tough-social-media-ban-compares-to-laws-in-other-countries accessed 19 April, 2025.

[36] EU Regulations on Children's Social Media Access, Reuters. "What countries do to regulate children's social media access" (2024)https://www.reuters.com/technology/what-countries-do-regulate-childrens-social-media-access-2024-11-28/ Accessed 19 April, 2025.

[37]Federal Trade Commission. "Complying with COPPA: Frequently Asked Questions" (2015) https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-accessed 19 April 2025questions](https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions accessed on 7th June, 2025.

[38] Canadian Centre for Child Protection. "Cybertip.ca: Canada's tipline for reporting the online sexual exploitation of children" (2024)https://www.cybertip.ca/](https://www.cybertip.ca/ accessed on 8th June, 2025.

policymakers in creating safe online environments for children. The ITU's Child Online Protection initiative emphasizes the need for harmonized national strategies, while UNICEF's guidelines focus on industry responsibilities in combating child sexual abuse material.[39]

6.0 CONCLUSION

This study has critically examined the institutional frameworks and legal instruments governing child rights and online safety in Nigeria, juxtaposing them with international best practices. The analysis reveals significant strides made through the enactment of the Child Rights Act (CRA) 2003 and the Cyber Crimes Act. However, it also uncovers substantial gaps in policy implementation, enforcement, and adaptation to the evolving digital landscape.The digital age introduces new challenges to child safety, with increasing reports of online exploitation, cyberbullying, and exposure to inappropriate content. The Nigerian Communications Commission has initiated efforts to address these issues through the development of child online protection policies and awareness campaigns.[40]

Recent survey data underscores the urgent need for preventive measures to safeguard Nigerian children online. A growing number of children are engaging in potentially dangerous online behaviors that expose them to a wide range of risks, from cyberbullying to sexual exploitation and online fraud. According to findings from a 2024 Ipsos-MTN report on children's digital safety in Lagos, 18% of children admitted to adding strangers to their chat contacts, while 32% acknowledged engaging in conversations with unknown individuals online. Alarmingly, 18% reported that they had met someone in person whom they first encountered online, an act that significantly increases the risk of grooming or exploitation.Moreover, 23% of respondents disclosed that they had shared personal information, such as their age, phone number, or home address, with people they met through digital platforms. These behaviors not only breach basic principles of online safety but also point to a concerning gap in digital literacy and child-focused awareness.[41]

Furthermore, the African Union's Child Online Safety and Empowerment Policy underscores the need for a continental approach to safeguarding children in the digital environment, advocating for comprehensive strategies that encompass legal, technical, and educational measures. Nigeria's alignment with such frameworks remains limited, highlighting the necessity for more concerted efforts in policy formulation and implementation.[42]

7.0 Recommendations

[39] International Telecommunication Union (ITU) "Guidelines for Policymakers on Child Online Protection" (2021)https://www.itu-cop-guidelines.com/policymakers accessed 19 April 2025.

[40]https://www.ncc.gov.ng/consumers/child-onlineprotection#:~:text=Keeping%20Children%20Safe%20Online%20%2D%20Advice,'accessed 19 April 2025

[41]Child online safety Lagos, Nigeria report, Marcus Hollington December, (2024)https://www.mtn.com/wp-content/uploads/2024/12/Nigeria-Lagos-Let-Children-be-Childrenaccessed 19 April 2025

[42]African Union Child Online Safety and Empowerment Policy | African Unionaccessed 19 April 2025

Building on the analysis of the Child Rights Act (CRA) in Nigeria and the current challenges surrounding online child safety, it is essential to strengthen the Act by explicitly incorporating clear and specific protections for children in the digital environment. Other recommendations are:

i. Development and Enforcement of Specific Online Child Protection Laws: The digital landscape presents unique challenges to child safety, necessitating specific legal provisions. The proposed Child Online Access Protection Bill 2023 aims to establish safety standards for digital platforms, including mandatory content regulation and stricter data privacy laws. The swift passage and enforcement of this bill will provide a robust legal framework to address online threats to children.

ii. Expand Legal Frameworks Beyond Sexual Exploitation: Current laws like the Cybercrime Act primarily target sexual offenses but do not adequately address other forms of digital harm such as cyberbullying, online fraud, exposure to harmful content, and privacy violations, hence existing legislation should be amended.

iii. Restricting social media Access for Children Under 16: It is recommended that children under the age of 16 be prohibited from accessing social media platforms. This measure aims to protect younger children from exposure to online risks such as cyberbullying, grooming, and harmful content by restricting their access until they reach a more appropriate age for digital engagement.

iv. Strengthening Institutional Capacities:Agencies such as the National Agency for the Prohibition of Trafficking in Persons (NAPTIP) and the Nigerian Communications Commission (NCC) play pivotal roles in child protection. Enhancing their capacities through adequate funding, training, and technological resources will enable them to effectively combat online child exploitation and enforce relevant laws.[43]

v. Public Awareness and Education Campaigns: Raising awareness about online child safety is crucial. Implementing nationwide education campaigns targeting parents, educators, and children can foster a culture of digital responsibility.

vi. Develop and Implement National Digital Literacy Programs: To empower children with the necessary knowledge and skills to navigate the digital world safely, targeted digital literacy and awareness campaigns must be established across schools, families, and communities. Integrating digital literacy into school curricula will equip children with the knowledge and skills to navigate the online environment safely. This education should encompass understanding online privacy, recognizing potential threats, and knowing how to seek help when necessary.These programs should educate children on the risks associated with sharing personal information online and interacting with strangers, fostering a culture of cautious and informed internet use from an early age.

[43] NAPTIP. "National Agency for the Prohibition of Trafficking in Persons" https://en.wikipedia.org/wiki/National_Agency_for_the_Prohibition_of_Trafficking_in_Persons? Accessed on 8th June, 2025.

vii. Establish Accessible Reporting Mechanisms: It is crucial to create and widely promote user-friendly reporting hotlines and online portals that allow children, parents, and educators to swiftly report incidents of online abuse and exploitation. These reporting channels must be supported by well-trained and responsive teams to ensure timely action, providing victims with accessible pathways to protection and justice.

viii. Mandate Accountability for Digital Service Providers: Internet service providers, social media platforms, and other digital content hosts must be legally required to implement robust child-friendly content moderation and privacy protections. This includes the swift removal of harmful material and regular audits to ensure compliance. Penalties for failure to uphold these responsibilities should be clearly defined and enforced to maintain a safe online environment for children.

ix. Promote Parental Engagement and Support: Parents should be encouraged and supported in their role of monitoring and guiding their children's online activities in a way that respects their privacy and autonomy. Parenting programs and accessible resources focused on digital safety can help bridge the awareness gap and foster safer online environments within homes.

x. Regular Review and Update of Policies: The digital world is constantly evolving, necessitating regular reviews and updates of policies and laws related to online child safety. Establishing a mechanism for periodic assessment will ensure that legal frameworks remain relevant and effective in addressing new challenges.