FINAL REPORT

STUDY ON YOUNG CHILDREN AND DIGITAL TECHNOLOGY: A SURVEY ACROSS NIGERIA

NIGERIAN COMMUNICATIONS COMMISSION

The study is designed to examine the current issues of young people and digital technology consistent with the Child Online Protection Policy of the International Telecommunication Union (ITU).

Table of Contents

Table of Figures

Table of Tables

EXECUTIVE SUMMARY

Digital technology brings communication, education, shopping, entertainment, news, games, fun and much more to everyone, including children. Technology provides children instantaneous access to huge quantities of beneficial materials and offers them a participatory pathway to involvement in society. Digital technology, especially the Internet, is also a vector for cyber-criminals to dispense harm, annoyance and other wrongdoings.

Nowadays, children go online more often, for longer periods, at younger ages with diverse devices and for different purposes. The ways in which the Nigerian child seeks out information, socialises, plays and learns have been altered by the rise and use of new technologies.

The proliferation of digital technologies is accompanied by increasing concern about children's exposure to associated risks and threats. Exposure to risks turns out to be a general side effect of today's children growing up in a digital world. This calls for a pragmatic approach to mitigate the desire to avoid risks and the necessity to access beneficial materials and to balance the immense benefits of digital technology with the safety of the children.

However, the risks and opportunities of digital technologies are not the same for all children. Large gaps exist in access, skills and use, which can affect both online and offline outcomes for children. In general, children who are vulnerable offline tend to be disadvantaged in online spaces as well.

This study is designed to provide an accurate depiction of how children consume digital technology in Nigeria. As such, the respondent pool is structured in favour of children of 4-16 years of age. The study explores the children's device ownership, usage and benefits in pari passu with their awareness of the risks and challenges.

The survey takes a child-centric approach, relying on the children's voices and views to identify and analyse the challenges children encounter with digital technology. The focus is to establish what children actually do online as opposed to what adults think they do. This

includes understanding children's definitions of digital technology, digital use, online contacts and risky or unsafe behaviour.

Stratified multi-stage sampling was the research design chosen for this study. The survey population was delineated into four strata with each stratum segmented into four clusters. This ensured that the survey selected samples in such a way that the target sub-groups were represented in the sample in the same proportion that they exist in the population. Secondary data were sourced through extensive desk review of literature focusing on tapping into the knowledge, experience and expertise of many organizations and individuals from across the world that are specialists in the field of child online protection. Extant pertinent Laws, Acts, Charters, Policies and Guidelines were comprehensively scrutinised to tease out gaps and ascertain adequacy.

The study yielded results in the following broad lines: a) articulation of the level of availability and penetration of technological devices to children (4-16 years of age); b) identification and analysis of challenges encountered by the children; and, c) recommendation of regulatory actions to be taken to shore up online protection for the Nigerian child.

DOCUMENT STRUCTURE

This report is structured as follows:

CHAPTER ONE: Project Background - Introduction
Introduces the study and outlines its key objectives as specified in the Terms of Reference (ToR). The chapter describes the purpose and scope of the study and the core issues and questions the study addresses.

CHAPTER TWO: Research Methodology and Work Plan
Discusses the key aspects of the research approach and work plan used for the study including the methodology overview; sources of data; delineation of the survey area; sampling techniques; data collection instruments; data analysis tools; resource persons and the bespoke training arrangements deployed for the field survey component of the study.

CHAPTER THREE: Results and Key Findings
Presents detailed analyses of the insights, feedbacks and responses from the study population namely children, parents, guardians, teachers and selected Industry stakeholders and policymakers.

CHAPTER FOUR: Conclusion and Recommendations
Submits a recap of the study's key findings and concludes with a rich bouquet of bespoke recommendations and suggestions for the children and all the other stakeholders in the child online protection ecosystem.

APPENDICES
Provide useful supplementary information including the Approved Work Plan for the study; the ToR in full; a digest of the Questionnaires used in the field; the list of selected Industry Stakeholders surveyed; the Definition of technical words; expansion of all the Acronyms used in the report; and a Bibliography of the books, documents and other resources referenced in the study.

CHAPTER ONE

PROJECT BACKGROUND

1.1 Introduction

In broad terms, digital technology refers to electronic tools, systems, processes, devices and resources that generate and store or process data to achieve a particular set of user-defined objectives. Well known examples include computers, television, radio, social media, online games, multimedia, mobile phones and so forth.

Digital technology has evoked a seismic shift in the ways children learn, play and communicate. New technologies have permeated and transformed life in the 21st century. Children in this era have been exposed to digital technologies for their entire lives and are the most frequent users of emerging online and digital services.[1] In fact, some research suggests pre-schoolers become familiar with digital devices even before they are exposed to books.[2]

Despite the proliferation of digital technologies and the growing number of children who use them, there are still many unknowns about children's interaction with these technologies. There is paucity of research on young children as the focus has historically been on adolescents and adults. Therefore, filling the gap on how younger children 4-16 years-old engage with technology and how this affects them is necessary.

It is against this backdrop that this study seeks to extensively identify and proffer possible regulatory remedies to checkmate the current challenges associated with the use of digital technology by young children across Nigeria.

[1] **OECD** (2016); Trends Shaping Education 2016, OECD Publishing Paris: https://dx.doi.org/10.1787/trends_edu-2016-en.
[2] **Hopkins, L., F. Brookes** and **J. Green** (2013), "Books, bytes and brains: The Implications of New Knowledge for Children's Early Literacy Learning", *Australasian Journal of Early Childhood*, Vol. 38/1, pp. 23-28.

1.2 Research Focus

The objective of the Study is to extensively identify and proffer possible regulatory remedies to checkmate the identified challenges associated with the use of digital technology by young children across Nigeria.

1.3 Objectives

The Study covers the entire thirty-six (36) states of the Federation and the Federal Capital Territory, FCT focusing on three core issues:

a) The level of availability and penetration of technology devices to children aged 4-16 years;
b) The identification and analysis of the challenges encountered by the children; and
c) Recommendation of regulatory and users' interventions to mitigate the challenges.

1.4 Scope

The Study seeks to provide answers to the following overarching issues and questions:

1) What are the issues surrounding young people in Nigeria and their use of digital technology in line with the Child Online Protection Policy of the International Telecommunications Union (ITU);
2) How do issues such as risk, privacy, fraud, explicit content that are related to information and communication technology (ICT) affect children in Nigeria;
3) How may effective online barriers be established to mitigate the challenges without undermining the openness of the Internet and its fundamental values;
4) How may children's ability be enhanced to deal with online insecurities and challenges;
5) How may feedback of consultation mechanisms for child online protection be developed;

6) What is the level of effectiveness of previous child online protection policies and guidelines on the stakeholders (children, parents, policymakers etc.);
7) What is the current penetration level of digital technology in relation to youth population across the 36 States of the Federation and the FCT; and
8) What suggestions/recommendations may improve the safe interaction between young people and digital technology?

CHAPTER TWO

METHODOLOGY

2.1 Research Methodology and Work Plan

The field survey and interviews took place over a staggered period of four months from 15th June, 2020 to 12th October, 2020. The enumeration data was collected using stratified sampling at the strata levels and multi-stage cluster sampling for each cluster. This ensured that the survey selected samples in such a way that the target sub-groups were represented in the sample in the same proportion that they exist in the population.

2.2 Survey Domains

The survey population was distributed into four domains, namely:

a. Urban Area;
b. Rural Area;
c. Children 4 -10 Years Old;
d. Children 11-16 Years Old.

The Urban Area domain comprised Abuja, all the thirty-six State capitals and one other major town from each State. The Rural Area domain included carefully selected headquarters of two Local Government Areas per State. The children were grouped into two age bands of 4-10 years old and 11-16 years old. This domain demarcation is in recognition of the different digital technology needs of each demographic.

2.3 Delineation of Survey Area

The Study covers the thirty-six (36) States of the Federation plus the FCT with equal emphasis on urban and rural areas. To this end, and for ease of data collation, the thirty-six (36) States of the Federation and the FCT were delineated into four strata titled Zone A, Zone B, Zone C and Zone D, each with a Project Implementation Unit (PIU) situated centrally within the zone.

The PIUs were located respectively at Abuja, FCT for Zone A; Ibadan, Oyo State for Zone B; Calabar, Cross River State for Zone C; and Jos, Plateau State for Zone D. The States were further subdivided into two urban and two rural area clusters respectively. To ensure Federal spread, the survey was segmented into 50% rural area clusters and 50% urban area clusters in four strata as outlined in the tables below.

Stratum	State	Urban Cluster	Rural Cluster	PIU Location
A	FCT	AMAC	Abaji	Abuja, HQ
		Gwagwalada	Bwari	
	Jigawa	Dutse	Hadejia	
		Birnin Kudu	Gwiwa	
	Kaduna	Kaduna	Birnin Gwari	
		Zaria	Zangon Kataf	
	Kano	Kano	Danbatta	
		Gwarzo	Doguwa	
	Katsina	Katsina	Faskari	
		Daura	Batsari	
	Kebbi	Birnin Kebbi	Wasagu	
		Bagudo	Ngaski	
	Niger	Minna	Suleja	
		Bida	Borgu	
	Sokoto	Sokoto	Sabon Birni	
		Kebbe	Gudu	
	Zamfara	Gusau	Bakura	
		Shinkafi	Maru	

Table 1: Stratum A - Member States and Clusters

Stratum	State	Urban Cluster	Rural Cluster	PIU Location
B	Edo	Benin City	Ovia South West	Ibadan
		Auchi	Esan South East	
	Ekiti	Ado Ekiti	Ijero	
		Ikole	Emure	
	Kogi	Lokoja	Ibaji	
		Ankpa	Yagba West	
	Kwara	Ilorin	Baruten	
		Offa	Pategi	
	Lagos	Ikeja	Eti Osa	
		Lagos Island	Ifako-Ijaiye	
	Ogun	Abeokuta	Ogun Waterside	
		Shagamu	Ipokia	
	Ondo	Akure	Ose	
		Okiti-Pupa	Akoko North West	
	Osun	Osogbo	Ifedaro	
		Ife South	Iwo	
	Oyo	Ibadan	Iwajowa	
		Irepo	Surulere	

Table 2: Stratum B - Member States and Clusters

Stratum	State	Urban Cluster	Rural Cluster	PIU Location
C	Abia	Umuahia	Isiukwuato	Calabar
		Aba	Ukwa West	
	Akwa Ibom	Uyo	Ikot Ekpene	
		Oron	Eket	
	Anambra	Awka	Ihiala	
		Onitsha	Orumba South	
	Bayelsa	Yenagoa	Ekeremor	
		Brass	Southern Ijaw	
	Cross River	Calabar	Ogoja	
		Obudu	Abi	
	Delta	Asaba	Ughelli South	
		Warri	Burutu	
	Ebonyi	Abakiliki	Ishielu	
		Afikpo	Ivo	
	Enugu	Enugu	Igbo Eze North	
		Nsukka	Aninri	
	Imo	Owerri	Ngor-Okpala	
		Orlu	Okigwe	
	Rivers	Port Harcourt	Ogba Egbema Ndoni	
		Bonny	Etche	

Table 3: Stratum C - Member States and Clusters

Stratum	State	Urban Cluster	Rural Cluster	PIU Location
D	Adamawa	Yola	Toungo	Jos
		Lamurde	Madagali	
	Bauchi	Bauchi	Bogoro	
		Ningi	Zaki	
	Benue	Makurdi	Agatu	
		Otukpo	Kwande	
	Borno	Maiduguri	Bayo	
		Gworza	Abadam	
	Gombe	Gombe	Nafada	
		Balanga	Shongom	
	Nasarawa	Lafia	Awe	
		Karu	Toto	
	Plateau	Jos	Wase	
		Pankshin	Bokkos	
	Taraba	Jalingo	Ibi	
		Ussa	Sardauna	
	Yobe	Damaturu	Machina	
		Potiskum	Yunusari	

Table 4: Stratum D - Member States and Clusters

2.4 Primary Sampling Unit

Given that majority of the members of the focus group comprising the children, parents and teachers are found mostly in households, primary schools and secondary schools the study surveyed parents, pupils and educators in the following sample size per State. The children were distributed in the ratio of 40:60 between the age groups 4-10 and 11-16 years old respectively.

Stratum	Cluster	Number of Clusters	Sampling Unit	Number of Units	Respondents	Number of Respondents	Total Number of Respondents
State	Urban	2	Household	10	Parents/Guardians	10	124
					Children 4-10[3]	20	
			Primary School[4]	-	Children 6-10	40	
					Teachers		
			Secondary School	4	Educators	4	
					Children 11-16	40	
			Street / Out-of-School[5]		Children 10-16	10	
	Rural	2	Households	10	Parents/Guardians	10	124
					Children 4-16	20	
			Primary School	-	Children 6-10	40	
					Teachers		
			Secondary School	4	Educators	4	
					Children 11-16	40	
			Street / Out-of-School Children		Children 10-16	10	

Table 5: Primary Sampling Units

[3] Children of primary school age enumerated as part of Households and in shopping malls, parks and gardens

[4] Due to Covid19 restrictions primary schools were not in session across the country during the field survey

[5] Almajirai, children hawking on the streets and children in homeless shelters

2.5 Source of Primary Data

Primary data came from three distinct sources which are: (a) interviews and questionnaires[6] administered primarily on the children, their parents/guardians and teachers;[7] (b) consultations with selected sector stakeholders; and (c) online using social media channels.[8]

In summary, 10 households, and eight secondary schools were surveyed per cluster giving a total of 740 households and 296 secondary schools across the country for a combined pool of 9176 respondents.

A total of 7013 usable responses were received comprising 740 (10.6%) from respondents who identified as parents and guardians; 592 (8.4%) from school teachers; 2272 from children 4-10 years of age; and, 3409 from children 11-16 years old. The children altogether constitute 81% of the total number of respondents.

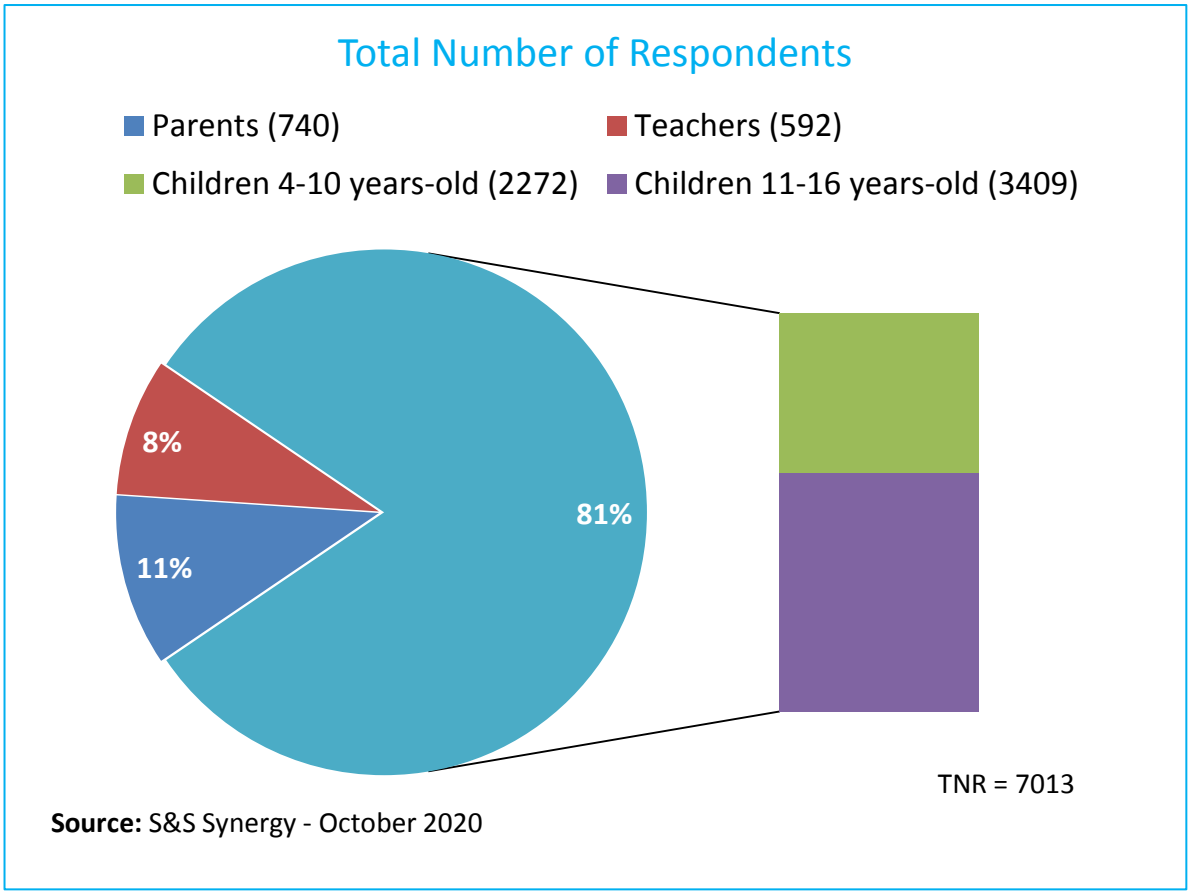


Figure 1: Total Number of Respondents

[6] See Appendix 2 – Survey Questionnaire for Children
[7] See Appendix 3 – Survey Questionnaire for Parents and Teachers
[8] Google Forms, Facebook, Twitter, Instagram

2.6 Gender /Age and Rural/Urban Distribution of Respondents

Because it is all about them, the survey was configured in favour of the children who constituted a total of 5681 (81%) of the respondents. The children were categorised in two domains of 4-10 year-olds and 11-16 year-olds. A total number of 3534 (62%) respondents identified as males while females totalled 2147 (38%).

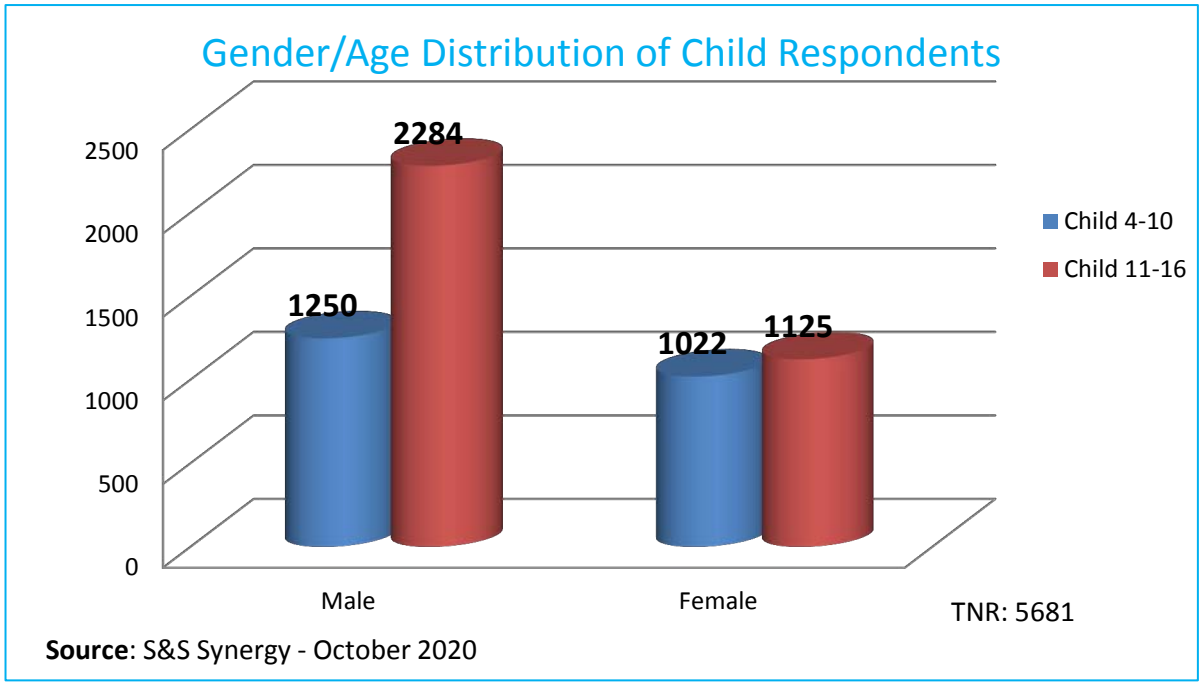


Figure 2: Gender/Age Distribution of all the Children

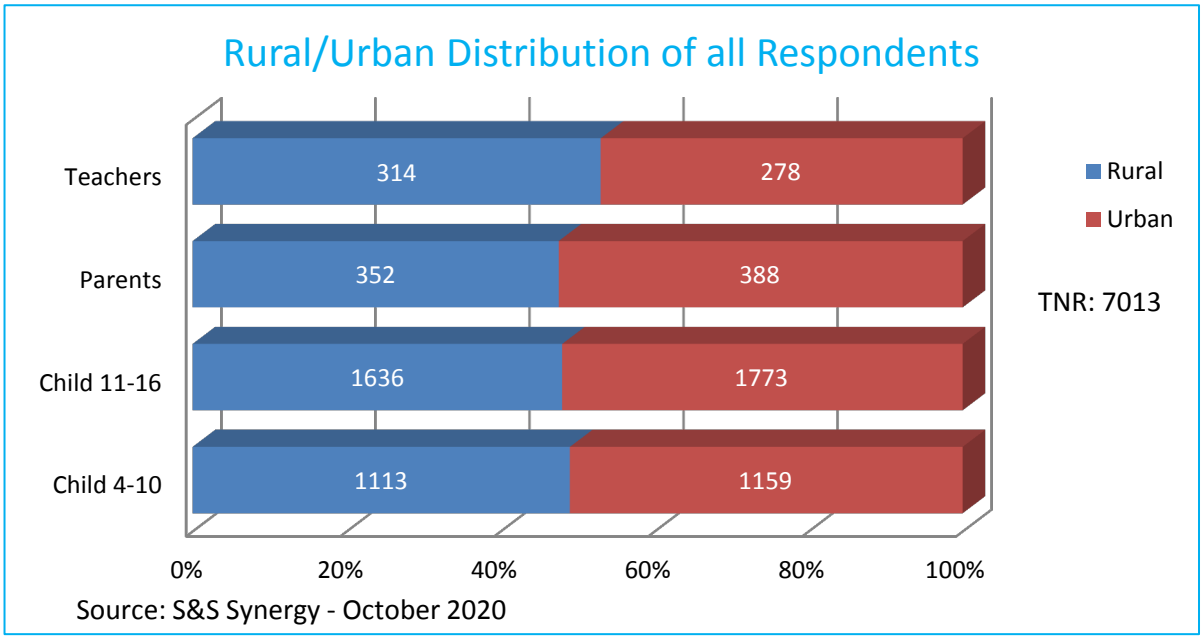


Figure 3: Rural/Urban Distribution of all the Respondents

2.7 Federal Distribution of Respondents

The target number of respondents from each State was 248, the survey garnered responses from all thirty-six (36) States and the FCT in the numbers per State as outlined in the table below.

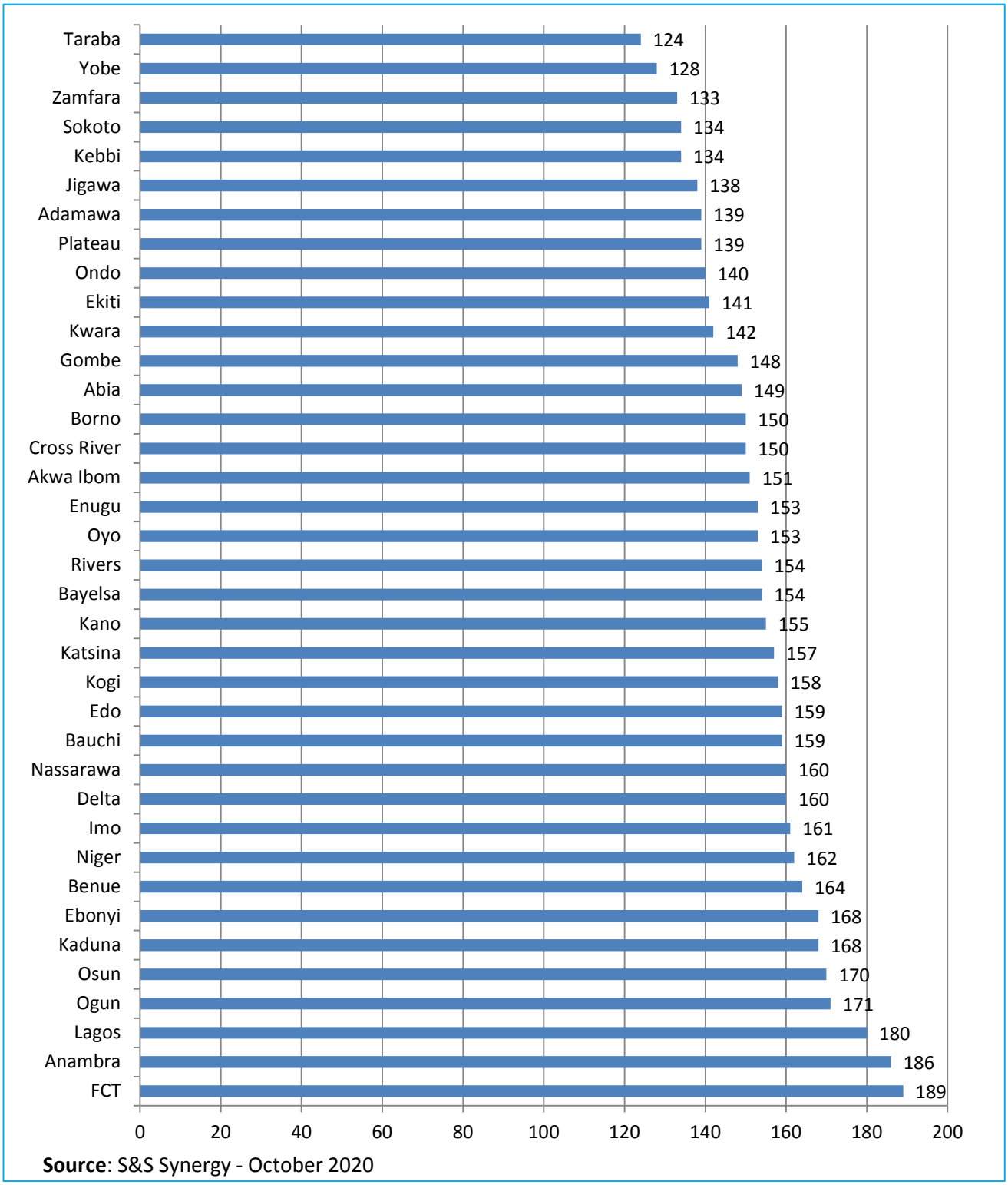


Figure 4: Federal Distribution of Respondents

2.8 Residency and Schooling Status of Child Respondents

The survey returned a total number of 1159 (20.4%) of the 4-10 years-old as living in the urban areas and 1636 (28.8%) of the 11-16 years-old are rural dwellers. The number of children that responded in the negative to the question: "Do you go to school?"[9] came to 965 (17%). These out-of-school children are spread out across both rural and urban areas. They make up the bulk of the almajirai. The survey discovered that most of the children in this category are astute consumers of digital technology especially mobile phones and radio.

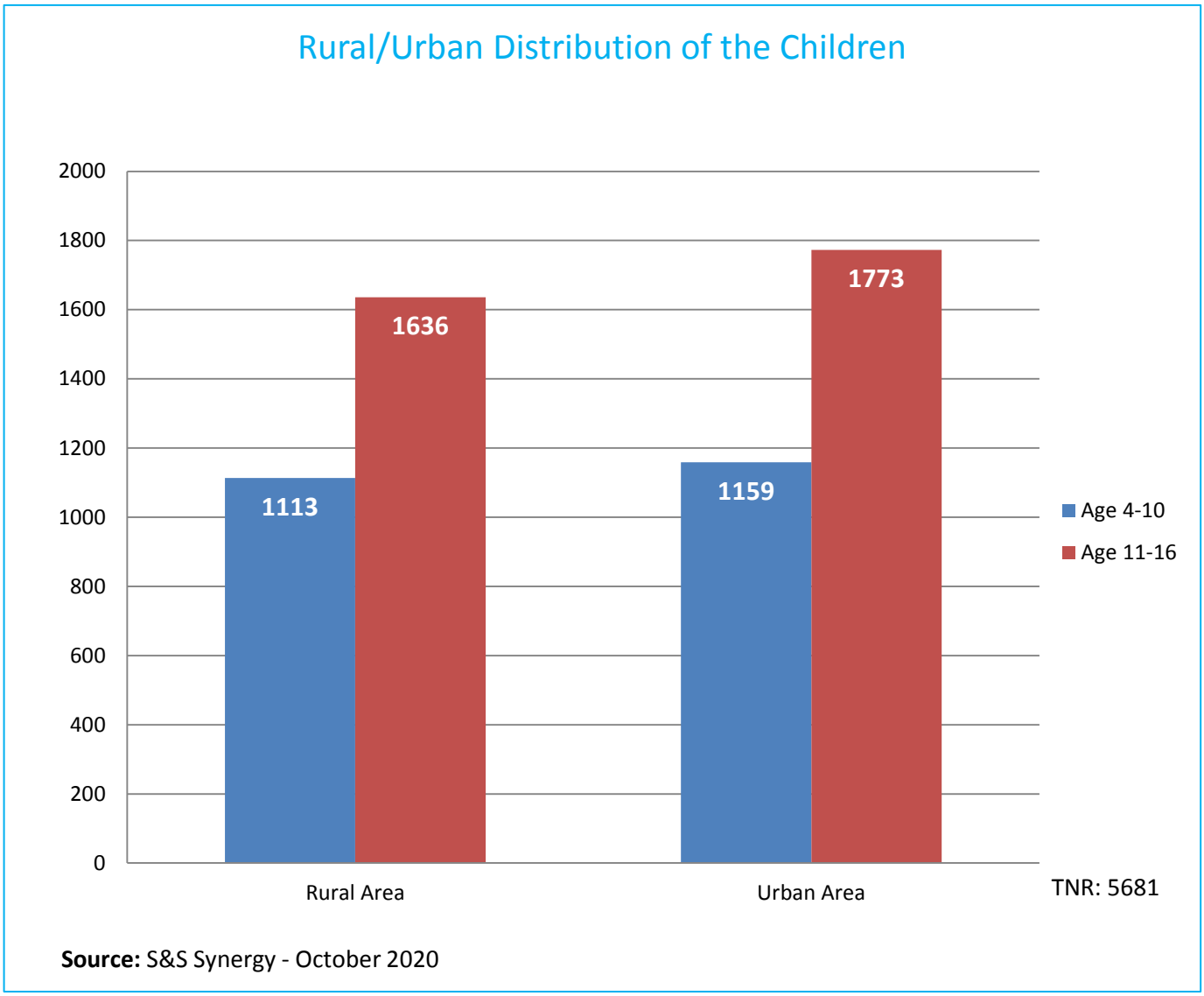


Figure 5: Rural/Urban Distribution of the Children

[9] Question 5 of the Questionnaire for Children

2.9 Source of Secondary Data

The research team conducted an extensive desk review of published materials both online and offline including particularly the following relevant literature.

	Literature	Source	Relevance
1	The Nigeria Child Online Protection Policy framework (2014)	NCC	A document developed through inter-agency collaborations with extensive use of various Local and International Institutions and sets out the framework for the National policy on online protection for children in Nigeria;
2	Child Online Protection Policy (2019) - Guidelines for Industry - Guidelines for Parents and Educators - Guidelines for Policymakers	ITU	A global framework on children's protection and safety online;
3	Industry Child Online Protection (2019)	UNICEF	A document birthed via multi-stakeholder and sectoral approach with collaboration by Governments, parliamentarians, civil society, the private sector, professionals working with children, parents and children themselves;
4	Legacy research materials on the Internet	Internet	Materials on children's exposure to digital technology;
5	United Nations Convention on the	UN	An important and significant legal tool in the

	Rights of the Child (1989)		defence and promotion of children's and young people's rights;
6	Empowering and Protecting Children Online (2009)	EU	A useful material for insight into international best practice on protecting children online;
7	Framework for Safer Mobile Use by Younger Teenagers and Children (2007)	GSMEurope	A self-regulatory initiative of the European mobile industry, which puts forward recommendations to ensure that younger teenagers and children can safely access content on their mobile phones;
8	Cybercrimes (Prohibition, Prevention, etc.) Act 2015	NSA	The first legislation in Nigeria that deals specifically with cybersecurity issues;
9	Publications on Child Online safety issues	Various	Drawn from various sources, climes and epochs for the richness of information;
10	Nigeria Data Protection Regulation (NDPR) (2019)	NITDA	Covers transactions around the processing of personal data and of person(s) residing in Nigeria or residing outside Nigeria but of Nigerian descent;
11	General Data Protection Regulation (GDPR) (2018)		A regulation in EU law on data protection and privacy; addresses the transfer of personal data outside the EU and EEA areas; and
12	Newspapers, magazines, blogs and bulletins	Various	For heads-up on trends, opinions, happenings in society relevant to the Study.

Table 6: Schedule of Desk Review Literature

2.10 Data Analysis

After the questionnaires were received at the PIUs from the field, a data entry team inputted the information through a data entry screen specially created with checkpoints to ensure accuracy. All questionnaires were double-checked for completeness. Erroneous entries were verified and corrected appropriately. The captured data was exported to Statistical Package for Social Sciences (SPSS) for cleansing. The cleansed data was weighted before final analysis using G- Forms with its wide array of visualisation tools in the form of charts, pivot tables, summary views, and custom themed widgets.

2.11 Survey Limitations

The Covid19 pandemic imposed some limitations on the survey. The questionnaires were administered on the 4 -10 year-olds on the streets and shopping malls and not within the relative tranquillity of their schools because primary schools were on lockdown across the country during the period. The window of opportunity to attend the selected secondary schools opened only when the Federal Government approved the return to school of exit students to complete their final exams.

Although field operatives received reinforced sensitization on the NCDC safety protocols, the survey was hampered by nationwide movement restrictions and school closures which shifted the interviews that should have happened inside households and primary schools to the streets and shopping precincts.

The study sought to caucus with selected sector stakeholders in roundtable settings. But this was hardly possible as many of the organisations were operating restricted access to their premises for non-staff. Meetings with this category of stakeholders were therefore mostly conducted mainly over the phone and by Zoom where possible.

The synchronisation of participants' calendars for the virtual meetings and bringing some of them up to speed with remote-access technology

coupled with network connectivity vagaries introduced some constraints to that segment of the survey.

CHAPTER THREE

RESULTS AND KEY FINDINGS

3.10 Objective One – Young People and Digital Technology

1. **What are the issues surrounding young people in Nigeria and their use of digital technology in line with the Child Online Protection Policy of the International Telecommunications Union (ITU)?**

3.11 Key Findings

Digital technology particularly the Internet has become an integral part of Nigerian children's lives. This is especially true for those children who use it more broadly for social networking, uploading photos, doing homework, playing digital games or watching videos. Motivations for using the Internet vary mainly by the children's age, location, devices and frequency with which they access it.

Numerous issues surround children in Nigeria and their use of digital technologies. The issues range from the availability of digital devices to high costs, low purchasing power and epileptic infrastructure especially for those in the rural or poor areas. There are also challenges around the physical and psychological wellbeing of the children emanating from disordered consumption of digital content and digital technology in general.

3.11 Disordered Use of Technology

Children across the two age spectrums spend an inordinate length of time engaged with digital technology each day. Through watching television, playing video games or surfing the Internet the Nigerian child on average can amass screen time for lengths of up to three hours per day. In extreme cases some children clock up to ten hours or more screen time per day verging on addiction disorder.

The problem of technology addiction disorder is rampant among children as they are the group most prone to uncontrolled video game playing or social media use.[10]

The 2020 Child Online Safety Index report submits higher levels of disordered use of technology among children in Nigeria, placing her 6th from the bottom of the list of 30 peer countries. The rating is based on four indices – the severity of gaming disorder symptoms; the percentage of children at risk of gaming disorder; the severity of social media disorder symptoms; and, the percentage of children at risk for social media disorder.

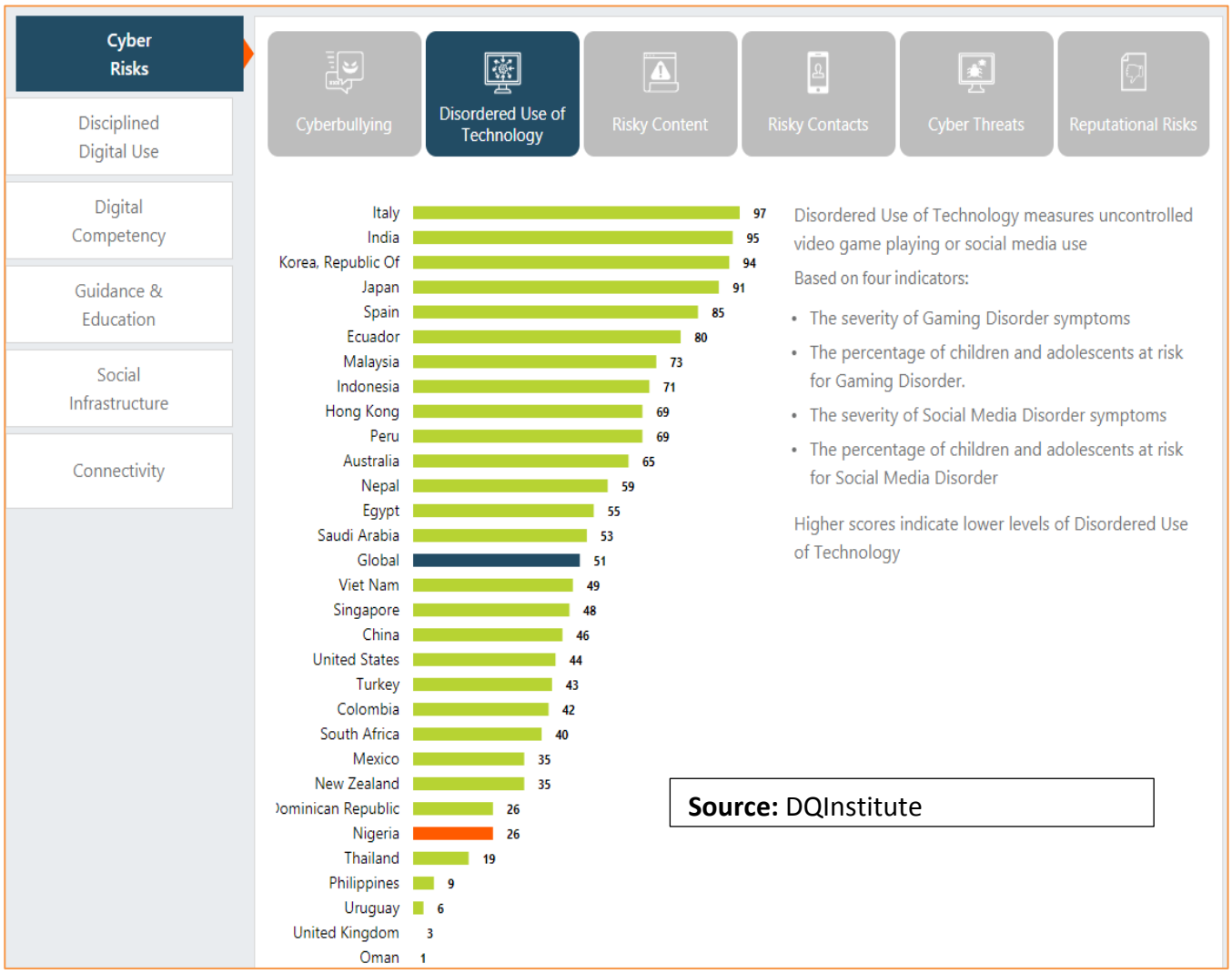


Figure 6: Nigeria's Peer Rating on Disordered Use of Technology

[10] **E. L Anderson,** Et Al; "Internet Use and Problematic Internet Use: A systematic Review"

Digital technology addictions manifest in different forms including excessive viewing of video clips, compulsive video game-playing and uncontrolled browsing and chatting on social media.

Disordered use of technology arises when an individual engages in online activities at the cost of fulfilling daily responsibilities or pursuing other interests and without regard for the negative consequences.[11] Parental educational level, age at first use of the Internet, and the frequency of using social networking sites and gaming sites are found to be associated with excessive Internet use among children.[12]

Seeking to probe the frequency and online activities of the Nigerian child, the survey uncovered that 85% of the urban 11-16 years-old children browse and chat on social networking sites every day as captured in the table below.

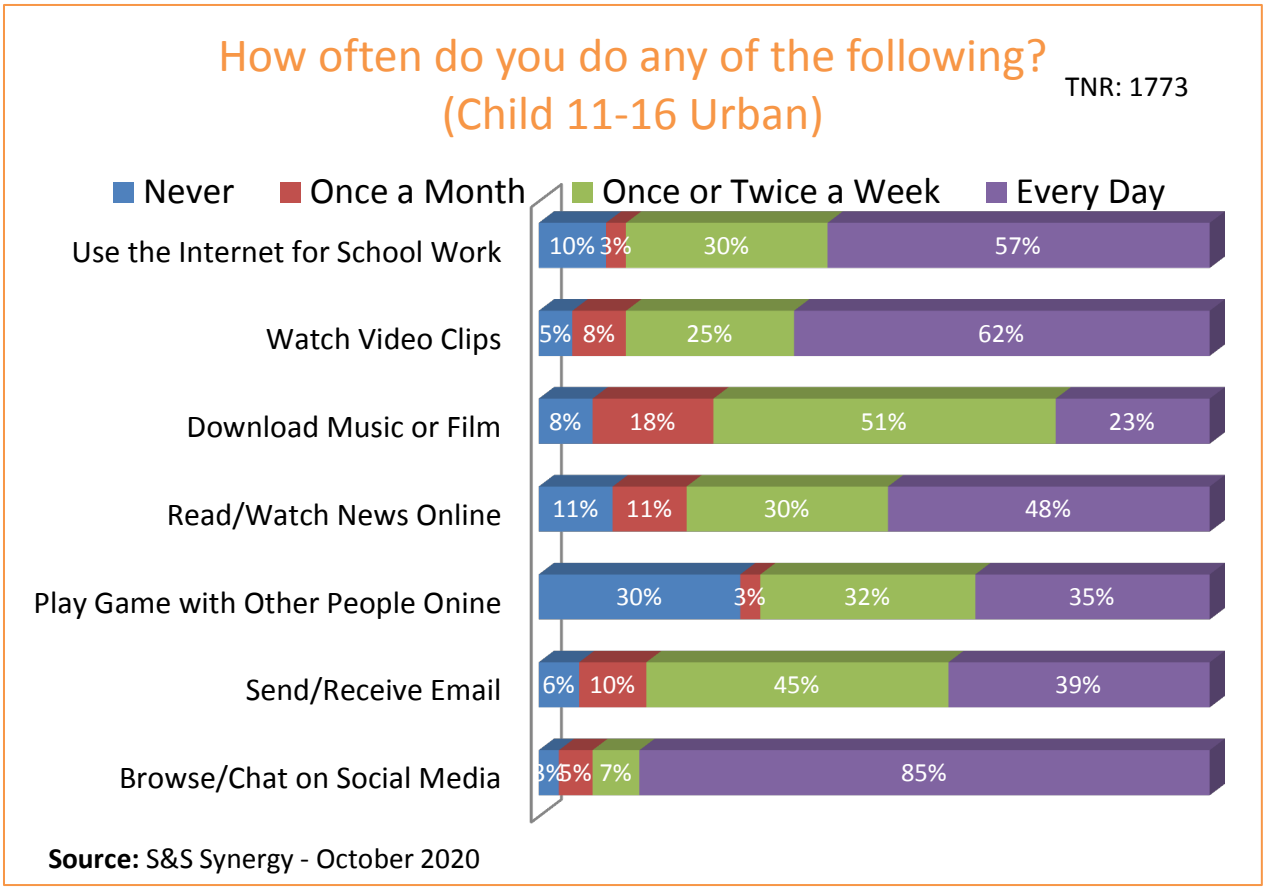


Figure 7: Frequency and Online Activities of Urban 11-16 Years-Old Children

[11] **Viswanath Venkatesh,** Et Al; "Children's Internet Addiction, Family-to-Work Conflict, and Job Outcomes"

[12] **Shankar Ramachandran:** "Technology: Smart tablet or just a new drug? - Lessons for Use of Technology with Children"

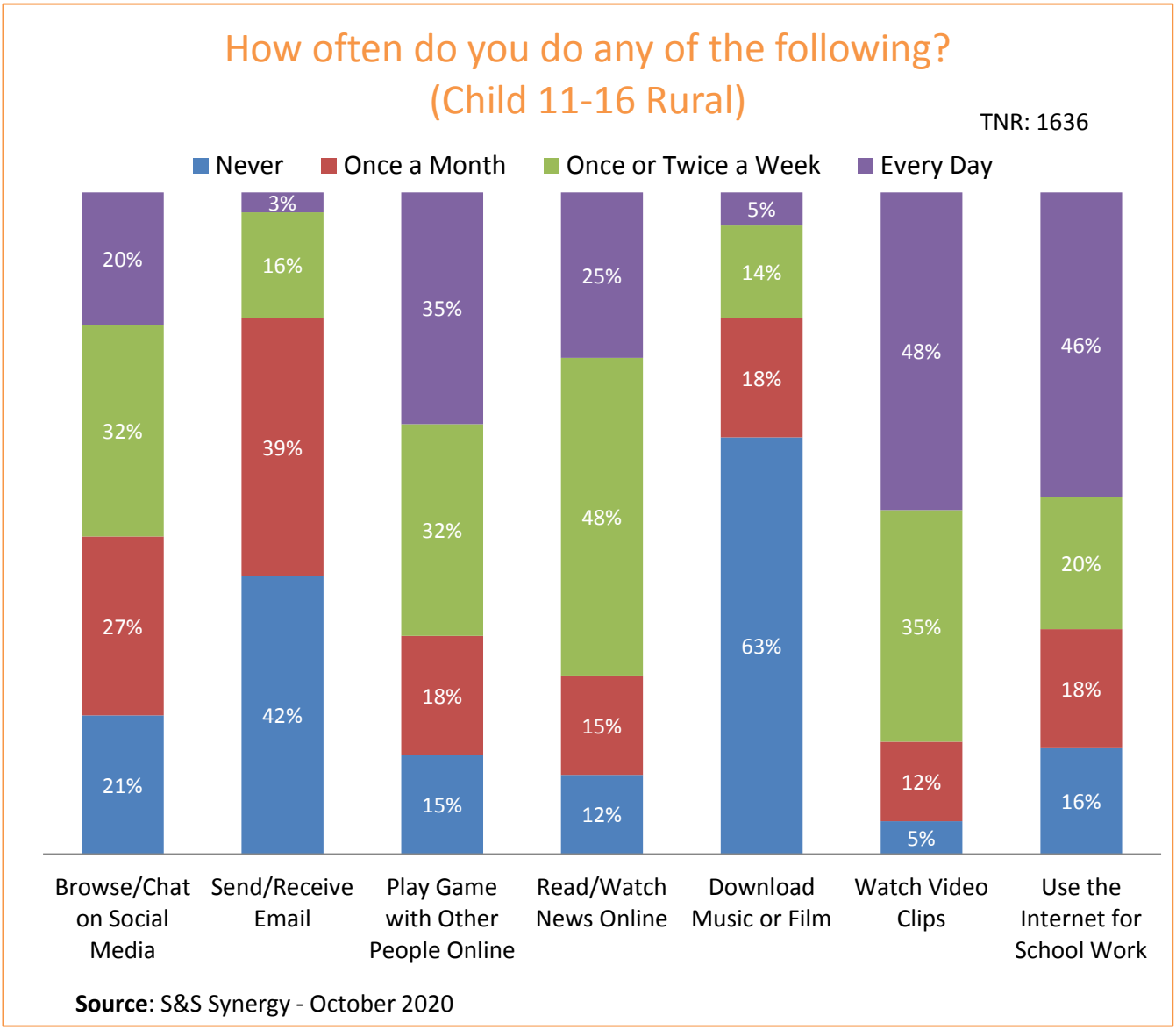


Figure 8: Frequency and Online Activities of Rural 11-16 Years-Old Children

The use pattern is different with the 11-16 years-old children in the rural areas where only 20% does chatting and browsing on social media every day. Watching video clips is an activity that rural 11-16 years-old children spend 48% of their online time doing every day.

Covid19 heralded an increase in the number of both rural and urban children using the Internet to conduct their school work at 57% urban and 46% rural daily average.

From the results, it is evident that there are remarkable differences between urban dwellers and their peers in the rural areas in the way and frequency with which each demographic uses digital technology.

Prevailing trends indicate that Nigerian children's access to technology devices and the Internet will continue to increase, which will correspond to both increased benefits of being online and increased risks. The children are particularly vulnerable not because of the expansion of access but from unawareness of the possible risks and the apparent lack of safeguards in place.

3.12 Means and Moderation of Access to the Internet

The survey findings show that 93% of the 11-16 year-olds and 45% of the 4-10 year-olds go online with their own mobile phones indicating a high rate of phone ownership among children in Nigeria. The least popular means of access to the Internet for both age groups is the school.

The implication of this is that children often go online mostly through means that are not as actively moderated as either the Internet café or the school. The aggregate effect is that children are inadvertently exposed to more online risks than would have been the case were they to use their schools' devices to get online.

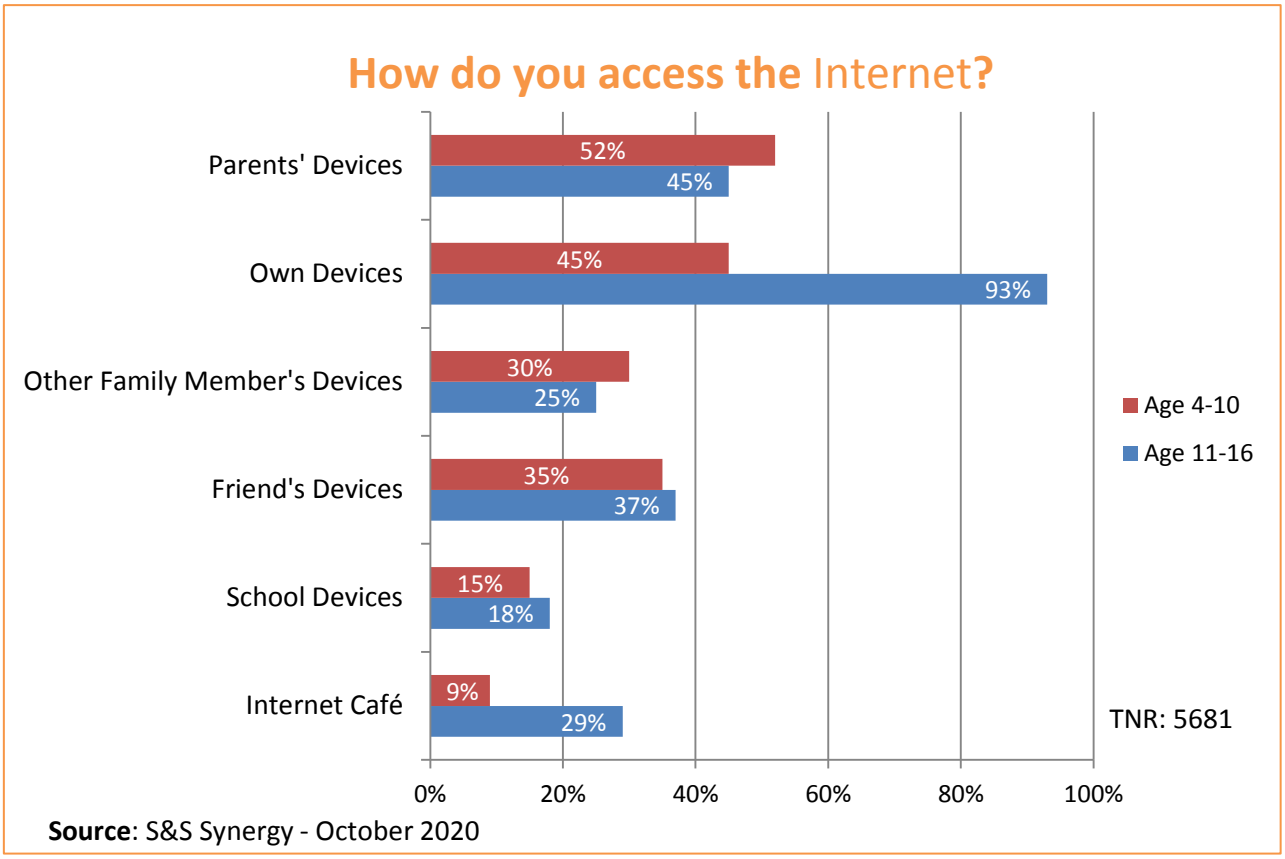


Figure 9: Means of Access to the Internet

Evidently, majority of children in Nigeria receive little or no curation with their online activities from either parents or guardians. Most parents appear not to have rules about their children's Internet use particularly with time limits and site restrictions.

A staggering 56% of the 11-16 year-olds in both urban and rural areas does not have any form of restriction on their Internet use. The aggregate implication of this is that this bunch of youngsters can become digital nomads at liberty to wander the cybersphere tethered only by the elasticity of their data bundles.

Perhaps because of tenderness of age or ownership of device, more of the 4-10 years-old children than their 11-16 years-old compatriots enjoy parental moderation of their Internet consumption with 94% enjoying mediation in one form or the other ranging from time limits (19%), restriction of access (45%) and both time limit and restriction of access (30%).

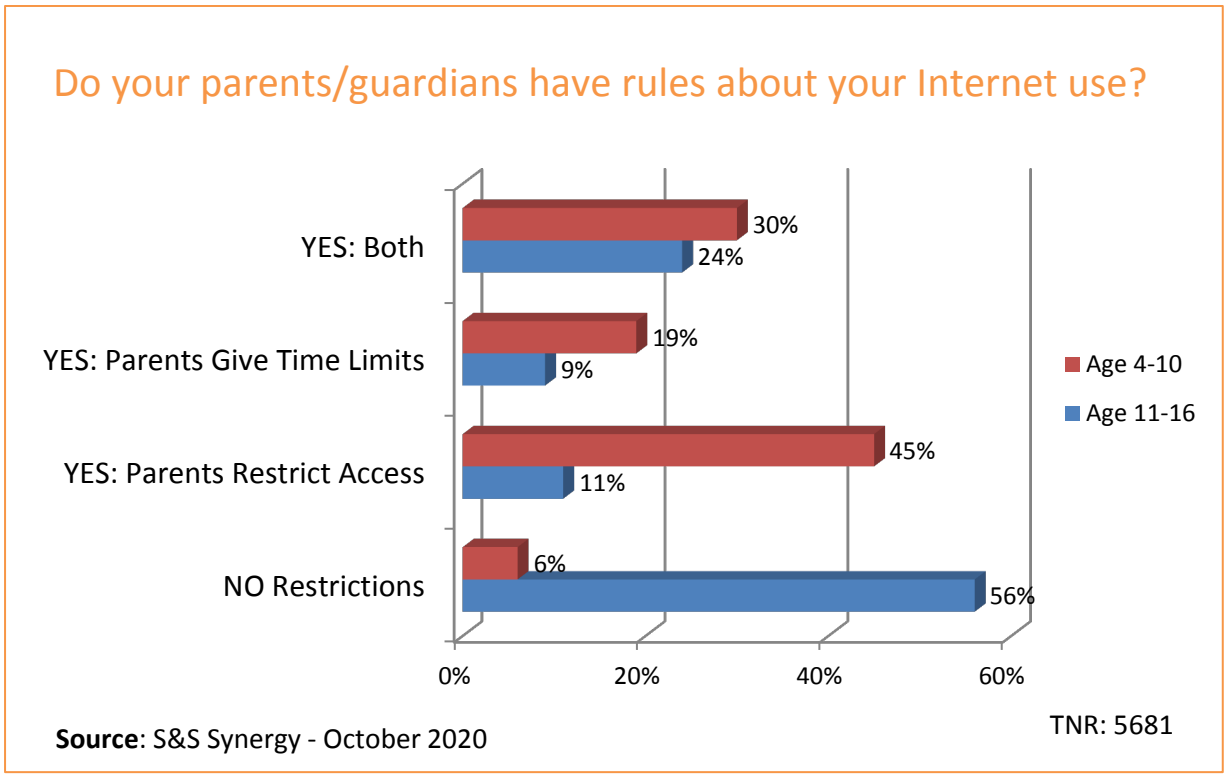


Figure 10: Parental Moderation of Access to the Internet

Another curious finding is that the 11-16 years-old children do not consider their parents as their first go-to persons to discuss their online

activities. It would appear as though the older the children get the wider the gulf of conversation gets between parent and child especially if the conversation is to do with the Internet.

The survey revealed that no conversation happens between parents and 50% of the 11-16 years-old children about their activities online. Only in the 4-10 years-old group does 76% talk openly and regularly with parents about their online activities. Even among the 4-10 years-old children there is 5% that said conversation with parents about their online activities never occurs.

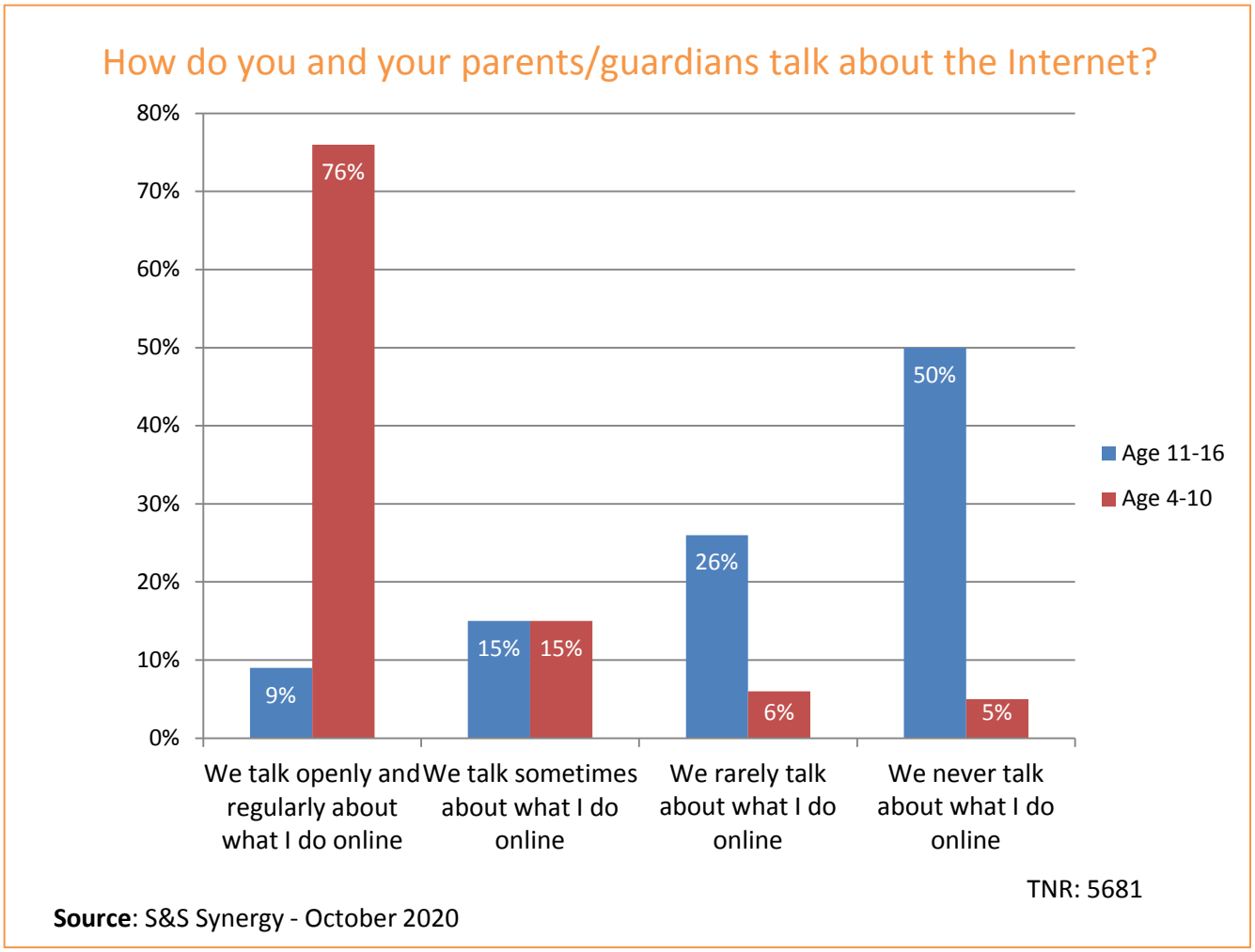


Figure 11: How and When Children and Parents Talk About What They Do Online

Parents, it would appear, are not the only ones at the receiving end of the children's rebuff when it comes to Internet issues. The teachers also struggle on such matters. This is evidenced by the 30% of the 11-16 years-old children who said no teacher had ever talked to them about what they do on the Internet.

On the other end of the scale 70% of the children had at one time or the other received help from a teacher whether for something that bothered them on the Internet, or explanation why some websites are good or bad or generally talked about what they do on the Internet.

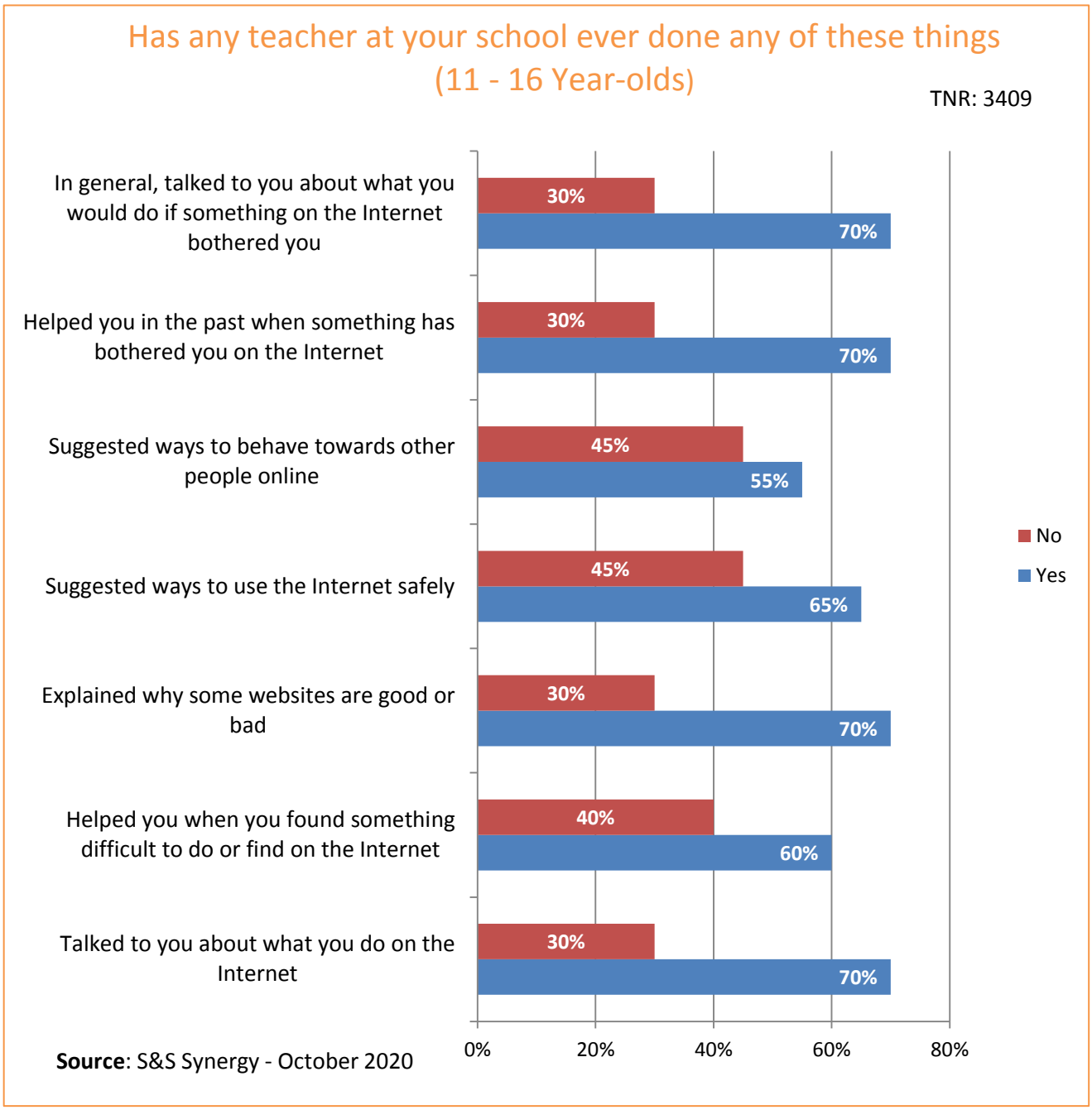


Figure 12: Measuring the Child-Teacher Communication Gap

3.13 Favourite Social Networking Sites (SNS) for Children in Nigeria

Globally, children like to watch video content and listen to music and spend time on social media. This is also true for children in Nigeria, who are most active across social media networks with their most popular Apps being WhatsApp, Facebook, Instagram and YouTube in that order. The Nigerian children also spend a lot of time playing already downloaded video or educational games on their mobile devices.

The results reveal that WhatsApp is the favourite social networking app for children in Nigeria at 87% followed by Facebook 85%, Instagram 57%, YouTube and Messenger at joint 54% with Twitter and Imo bringing up the rear at 30% and 8% respectively.

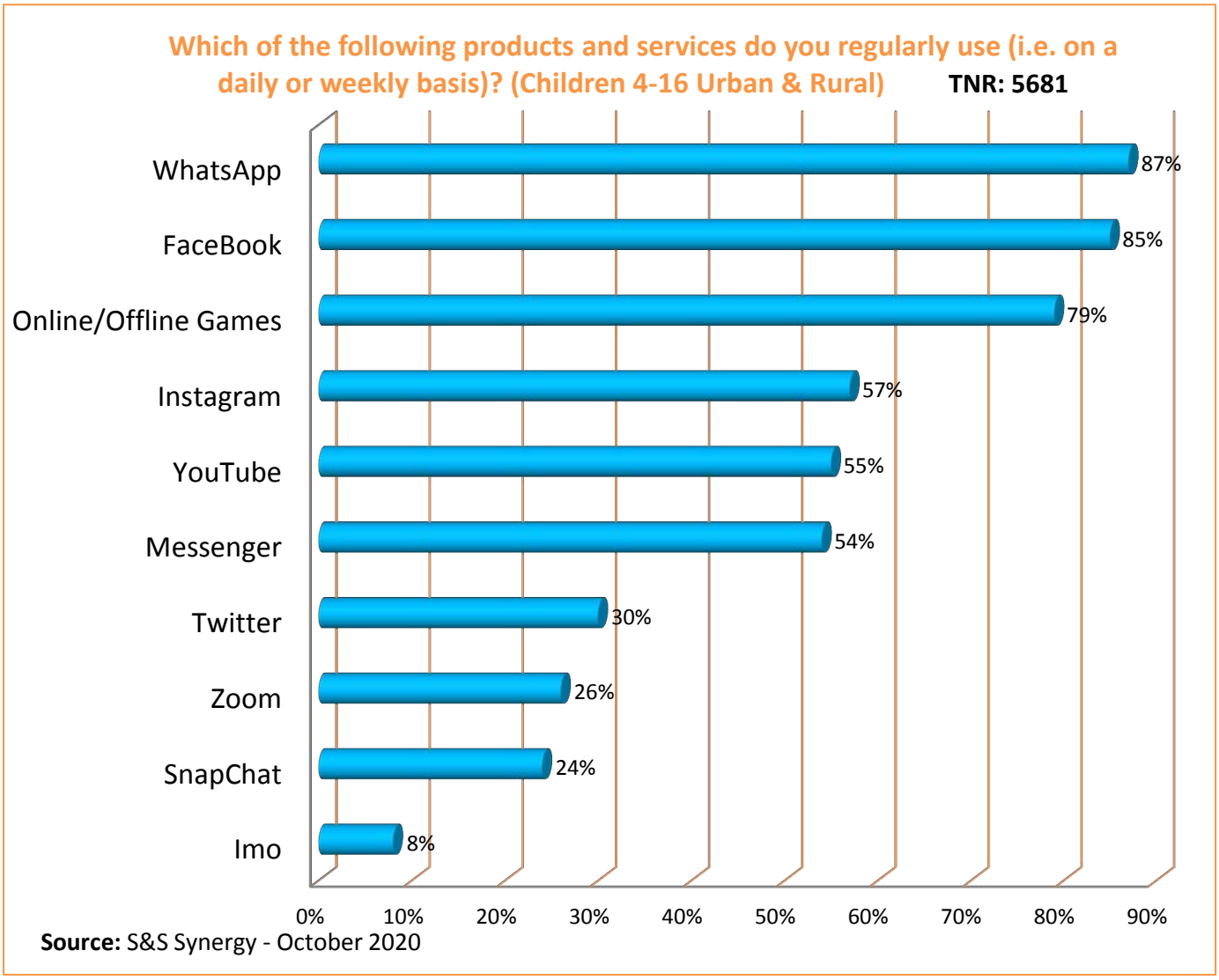


Figure 13: Favourite Apps and Social Networking Sites for Children (4-16 years old)

3.20 Objective Two – Risk, Privacy, Fraud and Explicit Content

2. How do issues such as risk, privacy, fraud and explicit content that are related to Information and Communications Technology (ICT) affect children in Nigeria?

3.21 Key Findings

The risks children face online fall into four broad categories namely content, contact, conduct and contract as fully described in the table below.

Table 7: Categories of Online Risks

Category	Description
Content Risk	Risky content contains nudity, sexual images or movies, hateful or violent material or information that advocate the use of drugs, tobacco or alcohol. Besides the Internet, influence can also come from other media such as television, song lyrics, magazines, movies/videos, and video games;[13] Where children encounter exposure to illegal and harmful content, such as pornography, gambling, self-harm sites and other content inappropriate for young people.[14] In most cases, operators of these sites do not take effective measures to restrict children's access to their websites; Sexting – the relatively new phenomenon where children and young people are putting themselves at risk by posting sexually provocative images of

[13] **Kelly Ladin L'Engle;** https://pubmed.ncbi.nlm.nih.gov/16488814/
[14] https://www.flicklearning.com/blog/e-safety-what-are-the-dangers

	themselves online or sending them to friends using mobile technologies. Relying upon or using inaccurate or incomplete information found online, in other words fake news, or information from an unknown and unreliable source; The preponderance of, and the privacy associated with social media technology limits the extent to which children can be supervised or monitored by adults or parents. Thus, most often, children are at liberty to watch, view or use sexual sites notwithstanding the risks involved.[15]
Contact Risks	Where children are involved in an adult initiated online activity e.g. grooming, stalking, sexual exploitation;[16] The most typical scenario of Risky Contact is that a sexual predator takes advantage when a child discloses vulnerability online. The predator offers to be an understanding and supporting adult and starts building a manipulative relationship with the child. When this process, called grooming, is completed, the potential victim often readily travels to meet the predator, even if aware of the adult's sexual intentions;[17] Often involves inappropriate contact, especially with adult impostors posing as children, pretending to be someone else, often another child, as part of a deliberate attempt to harm or harass someone else online. Both adults and young people can use the Internet to seek out children or other young people who are vulnerable. Frequently, their goal is to convince the target that they have developed a meaningful relationship, but the

[15] **Emmanuel Olagunju Amoo;** Effects of Adolescents Exposure to Sexual Contents on Social Media in Nigeria
[16] **Professor Sonia Livingstone**; LSE; Children's online activities, risks and safety
[17] **Marika Lüders,** Et Al; Online Opportunities and Risks for Children (pp.123-134)

	underlying purpose is manipulative; They may seek to persuade the child to perform sexual or other abusive acts online using a webcam or other recording device or they will try to arrange an in-person meeting and physical contact; Disclosure of personal information or sharing the real time location of a child leading to the risk of physical harm through real-life encounters with online acquaintances with the possibility of physical and sexual abuse, child trafficking and exploitation, blackmail or unwanted sexual advances.
Conduct Risks	Where children are victims or perpetrators in peer-to-peer exchanges e.g. bullying, revenge porn, self-harm, destructive and violent behaviours such as "happy slapping".[18] Exposures to radicalisation, racism, tribalism, hate speech and other discriminatory materials and images; Misrepresentation of a person's age - either a child pretending to be older to gain access to age-inappropriate sites or by an older person for the same reason; Inappropriate conduct – Children and adults may use the Internet to exploit other people; may sometimes broadcast hurtful comments or embarrassing images for defamation and damage to reputation or may steal content or infringe on copyrights; Criminal attempts to impersonate Internet users, primarily for financial gain. In some instances, this might include identity theft, although this is normally associated with attempts to defraud adults.

[18] the practice whereby a group of people assault a stranger at random while filming the incident on a mobile device, so as to circulate the images or post them online

Contract (or Commercial) Risks	Where children are exposed to inappropriate advertising, marketing schemes or hidden costs e.g. targeted advertising, fraud and scams. Some companies spam children through virtual world sites to sell products. This raises the issue of user consent and how this should be obtained; Infringement of their own or the rights of others through plagiarism and uploading of content (especially photos) without permission; Infringement of other people's copyright e.g. by downloading music, films or TV programmes that ought to be paid for; Targeting through spam and advertisements from companies using Internet sites to promote age and/or interest-targeted products; Unauthorised use of credit cards: the credit cards of parents or others which can be used to pay for membership fees, other service fees and merchandise; Use of parent's email account without consent: when parental consent is required to activate an account in virtual world sites for children, children may abuse access to the accounts of their parents. Some services accounts can be difficult for parents to delete once activated.

Risks to children online tend to feature more heavily in popular media than do opportunities. An analysis of media coverage of children and the Internet showed that 64% of coverage was on risks versus 18% on opportunities, with the most widely covered risks being pornography and cyberbullying.[19]

[19] **Livingstone, S.** et al. (2011), Risks and Safety on the Internet: Full Findings and Policy Implications, http://eprints.lse.ac.uk/33731/.

The Child Online Safety Index (COSI)[20] measured the level of online safety for children across the world based on six pillars: Cyber Risks, Disciplined Digital Use, Digital Competency, Guidance & Education, Social Infrastructure, and Connectivity. Its evaluation placed Nigeria on 18th overall position out of the 30 peer countries surveyed. [21]

Summary	NIGERIA Rank	NIGERIA Score	GLOBAL Average Score
Overall DQ	18	38	42
Cyber Risks	18	40	50
Disciplined Digital Use	7	74	49
Digital Competency	13	64	51
Guidance & Education	10	70	52
Social Infrastructure	15	50	51
Connectivity	29	4	50

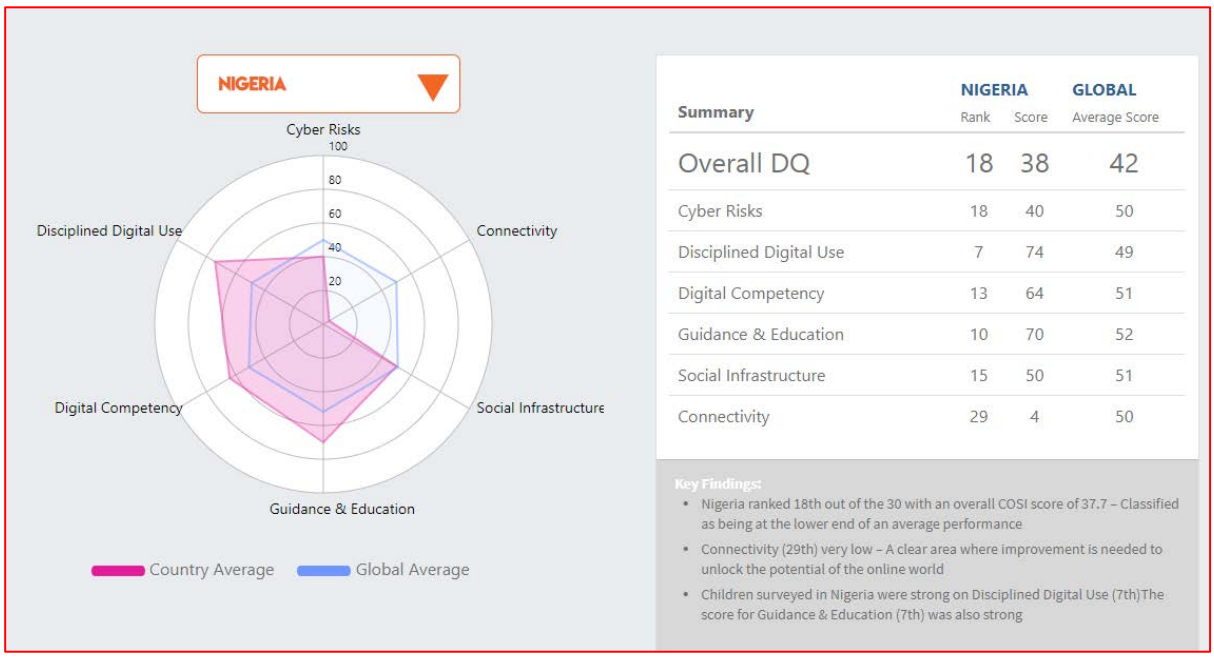


Figure 14: Nigeria's Overall Digital Quotient (DQ) Peer Rating; Source: DQInstitute

[20] Produced by DQInstitute in association with World Economic Forum
[21] DQ Impact Report; https://www.dqinstitute.org/child-online-safety-index/

3.22 What Are The Online Threats?

The survey discovered that unwanted sexual approach in a chat room, social networking site or email is considered as the biggest threat online by 97% of the 11-16 year-olds in Nigeria. This is followed closely by being sent sexual images or content at 89%.

Cyberbullying incidentally, is not a threat rated highly by the children as only 30% considers it a threat worth worrying about. The children also do not consider the possibility of someone taking unwanted photos of them and circulating them online as a major concern hence only 35% put it forward as a threat.

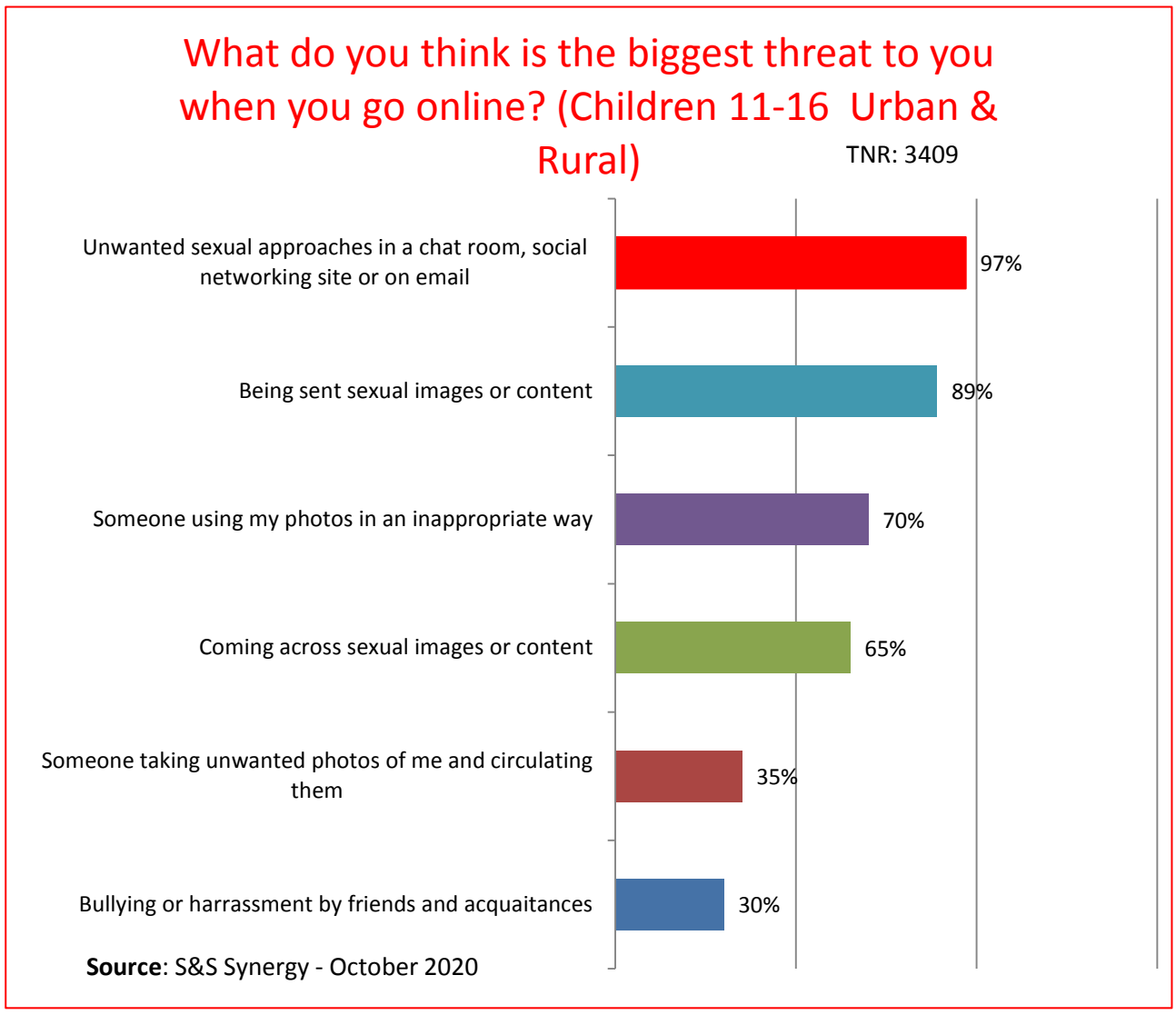


Figure 15: Children 11-16 Years-Old's Assessment of Online Threats

Parents and teachers rated unwanted sexual approaches in a Chatroom on social media or email and being sent sexual images or content or children coming across sexual images or content as some of the biggest threats children deal with online.

Interestingly, parents do not take the threat of bullying or harassment by friends and acquaintances as seriously as the teachers do.

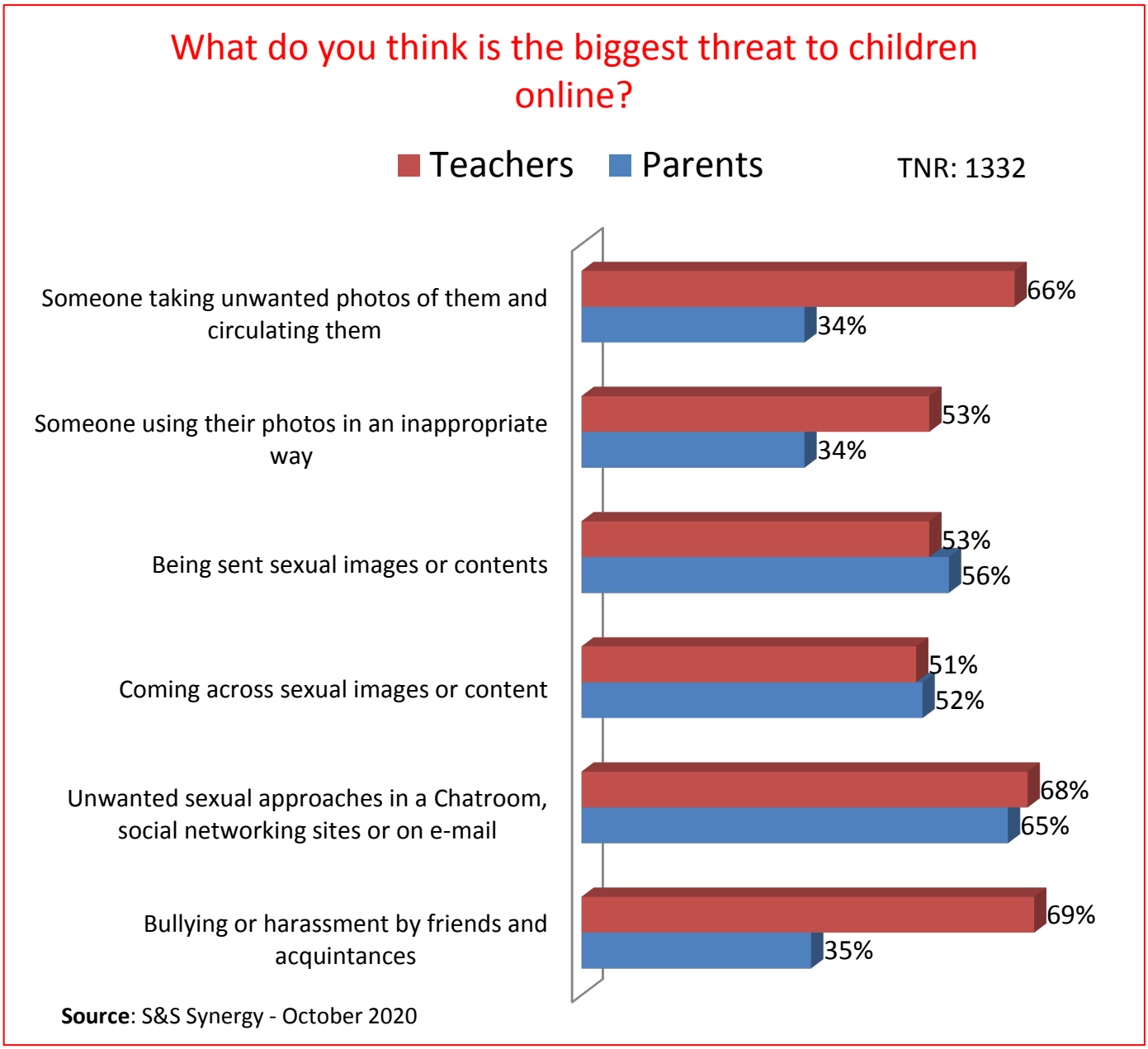


Figure 16: Parents and Teachers Perception of Online Threats

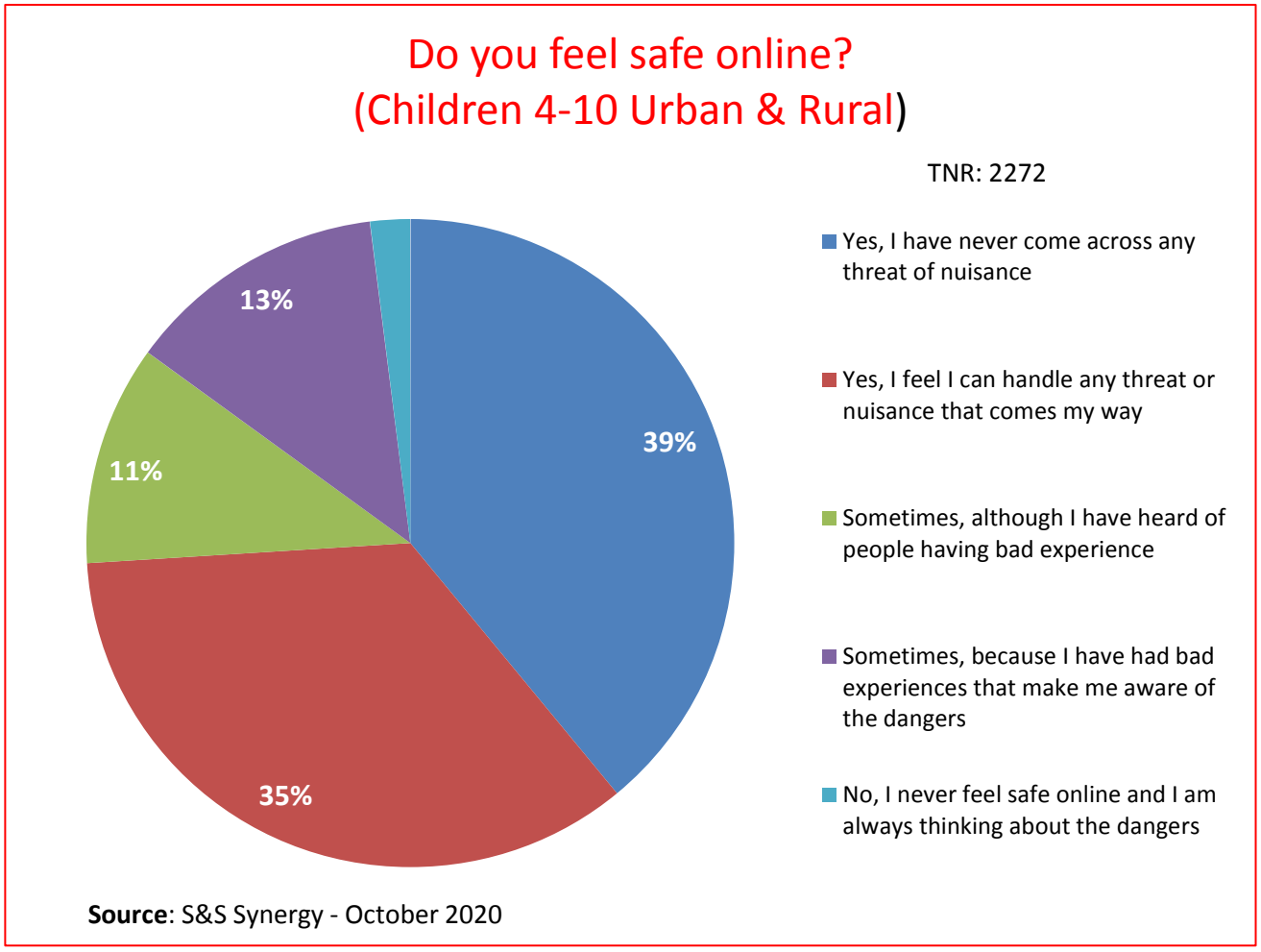


Figure 17: Children's perception of online risks (4-10 Years Old)

A higher number of the 4-10 years-old (39%) than the 11-16 years-old (9%) responded in the affirmative that they feel safe online. Maybe because children aged 4-10 have little comprehension of the risks and threats the Internet inherently embodies; their favourite activities are gaming and video watching on a variety of devices that sometimes are Wi-Fi connected. In general children of this age have limited or no perception of online risks, although some of them have already encountered inappropriate age content.

Perhaps, because they have had previous experience that makes them aware of the online dangers, 28% of the 11-16 years-old and 13% of the 4-10 years-old said it is only sometimes that they feel safe online, while 25% of the 11-16 year-olds does not feel safe online as they are always thinking of the dangers.

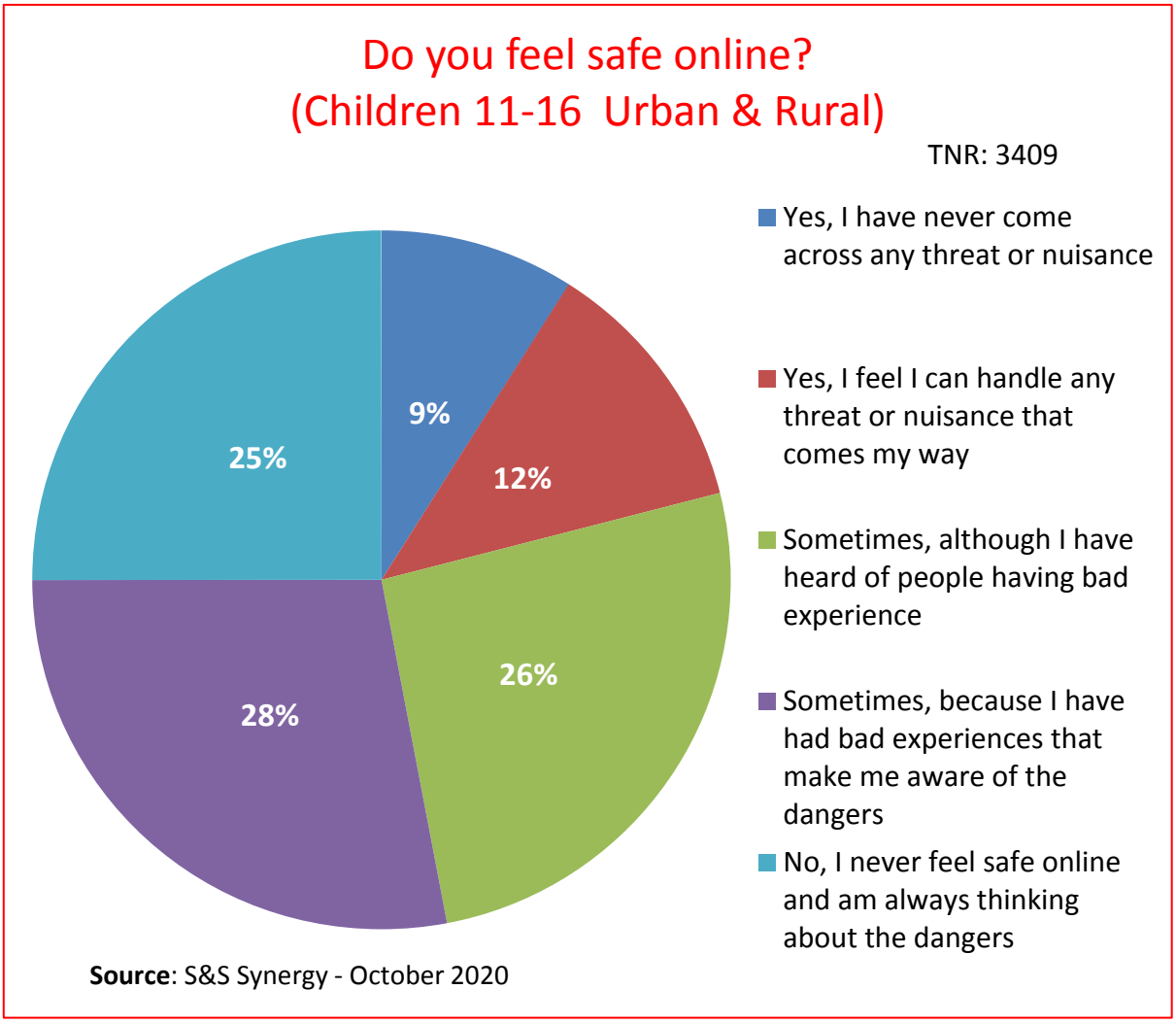


Figure 18: Children's Perception of Online Risks (11-16 Years Old)

The high number of children that don't feel safe online speaks to the urgency of the Government, Industry, regulator, and consumers collaborating to make the Internet not so scary place for the children.

3.23 Offline Challenges

The risks children face offline fall into three broad categories namely social, physical and mental as fully described in the table below.

Table 8: Categories of Offline Risks

Category	Description
Social Challenges	Compulsive and excessive use of digital technology especially Internet or console gaming, to the detriment of social and outdoor activities important for health, confidence building and general wellbeing can result in anti-social behaviour such as withdrawing from friends and isolation; When children use more social media they experience greater loneliness; when they try to seek out peer approval online through image-hosting social media sites, they are more likely to report superficial friendships, damaging their capacity to form strong bonds with their friends;[22] also having more friends on Facebook could predict clinically relevant symptoms of narcissism, and histrionic personality disorder.[23]
Physical Challenges	Excessive screen time also inhibits social skills development in children. When children did not use digital technologies for a few days, they were much better at identifying the emotions of strangers.[24] However, there is an increasing trend of replacing face-to-face interactions with computer-mediated communication; Lack of physical exercise, obesity, ailments with their eyes, hands, arms and backs are real negative impacts children face. When children have poor sleep, it affects their physical and mental health. A child's bad sleep is

[22] **Shawn M Bergman**, Et Al; Millennials: https://doi.org/10.1016/j.paid.2010.12.022
[23] **Larry Rosen,** Et Al; "iDisorders" https://psycnet.apa.org/record/2013-00251-001
[24] **Shamael Ali**; Relationship Between Technology Use and Development of Social Skills

	associated with lower self-esteem as well as increased levels of depression and anxiety.[25]
Mental Challenges	Children experience a decline in both quality and quantity of sleep when they become dependent on their devices.[26] Excessive use of the digital technology can have negative impacts for children including, behavioural changes: less sleep, less reading and less socialising. In particular, when children have access to technology such as a TV or mobile phone in the bedroom, important activities such as reading and sleeping are displaced due to the tendency for children to overuse such technologies;[27] Greater social media use is associated with poor mental and physical health as well as poor interpersonal relationships, and low happiness.[28] The situation gets worse when children are exposed to cyberbullying or other cyberrisks. There is a significant association between cyberbullying, being bullied and depression and suicide;[29] In fact, for children, almost every type of technology use predicates psychological issues, behaviour concerns, attention problems and physical health problems. This is extended to overall mental health. Adolescents who use more than 4 hours of social networking websites per day have worse mental health including higher levels of distress and suicidal thoughts.[30]

[25] **Heather C Woods**, Et Al; Sleepyteens: https://pubmed.ncbi.nlm.nih.gov/27294324/
[26] **Larry Rosen**, Et Al; Sleep Health: Journal of the National Sleep Foundation
[27] **Douglas A. Gentile**, Et Al; Bedroom media: One risk factor for development
[28] **Hugues Sampasa-Kanyinga,** Et Al; Cyberpsychology, Behaviour, and Social Networking
[29] **Mitch Van Geel**; Cyber-bullying: https://jamanetwork.com/journals/jamapediatrics/fullarticle/1840250
[30] **Larry Rosen,** Et Al; Computers In Human Behaviour, 35, 364-375

3.24 Exposure to Threats Online – Why Children Feel Unsafe Online

The Study found that 90% of 4-16 year-olds across the country has been exposed, at least once, to one or more of the rampant cyberrisks. This level of exposure has prompted some sector practitioners to declare that children globally are in the middle of a cyberrisks pandemic.[31]

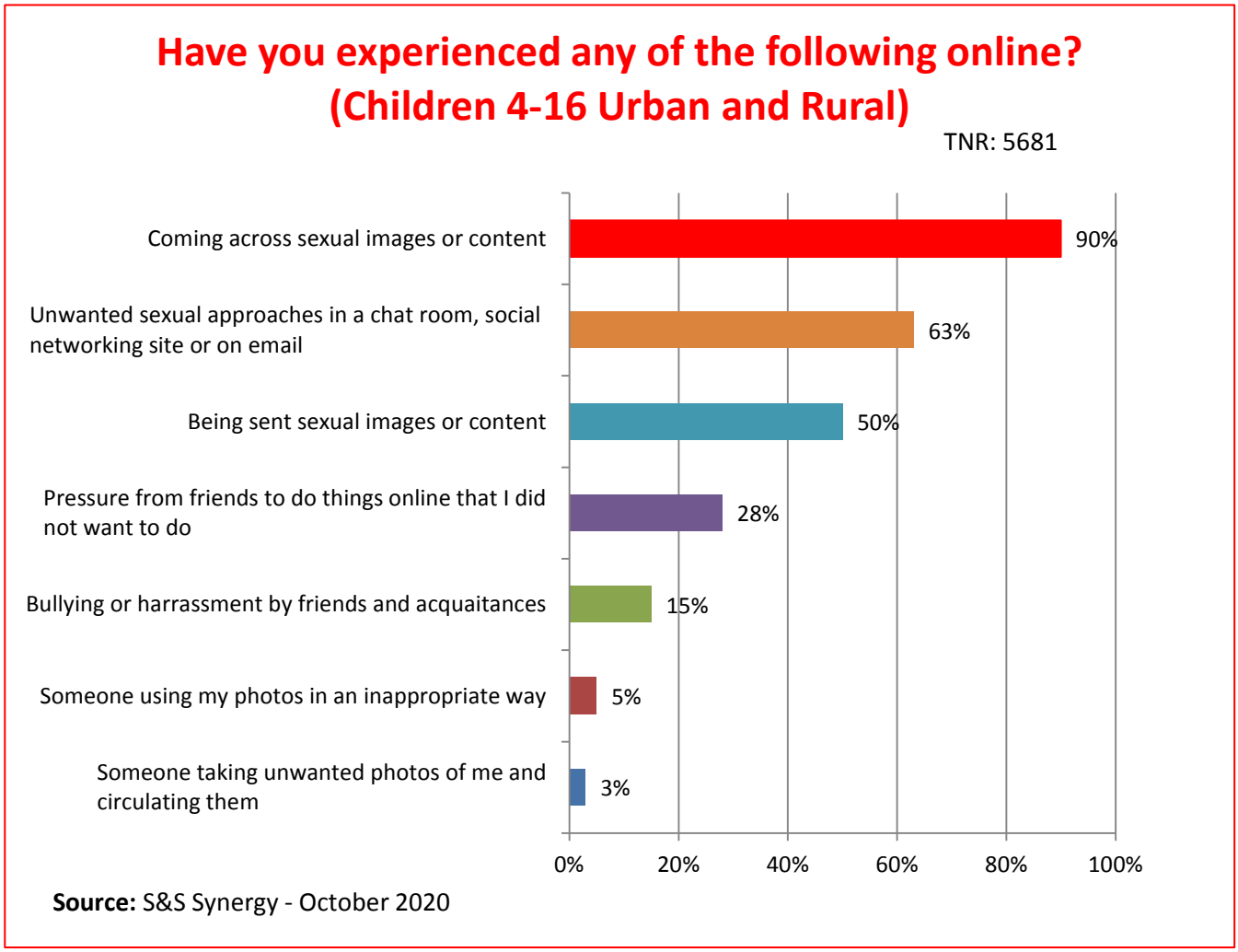


Figure 19: Children's Experience of Threats Online

Continuous exposure to these risks poses a danger to the overall development, well-being, relationships and future opportunities for children online. An illumination thrown up by the Study is that the cyberrisks pandemic is more virulent in developing countries than in advanced countries. The Study revealed that children from the less

[31] https://www.dqinstitute.org/2018dq_impact_report/

developed countries are 1.3 times more likely to be involved with cyberrisks compared to those from advanced countries.[32]

This disparity could be traced perhaps to the advanced countries having more experience and built-in social infrastructures to deal with computer-generated challenges, such as enhanced public awareness and online protection policies and practices, while developing countries leapfrog into mobile technology directly with neither awareness nor preparation to protect children from cyberrisks.

The Study also reveals that mobile phone ownership alone does not always affect a child's exposure to cyberrisks or excessive screen time. Potentially harmful exposure occurs mainly when children are active users of social media as well.

Children who own mobile phones and actively engage in social media have 70% likelihood to be exposed to at least one cyberrisk including cyberbullying, privacy invasion, hacking, digital misinformation, video game addiction, offline meetings and online sexual behaviours.[33]

In the wake of the Covid19 pandemic, it is not uncommon for children to be required to use the Internet for their schoolwork. The Study discovered that children spend an average of 32 hours per week in front of digital screens. This is longer than the time children spend in school.

When children own personal mobile phones, they start to get unlimited access to the digital world at any time and almost anywhere. Even young adults are accustomed to continue checking their mobile phones, and even a single day without access can be anxiety producing.[34]

Watching videos, listening to music, communicating with friends and family, visiting social networking sites and playing online games top the list of activities that children do on a daily basis.

[32] https://www.weforum.org/our-impact/helping-young-people-safely-navigate-the-digital-world
[33] Children in a Digital World; https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf
[34]**Marcello Russo,** Et Al; https://sloanreview.mit.edu/article/surviving-a-day-without-smartphones/

Notwithstanding that some literature term children as “digital natives”, suggesting that since children grew up surrounded by devices and gadgets they would know how to use them, it is evident that children being online or having access to online tools, does not mean that they have all the skills or sufficient knowledge to be safe and effective Internet users, or to exploit the benefits of being online.[35] Despite their early and frequent exposure to technology, it is important to keep in mind that children need guidance on safe and responsible uses of technology.

It is also important to note that although there is a lot of emphasis on the negative aspects of digital technology use by children such as risks and maladaptive behaviours it is crucial to expand the knowledge base on the different online opportunities children can harness, both in personal and educational settings.

3.25 Reputational Risks and Cyber Threats

In an age of trolling, coupled with the ubiquity of smartphones, CCTV cameras and varieties of recording equipment, a person is only one click away from digital disgrace.[36] Offline actions have been known to incur online consequences. For instance, the beauty queen who went viral for alleged inappropriate use of a cucumber[37] or the Senator caught on camera assaulting a shop assistant.[38]

Social media undoubtedly expands the spectrum of reputational risks. Without meaning to, children do share more online than they should. Little do they know that photos, videos and comments made online usually cannot be taken back once they are posted. Even when a child thinks something has been deleted, it can be impossible to completely erase it from the Internet.

[35] **Helsper, E.** and **R. Eynon** (2010), “Digital natives: Where is the evidence?” British Educational Research Journal, Vol. 36/3, pp. 503-520, http://dx.doi.org/10.1080/01411920902989227.
[36] **Sue Scheff**; Shame Nation: The Global Epidemic of Online Hate
[37] https://dailypost.ng/2017/06/29/miss-anambra-sex-scandal-happened-chidinma-okeke/
[38] https://www.vanguardngr.com/2019/07/senator-caught-on-camera-assaulting-woman-at-sex-toy-shop/

Posting an inappropriate photo can damage a reputation and cause problems years later such as when a potential employer or school admissions officer does a background check.

Nigeria is placed third from the top on the COSI on Reputational Risks, way above the global average, indicating that not many children in Nigeria have experienced cyber shaming or have risked harming others' reputation online.

Figure 20: Nigeria's Peer Rating on Reputational Risks; Source: DQInstitute

According to UNICEF, one in three young people has been a victim of one online cybercrime or another with social networks such as Facebook, Instagram, Snapchat and Twitter, as the most commonplace for online bullying.[39] Cyberbullying is the use of information and communication technology, for the harassment or mistreatment of another. It includes posting repetitive offensive comments or photos on social media and or

[39] https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying

creating fake online profiles to belittle another person. It sometimes involves death threats and "doxing".[40]

The Cybercrimes (Prohibition, Prevention, Etc.,) Act 2015, explicitly forbids people from knowingly transmitting any communication to bully, threaten or harass another, causing fear, violence or bodily harm.[41]

More examples of cyber threats confronting children online include phishing,[42] hacking, Trojans,[43] Drive-by-downloads[44] and perhaps malware.[45] Stories abound of users having their accounts hacked, especially Facebook, Instagram and emails by cyber-fraudsters snooping for people's personal details to use for their nefarious activities.

The Nigerian child already imbued with the socio-cultural awareness of the '419' syndrome[46] would come online subconsciously ready to fish out most phishing attempts. By implication, children in Nigeria, while not being the most proficient in the world, tend to have an enhanced level of awareness about some of the numerous insecurities lurking online.

Many Nigerian children even practise reverse mediation, whereby children very often help their parents when they find something difficult on the Internet indicating a continuing generational gap where parents lag behind their children in digital skills. Or more positively, it may suggest that parents are not afraid to let their children help them manage their digital environment.

[40] **Doxing** - to search for and publish private or identifying information about a particular individual on the Internet, typically with malicious intent
[41] Section 24 - The Cyber Crimes (Prohibition, Prevention, etc.,) Act, 2015
[42] **Phishing** is when a cybercriminal attempts to lure individuals into providing sensitive data
[43] A **Trojan** creates a backdoor in a system, allowing the attacker to gain control of the computer
[44] A **drive-by download** is a download that happens without a person's knowledge often installing a virus
[45] **Malware** is software that does malicious tasks on a device such as corrupting data or taking unauthorised control
[46] **419** advance fee fraud - derives from the section of Nigerian law that con artistry and fraud come under

3.30 Objective Three –Effective Online Barriers

3. How may effective online barriers be established to mitigate the challenges without undermining the openness of the Internet and its fundamental values?

3.31 Key Findings

Balancing children's online opportunities and risks remains a challenge for all stakeholders in the child online ecosystem including the Government, Industry, parents, teachers and the children themselves. Without unduly exaggerating the dangers, it is essential to discuss openly the risks that exist with children and digital technology and even more importantly to empower the children to recognise the risks and be better equipped to prevent or deal with the harms if they should occur. As indicated, while efforts to promote opportunities for children online must continue to be a priority, this must be carefully balanced with rights to safe conditions under which they can participate in and benefit from the digital world.[47]

Similarly, it is crucial that the concern to protect children online is not allowed to become a platform to justify an assault on such fundamental human rights as free speech, free expression or the freedom of association.

To be safe users of digital technology, children must be aware of their rights. This empowers them to recognize when something is wrong to alert a responsible adult, and to be able to report a violation of their rights. For this to happen, teachers and parents must also understand

[47] ITU News (2018), Celebrating 10 Years of Child Online Protection, https:// news .itu .int/ celebrating -10 -years -child -online -protection/ .

the rights of children online and be able to pass them on, in a language that is appropriate to each child's age.

3.32 Using technology and software to establish barriers

To create effective barriers against online abuse and exploitation, all relevant agencies and organizations including private companies that provide online services must use the full range of suitable technologies available to close the technical gaps that make it easy for abusers to operate online. The right system plays a crucial role in preventing harms and flagging serious behaviour for the attention of human moderators.

Software and solutions already exist to help private companies, regulators and law enforcement detect, report, and otherwise act against sites and services hosting child sex abuse materials (CSAM). Many of these solutions are highly automated and use hashing algorithms to minimize the exposure of staff to harmful content. Many are also available at little or no cost.

They include:

- Blocking technologies: usually operating at the ISPs' level, blocking technology recognizes and blocks content or sites that promote harm to children;
- Heuristic filtering: technologies that look at variables such as the IP address, content, and keywords and block sites that are not blacklisted but may contain harmful content;
- Automated CSAM detection: using solutions, such as classifiers that reference hashed blacklists of CSAM, providers can instantly spot, block, and/or report child-abuse content;
- Web crawlers: looking for the same variables as filters (keywords; CSAM images etc.), web crawlers actively search for harmful sites then alert authorities;
- Facial recognition: using facial-recognition technology, authorities and other actors in the sector can quickly identify known victims and perpetrators;
- NetClean ProActive: software based on signature matching and other detection algorithms, which automatically detect child sexual abuse images and videos in enterprise environments;
- Thorn's Safer: a tool that can be deployed directly onto a platform to identify, remove, and report CSAM;

- Griffeye Brain: an AI that scans previously unclassified content compares it with the attributes of known CSAM content, and flags suspect items for review by an agent;
- PhotoDNA: a tool that creates hashes of images and compares them to a database of hashes already identified and confirmed to be CSAM. If it finds a match, the image is blocked.

Digital technology does not have one responsible stakeholder, it has many. From the Government, to regulators, law enforcement agencies, businesses, the tech sector, academia, teachers, families, parents and children themselves. Child online protection relies on all of these stakeholders working in partnership, each taking a part of that responsibility, each doing what is necessary to protect children and build a safer Internet ecosystem for all.

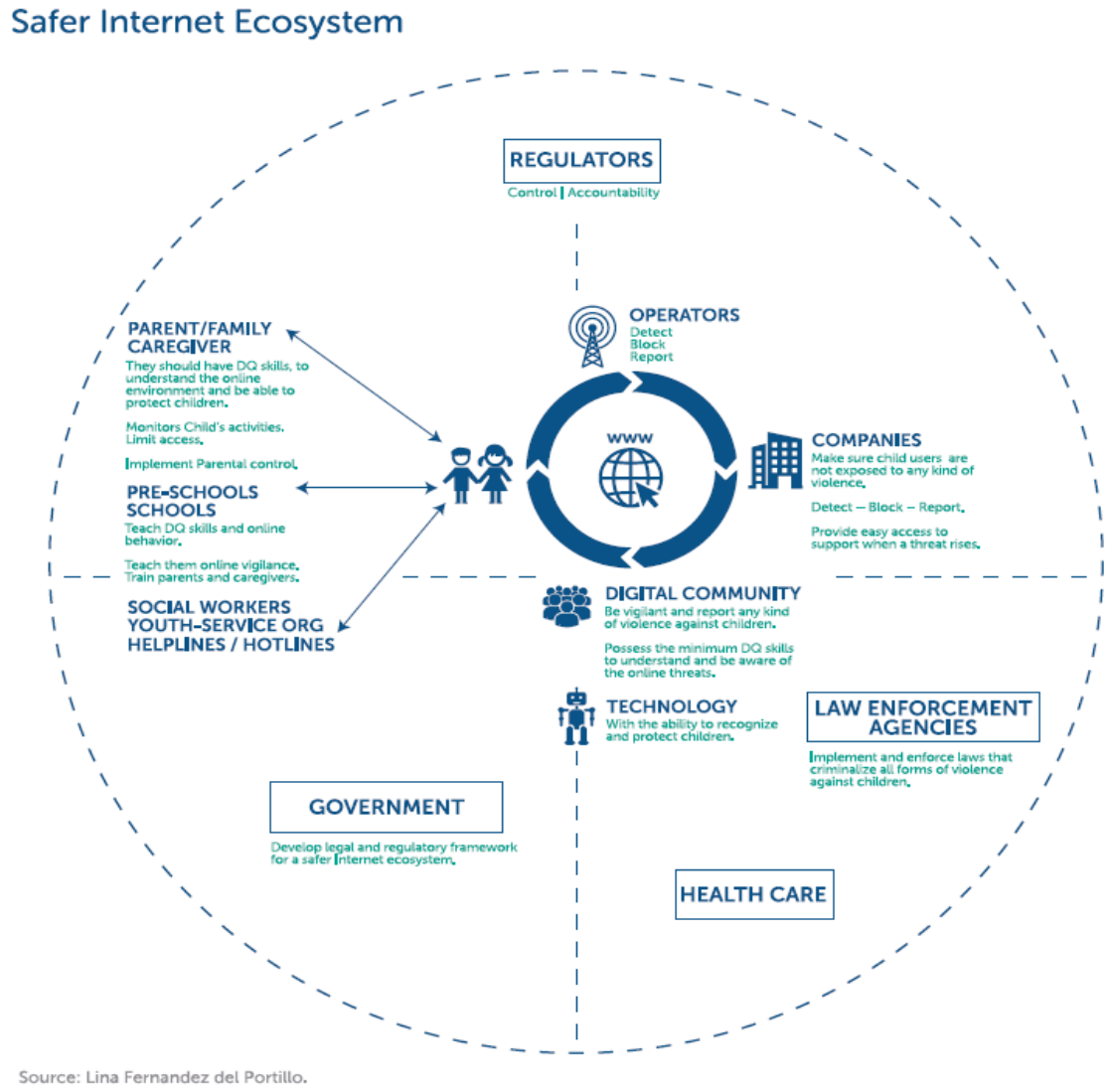


Figure 21: Stakeholders in the Safer Internet Ecosystem

3.33 Privacy Management and Critical Thinking as Effective Barrier

"The Internet never forgets and the public never forgives" should be the guiding code to every child online. Information disclosed on social network sites are persistent, can be easily accessed, spread and replicated.[48] Disclosures on SNS may result in a negative experience and even harm if published information and materials are in some way misused.

The best way to counter the blight of Internet history is self-censorship, balancing between disclosures and concealments, striving for the most positive outcomes but, at the same time, fearing potential risks.[49]

Even though youth in Nigeria seem to be savvy social media users, they still need to develop the cognitive, social, and digital skills required to sustain optimal levels of online privacy.

Mobile and social media use have transformed when and how children interact with others. The ability to instantly share thoughts, feelings and behaviours with the rest of society via digital channels can occur often without the empathetic social filter that accompanies traditional communications.

Digital communications are devoid of many of the emotional signals and cues experienced in face-to-face settings, often leading to more impersonal interactions.[50] It is crucial therefore, that Nigerian children develop critical thinking capabilities. This is the process of thinking carefully about a subject or idea, without allowing feelings or opinions to affect one's judgement. It is an important skill that all online children need to navigate the Internet safely and find accurate facts and information.

With the vast assortment of content online, it is increasingly possible for a young person to consume material without consideration as to how reliable it is. Being a critical thinker doesn't presuppose rejecting all information the child encounters. It portends not accepting information

[48] **Danah Boyd**; "Privacy and Publicity in the Context of Big Data
[49] **David Siesage**; The Internet Never Forgets, So Be Careful What You Put On It
[50] **Joseph B Walther**; Theories Of Computer-Mediated Communication And Interpersonal Relations

immediately at face value, weighing up what they know to be true, asking questions, forming judgements and checking with others if they are unclear.[51]

3.34 Proficiency in Screen Time Management as Effective Barrier

Screen time can be the best time for kids to learn and practice the skills they need to be successful in school and life. It encompasses all the activities that involve screens such as watching television, playing video games, texting and chatting online with friends and working on a computer.

Existing guidance in managing children's screen time may not be as beneficial as first thought. An Oxford University research paper disputes digital device use guidelines for teenagers and proposes that a moderate amount of screen-time, known as the 'Goldilocks'[52] period, might boost teenage wellbeing; suggesting that in the broader family context, how parents set rules about digital screen time, and if they are actively engaged in exploring the digital world together, are more important than the raw screen time.[53]

One finding of note is that digital screen use increases with age, is higher in boys, children with less-educated parents and children from less affluent households.[54]

3.35 Online and Offline Privacy Management as Barrier

Despite the many opportunities of being online, digitally engaged children are exposed to various cyber risks. Exposure to sexual, violent or hateful content and risks associated with personal disclosure such as giving out personal information appear quite frequently. Contact as well as conduct risks vary in incidence. While bullying online and receiving or sending sexual messages seem quite normal, meeting online contacts offline is less common.

[51] Critical Thinking - https://www.childnet.com/teachers-and-professionals/hot-topics/critical-thinking
[52] **Goldilocks** - not being extreme or not varying drastically between extremes
[53] https://www.ox.ac.uk/news/2017-12-14-children%E2%80%99s-screen-time-guidelines-too-restrictive-according-new-research
[54] **Allen Nnanwuba A**; The Displacement Effect of Screen Time among In-School Adolescents in Nigeria

With the increasing importance of social media in children's daily lives, asking them to stay away from such activities seems increasingly futile. It may be much more reasonable to emphasise risk management over risk avoidance – even for the 4-10 years-old children. This may offer the best protection while also allowing the children to take full advantage of the opportunities the Internet offers.

Being discerning about the granularity of the personal identification information (PII) children publish on their social media accounts is one way of establishing safety barriers against contact risks.

The survey (see Figure: 22) revealed that up to 45% of the children put their full names and correct dates of birth online inadvertently setting up a treasure trove akin to a goldmine for cybercriminals sniffing about for just such complete information.

Interestingly, 55% of the children admitted inputting an age that is not their real age. This perhaps accounts for the high number of children in the 4-10 years-old group that have social media accounts despite the minimum signing-up age of 13 that most social media sites stipulate.

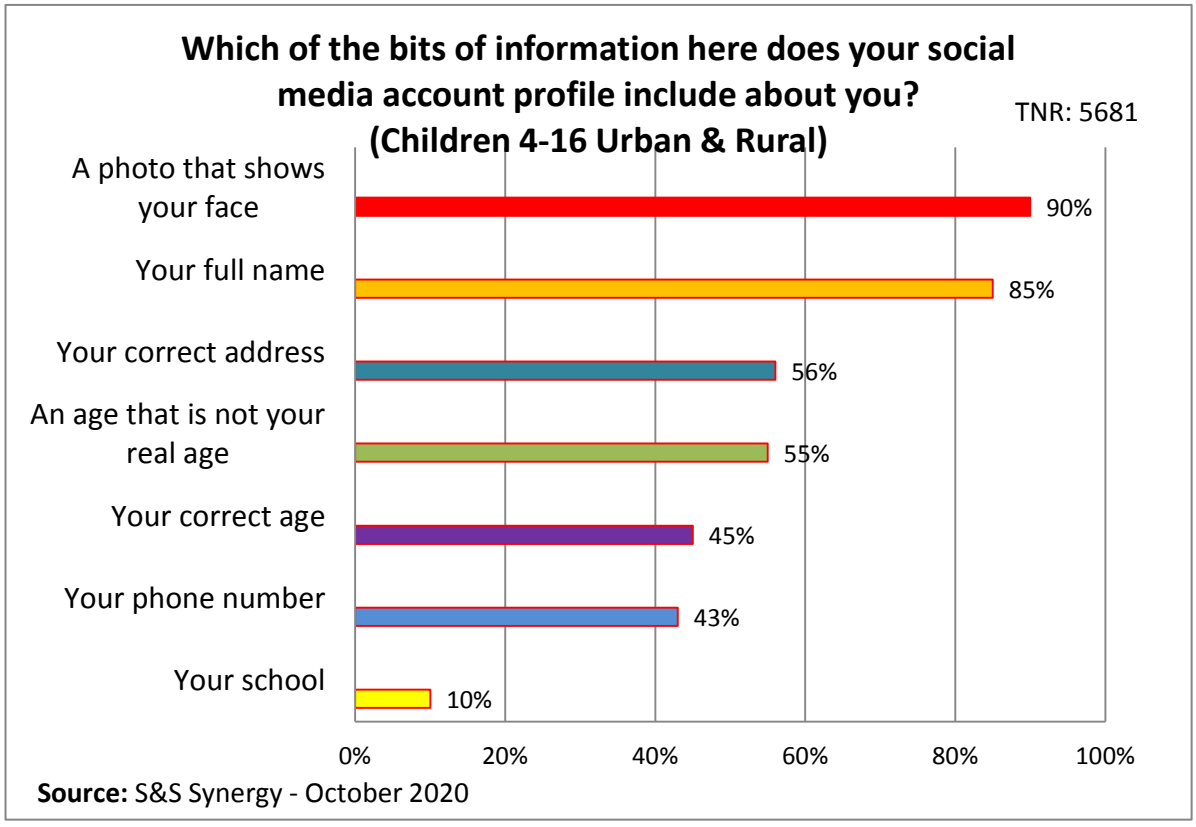


Figure 22: Personal Identification Information Children Display Online

So from an average social media account of a child, a savvy cyber-stalker can obtain the photograph, full name, correct address, phone number and date-of-birth of his prospective victim without much effort.

From the survey a pattern of carefreeness is discernible as even offline children dispense their PII to strangers in numbers that are high enough to be regarded as risky. This behaviour, unbeknown to the children, portends real risks to the security of their personal data and physical safety.

Forty-five percent of the children had sometime shared their home address offline with a stranger and 55% had similarly shared their age.

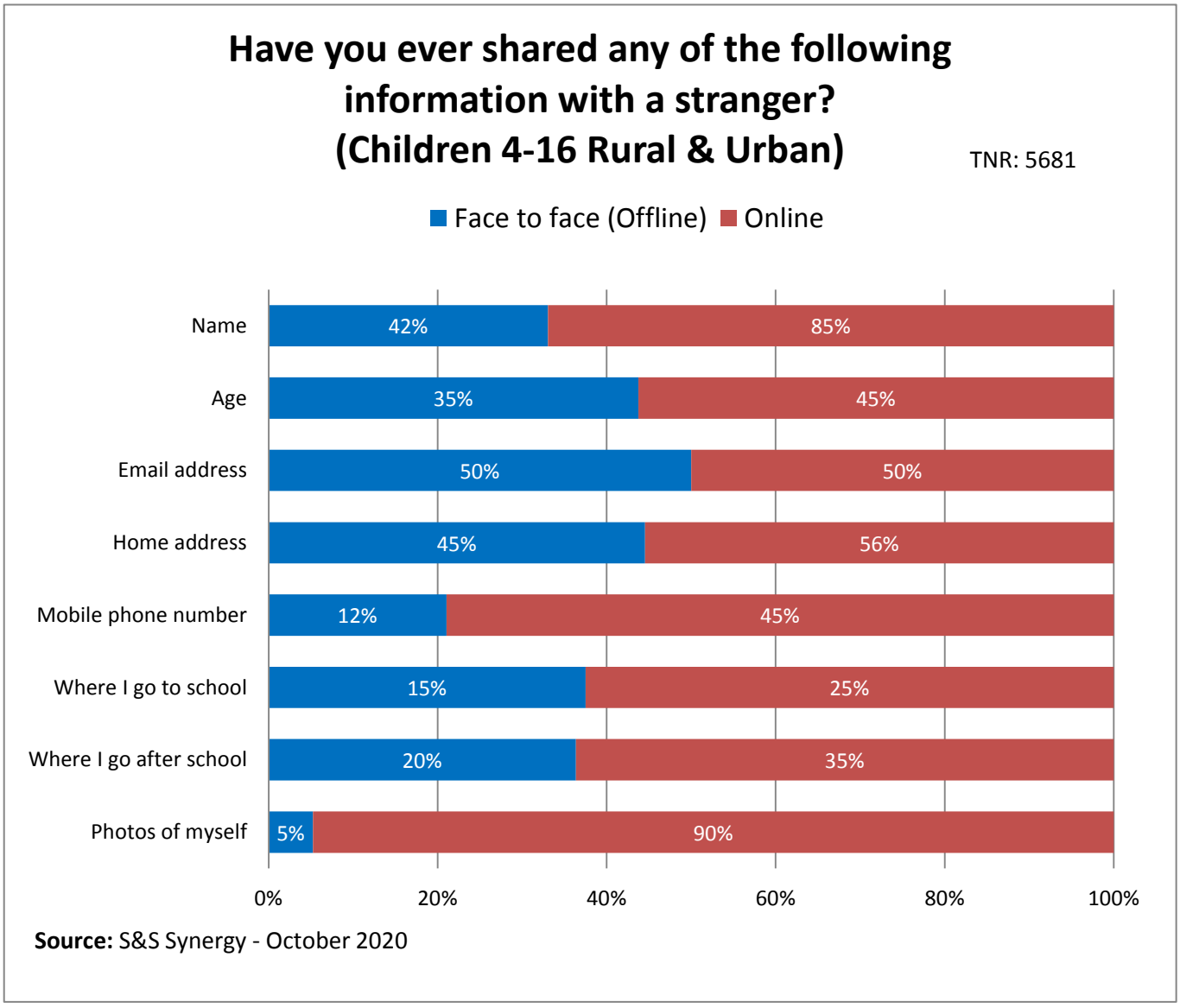


Figure 23: Offline and Online Sharing of PII

3.35 Digital Footprint Management as a Barrier Tool

While digital footprints are considered to be a liability, if managed well they can be an asset. Digital footprints can showcase identity, skills and interests. This is important in an era where employers "google" candidates to check their identity and verify their suitability.[55] In this context, having no digital footprint can be as much of a disadvantage as having a poorly managed one.

Proficiency in digital footprint management entails knowing what to display publicly and what should remain private. Digital artefacts such as school projects, awards and pieces of writing which demonstrate the child's interests, achievements and skills could be both public and identifiable.[56]

Almost all social media platforms harvest one form of PII or the other from the children. These personal pieces of information range from name, date-of-birth and phone number.

The online collection of personal data occurs in the context of online behavioural advertising (OBA). OBA consists of tracking users' behaviour online through the collection of unique identifiers and using the information obtained to identify patterns for building a profile of the data subject to send targeted advertisements to the individual that are consistent with his interests.

For example, Facebook uses the data obtained from users of its social network to provide more targeted markets for advertisers;[57] Google, in analysing the search queries of users of its search engine service, can identify the interest of users or websites visited, as a commercial basis for targeted advertisement.[58]

[55] **Rachel Buchanan;** How To Help Children Build A Positive Presence Online
[56] https://www.weforum.org/agenda/2018/01/why-children-should-be-taught-to-build-a-positive-online-presence
[57] **Cassandra Liem,** Et Al; The Economic Value of Personal Data for Online Platforms, Firms and Consumers
[58] http:// bruegel.org/2016/01/the-economic-value-of-personal-data-for-onlineplatforms-firms-and-consumers/

Another application of personal information collected by online platforms is in the context of predictive analysis, which enables the extraction of huge amounts of information.[59]

To ensure that the Nigerian child does not disclose too much information about himself too early and too often, it is essential to equip him with the required digital literacy to demonstrate discernment when asked about his personal details be it online or offline.

It is illustrative to outline (see Table 6) some of the PII routinely collected and stored by social networking sites and apps.

Table 9: Types of PII Collected Online

Social Networking Site \ Website URL	Type of Personal Information Collected								
	Name	IP Address	Clickstream Data	Date of Birth	Facial Photograph	Location / Address	Telephone number	Email address	Payment card
Facebook	☐	☐	☐	☐	☐	☐	☐	☐	☐
YouTube	☐	☐	☐			☐	☐	☐	☐
Instagram	☐	☐	☐	☐	☐		☐	☐	
Twitter	☐	☐	☐	☐	☐	☐	☐	☐	
WhatsApp		☐	☐			☐	☐	☐	
TrueCaller	☐					☐	☐	☐	
Google	☐	☐	☐	☐		☐	☐	☐	
Yahoo	☐	☐	☐	☐		☐	☐	☐	
LinkedIn	☐	☐		☐	☐	☐	☐	☐	☐
Jumia	☐	☐	☐	☐		☐	☐	☐	☐
Opera	☐	☐	☐			☐		☐	
Netflix	☐	☐					☐	☐	

[59] **Paul M. Schwartz;** 'Data Protection Law And the Ethical Use of Analytics'

3.40 Objective Four – Online Insecurities and Challenges

4. How may the children's ability be developed to deal with online insecurities and challenges?

3.41 Key Findings

Technology permeates everything today's children do. From school to home the perpetual connectivity has caused no shortage of alarm for parents. The children require enhanced digital skills to grow into savvy consumers of digital technology. The teachers, parents and guardians should also have at least basic digital skills enough to help their children derive the maximum benefit from being connected, while also recognizing and appropriately responding to potential harms.

To this end, DQ Institute, an international think-tank dedicated to setting global standards for digital intelligence education, has defined eight key areas of digital competencies that all stakeholders in the child online protection ecosystem should master for children to be safe and have a positive experience online.

All eight competencies are important if a child is to have a fully developed ability to deal with the numerous insecurities and challenges and enjoy full access to his rights online.

These eight areas are:

1. Digital Identity: the ability to create and sustain a positive online identity;
2. Digital Use: the ability to use technology in a healthy and balanced way;
3. Digital Safety: the ability to mitigate a range of online risks;
4. Digital Security: the ability to manage and avoid risks to devices and data;

5. Digital Emotional Intelligence (EQ): the ability to recognize, navigate, and express emotions online;
6. Digital Communication: the ability to communicate and collaborate using technology;
7. Digital Literacy: the ability to find, read, evaluate, create and share digital information; and
8. Digital Rights: the ability to understand and uphold human and legal rights online.

In trials, this approach has been shown to be successful. Children trained in the eight competencies were found to have a 15% lower risk of harm online than children who had not been trained.[60]

These digital competencies are core requirements to equip Nigerian children with a holistic set of digital life skills to become ethical and discerning digital citizens who can proactively mitigate various cyberrisks, while maximizing the potential of technology for both now and the future. The DQ competencies are grounded in universal moral values that will enable children to adapt to the demands of digital life throughout their lifetimes. [61]

Digital Intelligence does not merely refer to the skills needed to use technology more effectively or being aware of potential dangers for children who are constantly online; it is all-encompassing in that it covers all areas of children's digital life ranging from their personal and social identities to their use of technology, their practical, operational and technical capabilities critical for daily digital lives and the potential safety and security issues in this digital age.[62]

DQ is further divided into three distinct levels:

- Digital Citizenship - The ability to use digital technology and media in safe, responsible, and ethical ways which are fundamental digital life skills that every child needs to have;

[60] World Economic Forum (2019) Cyber-risk exposure among 8-12-year olds drops by 15%. [online] Available at: https://www.weforum.org/our-impact/helping-young-people-safely-navigate-the-digital-world
[61] DQ Institute; "What is DQ (Digital Intelligence)?"
[62] **Yuhyun Park**; "DQ Global Standards Report 2019" (PDF) DQ Institute

- Digital Creativity - the ability to become a part of the digital ecosystem and to create new knowledge, technologies and content to turn ideas into reality; and
- Digital Competitiveness - the ability to solve global challenges; to innovate and to create new opportunities in the digital economy by driving entrepreneurship, jobs, growth and impact.

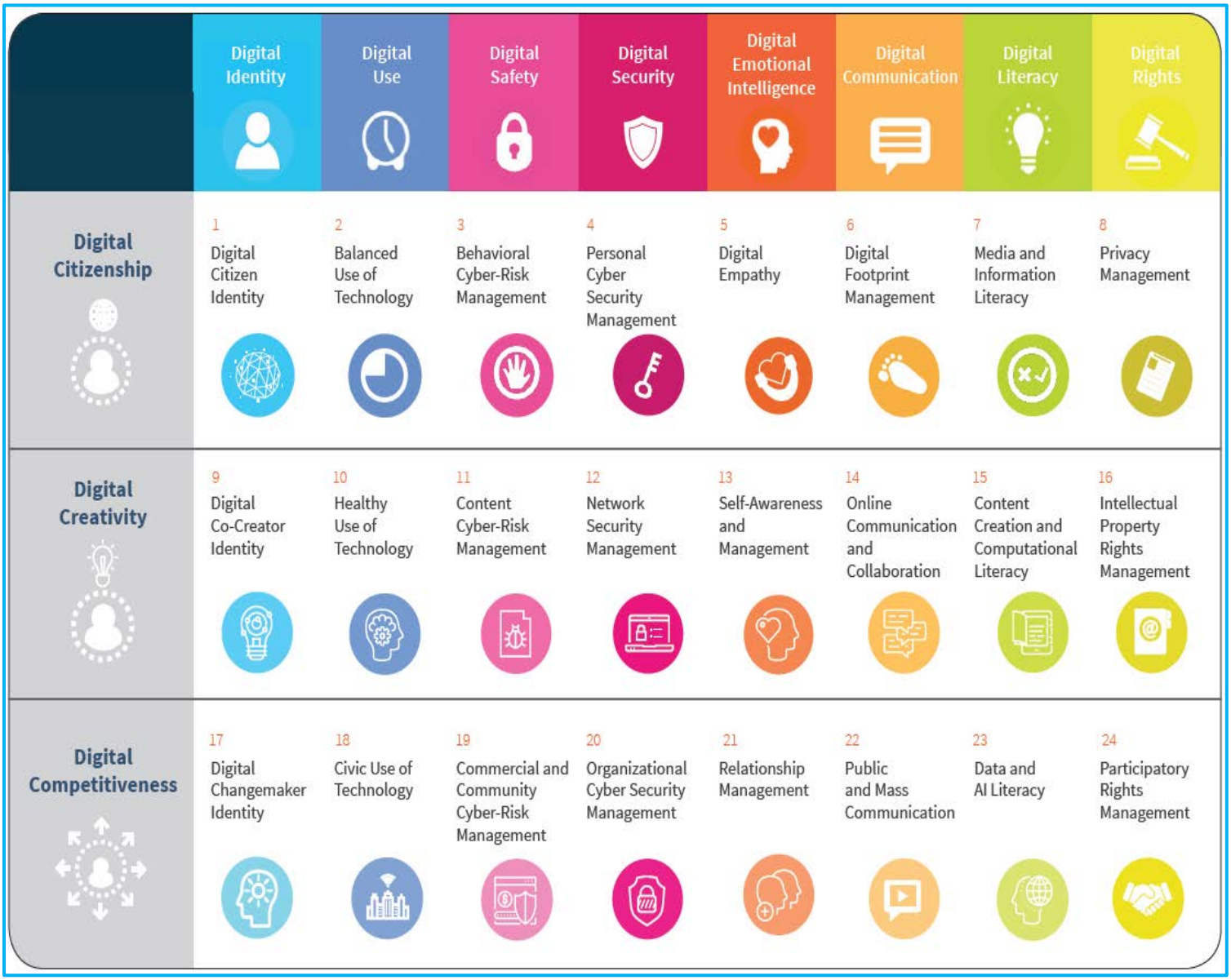


Figure 24: The 24 DQ Competencies; Source: DQInstitute

3.42 The Characteristics of the Digital Competencies

The eight digital competencies are fully described in the table below.

Table 10: Description of the Eight Required Digital Competencies

	Competency	Description	Performance Indicator
1	Digital Identity *Guiding Principle: Respect for oneself*	The ability to build and manage a healthy identity as a digital citizen with integrity.	Children understand the basic vocabulary needed for discussing the media landscapes in which they are embedded; the social and multicultural nature of digital media and technologies; the construction of their self-image and persona in the digital environment; the impact that technology may have on their self-image and values (e.g., body images, gender stereotypes that may be idealized in digital media such as video game or advertising, and racial stereotypes that may be embedded in the system), and how personal use of digital media may have offline implications; Children can demonstrate ethical and considerate behaviour and netiquette when using technology across different audiences, to control and shape their

			own digital identity by creating and curating their online identities to tell their stories while engaging with others from different cultures and possessing global awareness in a way that demonstrates non-discriminatory and culturally sensitive behaviour; Children exhibit coherency and integrity across online and offline behaviours, honesty when using technology and demonstrate self-efficacy by finding ways to take advantage of the opportunities afforded to them online.
2	Digital Use *Guiding Principle: Respect for time and the environment*	The ability to manage one's life both online and offline in a balanced way by exercising self-control to manage screen time, multitasking and one's engagement with digital media and devices.	Children understand the nature and impact of technology use (e.g. excessive screen time and multitasking) on their health, work productivity, well-being and lifestyles, and have the appropriate knowledge to deal with these impacts; Children can assess health risks and reduce technology-related issues

			to better self-regulate their technology usage in doing so, they become able to develop time and resource management skills to more successfully perform tasks and more safely enjoy entertainment; By using technology with purpose-driven intentions, children exhibit integrity by adhering to goals in terms of screen time and technology usage and develop positive relationships through the self-regulated use of technology.
3	Digital Safety *Guiding Principle:* *Respect for life*	The ability to understand, mitigate and manage various cyberrisks through safe, responsible, and ethical use of technology.	Children understand the different types of behavioural cyberrisks (e.g., cyberbullying, harassment, and stalking), how they might encounter these risks, how these risks might affect them, and how they can formulate strategies for dealing with them; Children develop the appropriate technical, socio-cognitive, communicative, and decision-making skills to address behavioural

			cyberrisk incidents as they occur, whether as a bystander or victim and gain valuable coping tools to address these negative online experiences; Children exhibit kindness when online, know the supportive framework in place to address risks and can manage their online behaviour as part of contributing to positive and supportive online communities.
4	Digital Security *Guiding Principle: Respect for property*	The ability to detect, avoid and manage different levels of cyber threats to protect data, devices, networks and systems.	Children understand their online risk profiles and how to identify different types of cyber threats (e.g., hacking, scams, and malware), and also identify available strategies and tools they can use to avoid such threats; Children can identify cyber threats, use relevant cybersecurity practices (e.g., secure passwords, firewalls, and anti-malware applications), and use technology without compromising their data and devices;

			Children exhibit resilience and vigilance against careless or negligent behaviours that may compromise their own or others' data and device security, and have confidence about what to do when there is a problem.
5	Digital EQ *Guiding Principle: Respect for others*	The ability to recognize, navigate and express emotions in one's digital intra- and inter-personal interactions.	Children understand how their online interactions might affect others' feelings and recognize how others may be influenced by their online interactions (e.g., effects of online trolls); Children develop socio-emotional skills by becoming sensitive to and respecting others' perspectives and emotions through synchronous and asynchronous interactions online and can regulate and respond accordingly; Children demonstrate an awareness and compassion for the feelings, needs and concerns of others online.
6	Digital Communications *Guiding Principle:*	The ability to communicate and collaborate with others using technology.	Children understand the concept of digital footprints, the consequences that such

	Respect for reputation and relationships		trails of information and corresponding metadata may have on their reputation and others, and the possible uses of such information when shared online; Children can manage their digital footprints and use technology in a manner that contributes to a positive reputation both for themselves and others; Children exhibit care, prudence and responsibility online to actively manage the types of information that may be shared, tagged, released, gathered, and collected by themselves and others across multiple platforms throughout time.
7	Digital Literacy *Guiding Principle: Respect for knowledge*	The ability to find, read, evaluate, synthesize, create, adapt, and share information, media, and technology.	Children acquire the ability to synthesize, create, and produce information, media, and technology in an innovative and creative manner; Children learn to find, organize, analyse, and evaluate media and information with critical reasoning;

			Children understand how to keep up with advancements in information and communication technology as well as integrate digital technologies into their everyday lives in a way that is complementary and productive rather than disruptive. In turn, they learn to be open to experimenting with new technology and when to reject them. In doing so, they can seek out co-creation opportunities (e.g., new models of products or services) borne from these technology progressions in the digital ecosystem.
8	Digital Rights *Guiding Principle: Respect for rights*	The ability to understand and uphold human rights and legal rights when using technology.	Children understand privacy as a human right, what personal information is and how it can be used, stored, processed and shared in digital platforms along with strategies and tools that help them keep their personal information private and secure;

			Children develop behavioural and technical strategies to limit privacy violations and can make good decisions around creating and sharing information and content of their own as well as that of others; Children show respect for their own and others' privacy and personal information, treating these as valuable and personal assets worth protecting; Children become equipped to develop cognitive and meta-cognitive skills for synthesizing existing legislation with their own practices to ensure that digital rights are upheld and respected online.

3.50 Objective Five – Consultation and Feedback Mechanisms

5. How may feedback or consultation mechanisms for child online protection be developed?

3.51 Key Findings

All the stakeholders, spanning the Government, law enforcement, Industry, parents, teachers and the children recognize that multi-stakeholder collaboration is crucial in establishing the foundation for safe, secure and positive uses of the Internet and associated technologies. They recognize the need for more effective tools that will foster cooperation and improve the feedback and consultation mechanism in the child online protection system. The said tools should be platform neutral, shareable and openly available as described in the table below.

Table 11: Feedback and Consultation Mechanisms

Enabler	Mechanism	Context	Outcome
Cross sector, multi-disciplinary collaboration	An accountable national governance and oversight agency with the suggested moniker National Child Online Protection Commission.	A dedicated agency with mandate to deal with online child protection issues and increased accessibility to children via online technologies including SMS, chat and social media.	Comprehensive understanding of child online protection within the highest levels of Government and law enforcement. Coordination of the efforts of multiple stakeholders to ensure enhanced feedback and response to child
	A specialist team within the Nigerian Police Force – can be titled Child	Unit with national remit; trained officers; victim-focused	

	Protection Force - dedicated solely to online child protection matters.	proactive and reactive investigations with international cooperation. To provide self-help and awareness sensitisation. Will have access to national and INTERPOL CSAM databases.	online protection issues.
	A Federal Offender Management System		Prevent re-offending of those in the criminal justice system nationally. Achieve proper victim-focused investigations and secure positive judicial outcomes; offenders are managed and reoffending prevented.
Supportive Feedback Environment	A national Child Helpline devolved to State level.	A free-of-charge child helpline accessible to all children to report cases and receive support; counselling and information.	The public can proactively report cyber offences against children. Promotes engagement and inclusivity; it is flexible and includes out-of-school children and children with disabilities. Child-friendly where children are treated with respect, understanding and calmness and where they feel comfortable asking questions or giving feedback.
	A national Hotline devolved to State level.	Dedicated hotline to collect information from children as a robust feedback mechanism. Anonymous reporting of offences and crimes against children both online and offline with links to law enforcement and child protection systems.	
	Child Online Protection clubs.		

3.52 Dialogue and Discussion as Feedback Mechanism

Apart from censoring content, it is important that children feel able to talk to someone especially if they are upset, worried or concerned about something that they have seen or that has happened to them online. The survey discovered that many young people are reluctant to speak to an adult about a negative online experience. This reluctance could emanate from the fear of the consequences like being banned from particular sites or devices and being blamed for something that may not have been their fault.

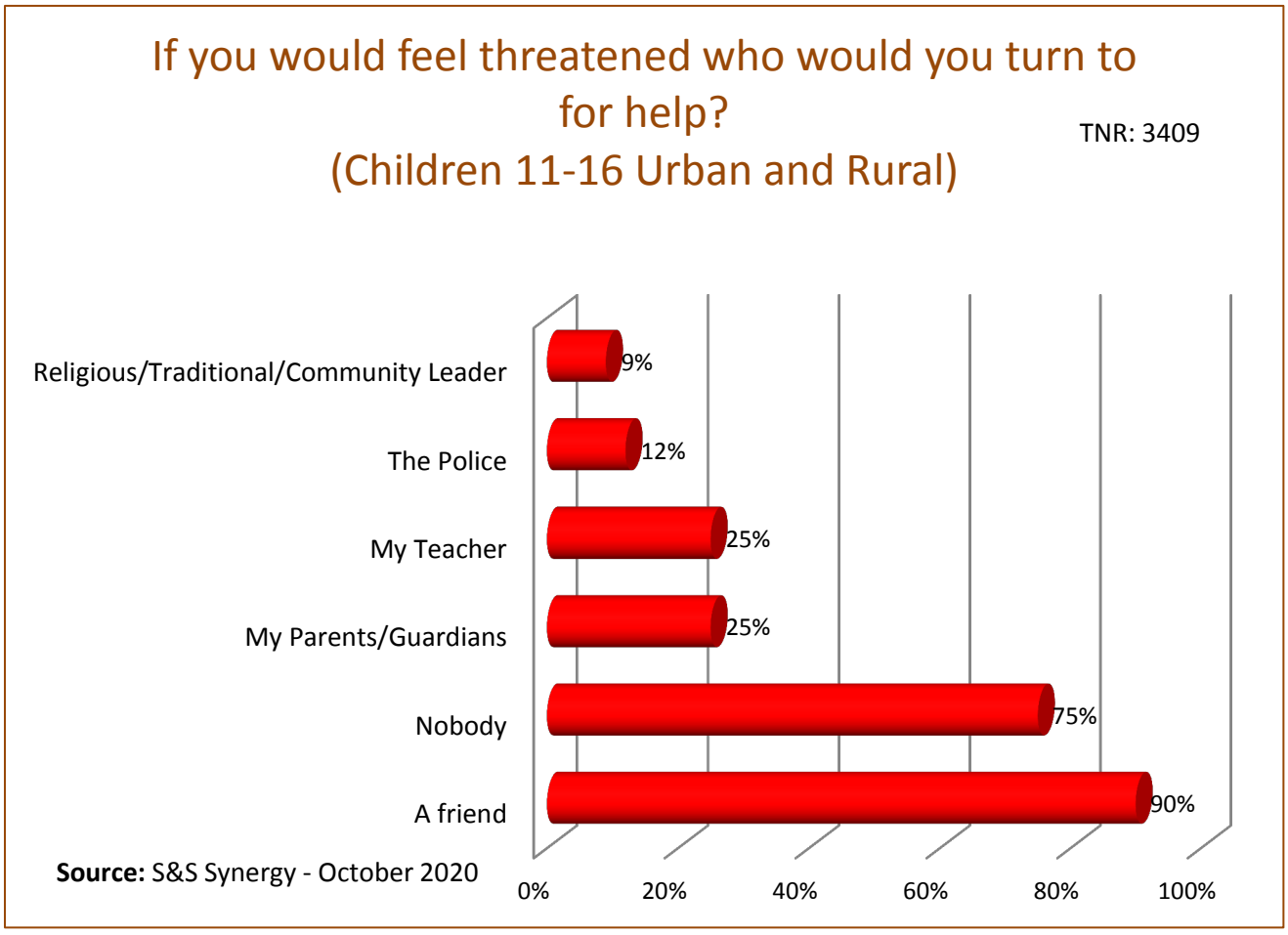


Figure 25: Children's Feedback Consultation Preference

The survey found that 90% of the time, children would rather deal with any online threat by going to a friend. Only in 12% of the time would they consider going to the police. An equally low proportion of the children (25%) said they would turn to either their teacher or parent/guardian for help.

What this connotes is that children do not feel that help for any online threat they may face would come from outside of themselves or their peer groups.

The gap in communication between parents and their children is certainly an area upon which improvement is required as it is such a vital component of the feedback and consultation mechanism that would engender a safer online world for the children.

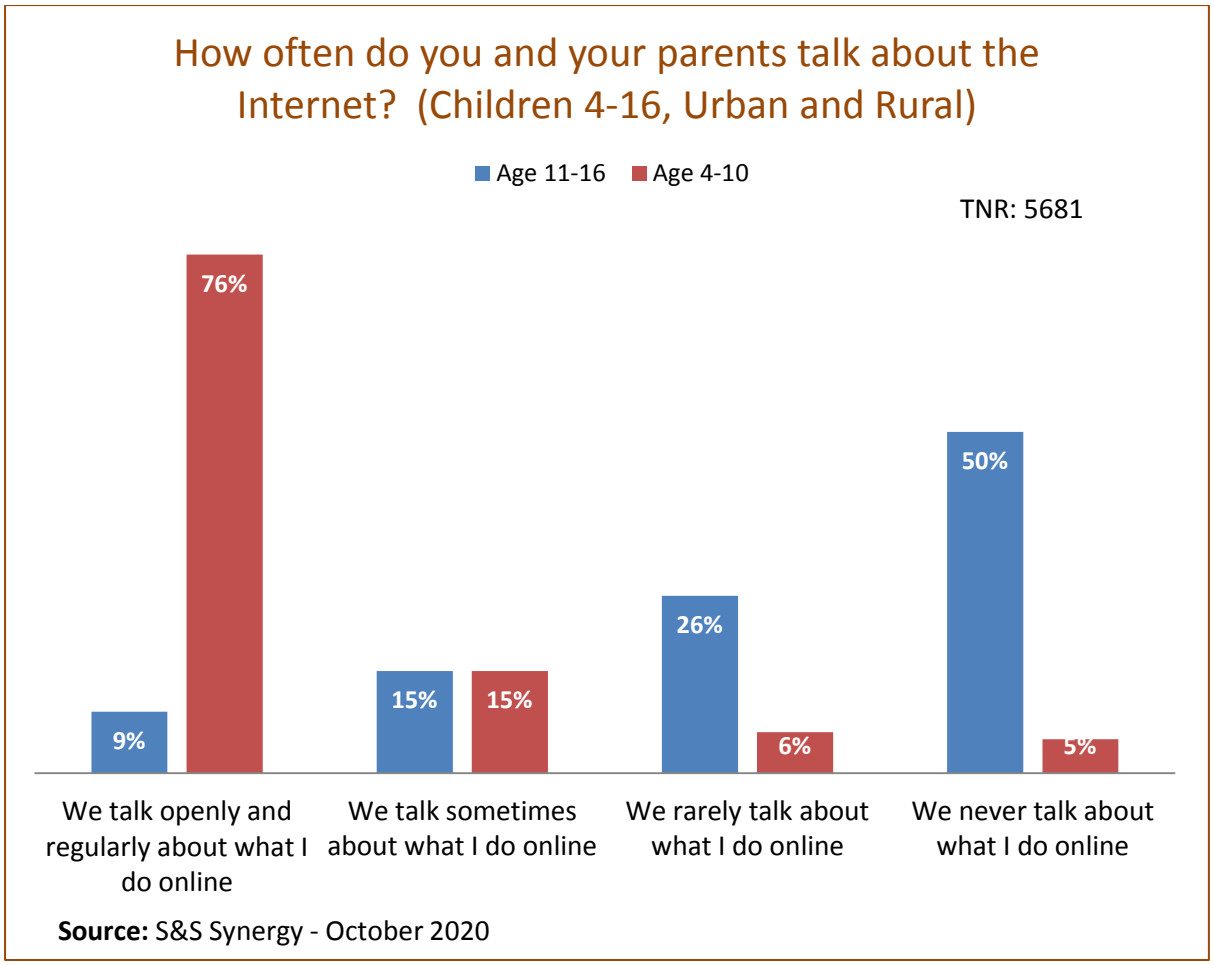


Figure 26: Frequency of Parent and Child Consultation

From the survey results, it is apparent that conversation between parent and child dwindles as the child gets older. A whopping 76% of the 4-10 years-old talks openly and regularly with their parents about the Internet compared to 50% of their older 11-16 years-old peers who never talks to their parents about what they do online.

There is a range of aspects for parents to consider in developing an effective feedback structure with their wards. As soon as a child begins to use technology, parents should discuss and establish a list of agreed rules. These rules should include when they can use the Internet and how they should use it, as well as expectations of screen time.

Also, spending time online with them will help set the right examples for children. This is because children are more likely to adopt parents' behaviours even online.

Parents can also leverage the Internet service providers and mobile network operators who will provide parental control tools that allow them to block and restrict access to certain types of content. It also allows them to limit the amount of time spent on devices.

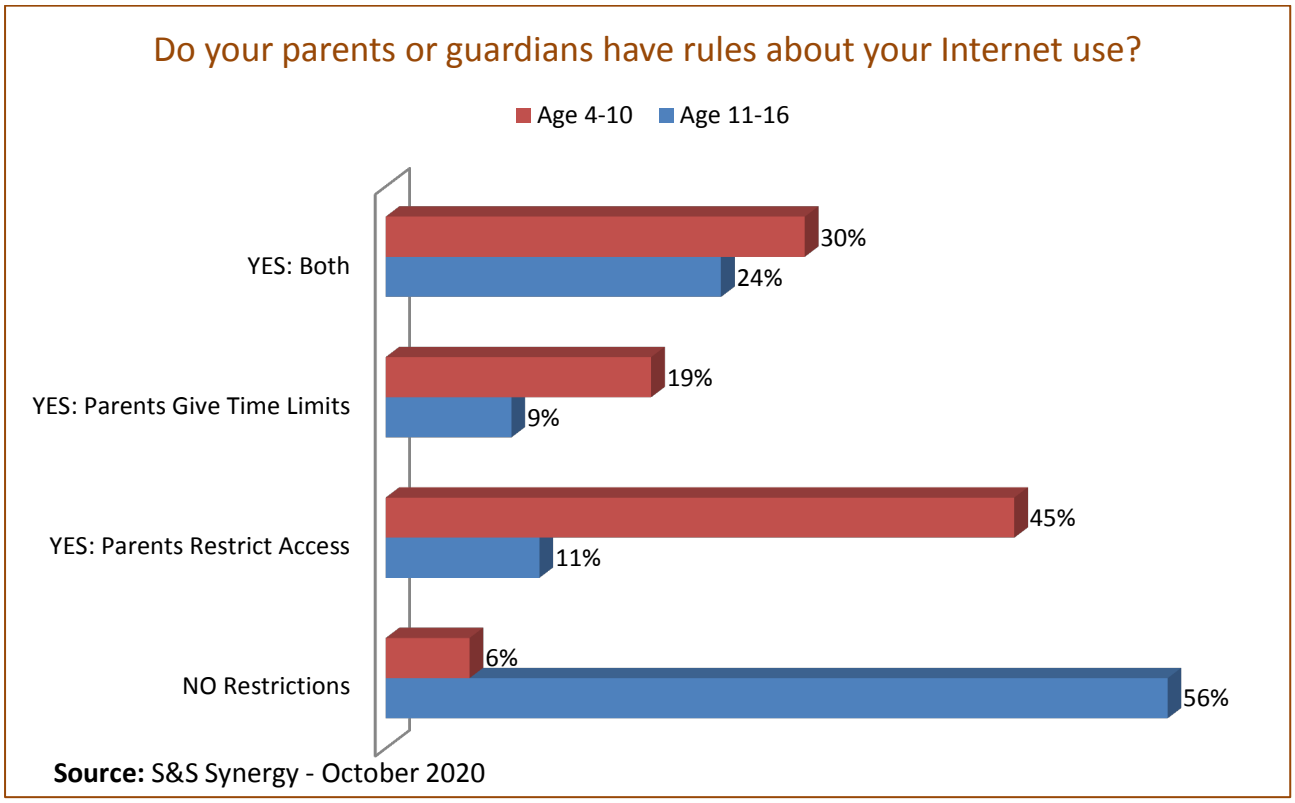


Figure 27: Use of Parental Rules as a Feedback Mechanism

As children learn more about the online world, they may wish to meet people who they have formed a relationship with online. However, with people online often wearing masks of personality, children could be in real danger if they physically meet strangers with whom they have communicated only online. So, it is important to educate children on the dangers of meeting up with strangers they've been speaking with online.

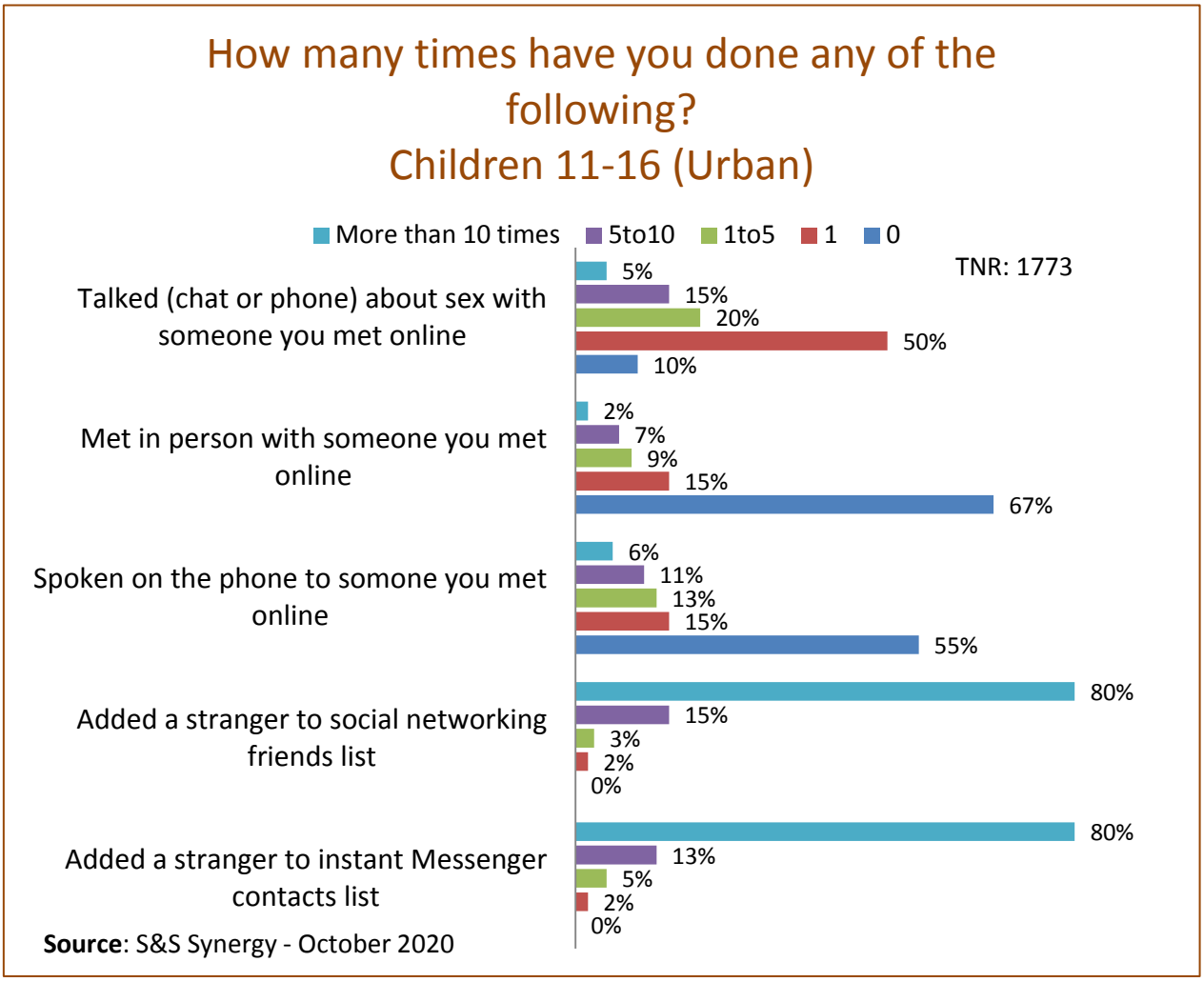


Figure 28: Probe of Children's Online and Offline Interactions

The survey examined the children's interaction with strangers online and offline and unearthed some uncommon responses. For more than 10 times, 80% of the 11 -16 year-old urban children admitted to having added strangers to both their Instant Messenger contacts and social networking friends lists. Up to 50% has at least once talked (by chat or phone) about sex with someone they met online. Although this behaviour is more prevalent among the 11-16 year-olds than the 4-10 year-olds it portends clear and obvious danger to the children involved.

Admittedly, adding strangers to one's contacts and friends lists is not a threat on its own, what is of concern is that 2% of children admitted to having met offline with someone they first came into contact with online.

Even though stories abound of young people coming to grief through meeting online contacts offline,[63] 2% of children in Nigeria appears not to appreciate the inherent dangers of doing so.

Keeping children safe is much more important than their privacy. So should not be out-of-place for parents to check their children's friend and group lists on social media platforms among others to help understand and perhaps check some of their shenanigans online. What and who children see online can significantly influence their views. So it is important for parents and teachers to engage with the children to help them develop their online media moral and literacy.

As the survey uncovered, many parents and teachers however, are not altogether confident that they have sufficient digital knowhow to curate their wards' online activities. Asked if they feel they know enough to help their children manage online risks, 68% of parents and 28% of teachers strongly disagreed with only 3% of parents and 19% of teachers strongly agreeing. This data is important to help policymakers identify the areas of training needs for teachers, parents and children.

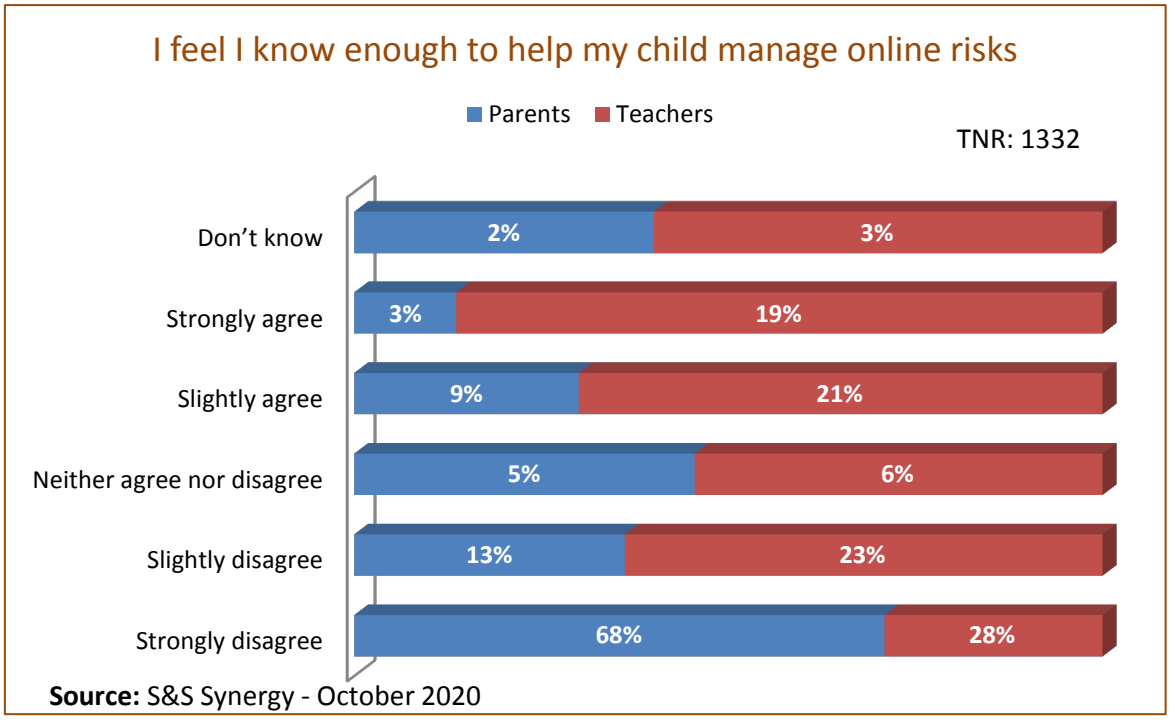


Figure 29: Parents and Teachers Digital Knowledge Confidence Levels

[63] https://news.sky.com/story/my-son-was-murdered-by-a-teenager-he-met-online-through-gaming-11931414

Similarly, knowing the apps and services used by children will help parents and teachers to understand how and where children spend their time online. It will also help to ensure that the platforms they use are as safe as possible.

There are various feedback buttons embedded in many of the most popular apps and social media sites. But as this survey discovered not many children are aware of them and as such do not use them.

Describing the usefulness of Report Abuse buttons and privacy settings on social networking sites, 89% of the children said they were not even aware of the existence of report abuse buttons, which is indeed a key feedback feature and of which all users ought to be aware.

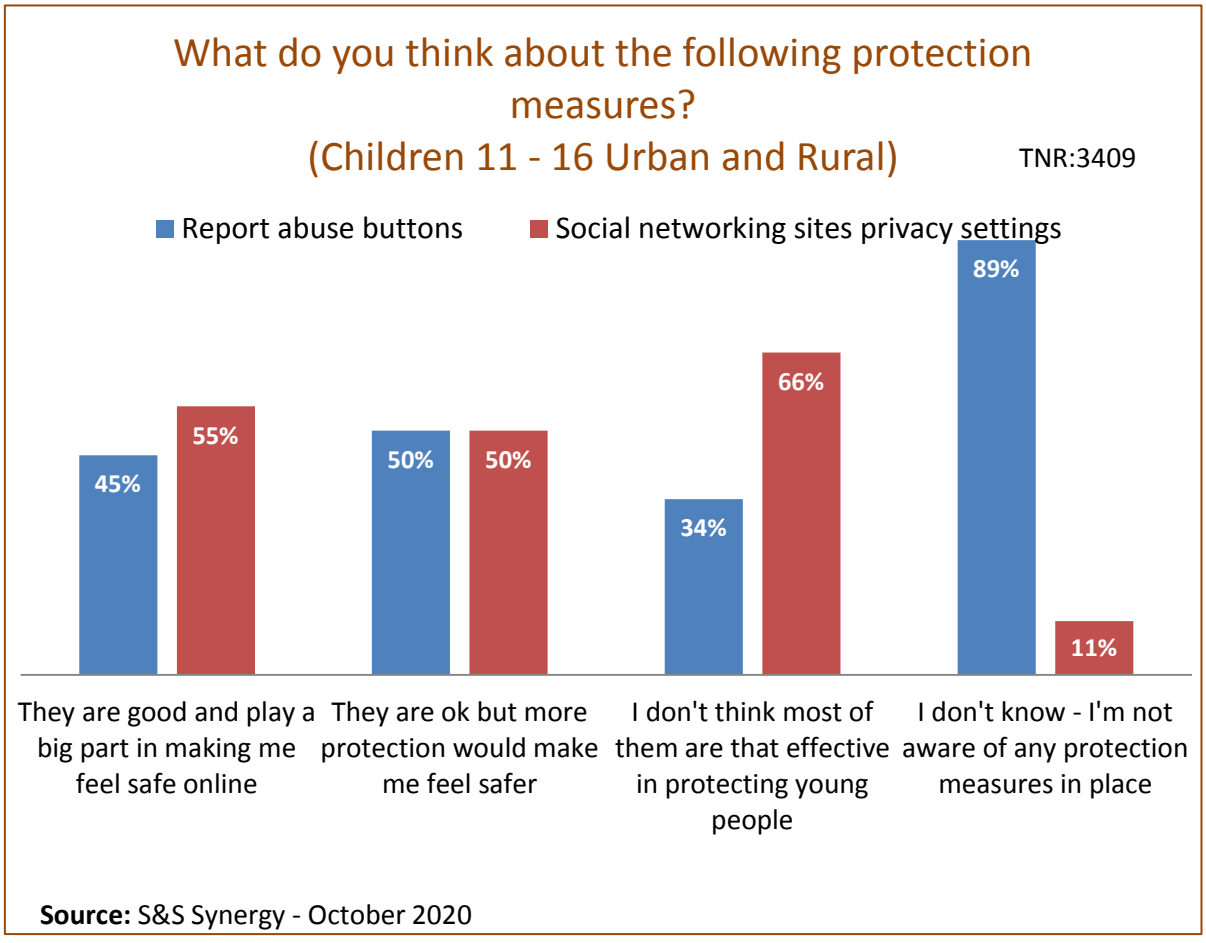


Figure 30: Children's Awareness of Online Feedback Measures

One of the best ways to improve consultation among all the online child protection actors is to ensure that all parties are carried along, more especially the children. Currently child participation is hampered by the persistence of traditional attitudes which limit children's rights to express their views in policies and decision-making procedures affecting them. A large number of children - 68% of the 11-16 year-olds and 58% of the 4-10 year-olds - expressed misgivings that the Government and Industry do not listen to them enough about the issues they face online.

Majority of the adults agreed with the children with 34% of the parents and 48% of the teachers respectively saying they do not feel young people have enough say on the issues that affect them online.

Changing this scenario and involving the children more will bring immense feedback and consultation benefits to the child online protection sphere.

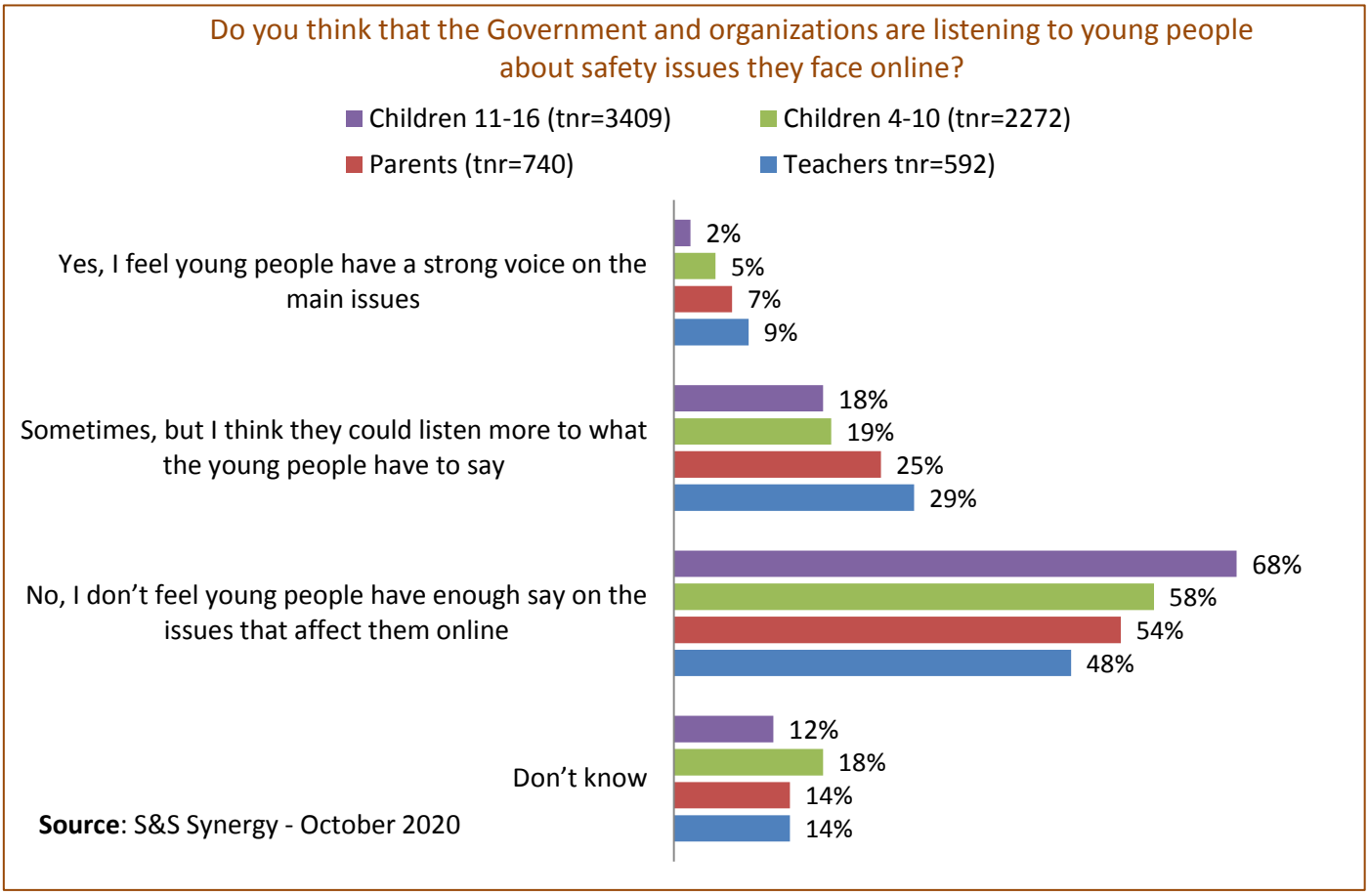


Figure 31: Respondents' Assessment of Children's Consultation and Involvement

3.60 Objective Six – Extant Policies and Guidelines

6. What is the level of effectiveness of previous child online protection policies and guidelines on the stakeholders (children, parents, policymakers etc.)?

3.61 Key Findings

From all indications, the Federal Government of Nigeria takes child online protection seriously as evidenced by the numerous strategy efforts on the matter by various Government agencies such as NSA, NITDA, NCC, EFCC, ngCERT, to name just a few. One of the cardinal principles contained in the National Cybersecurity Strategy document is to harness counter-measures through legislative framework, policy and strategic actions, including international cooperation, to address cyber abuse and online exploitation of the Nigerian child.[64]

In Nigeria, the fight against cybercrimes has culminated in the enactment of the Nigerian Cybercrime (Prohibition, Prevention, etc.) Act of 2015, which addresses issues of child pornography (Section 23), cybersquatting (Section 25), cyberstalking (Section 24), racist and xenophobic offences (Section 26), and cyber terrorism (Section 18).

The Constitution of the Federal Republic of Nigeria guarantees certain fundamental rights to all persons including children. These rights include among others: the right to privacy and family life;[65] the right to freedom of expression;[66] and, the right to freedom of thought, conscience and religion.[67] Apart from the Constitution, there are other statutes in the country dealing with the rights of the child. The various laws and instruments on the rights of the child emphasize that "in all

[64] https://www.cert.gov.ng/ngcert/resources/NATIONAL_CYBESECURITY_STRATEGY.pdf
[65] Section 37 – Federal Constitution of Nigeria, 1999
[66] Section 38 – Federal Constitution of Nigeria, 1999
[67] Section 39 – Federal Constitution of Nigeria, 1999

actions concerning the child undertaken by any person or authority the best interests of the child shall be the primary consideration."[68]

Anchored on these rights are several policies and strategies from various MDAs active in the cyber policy and regulation space including among others: the Nigeria Computer Emergency Response Team (ngCERT) with the mission to achieve a safe, secure and resilient cyberspace in Nigeria;[69] NITDA that fosters the development and growth of ICT in Nigeria;[70] and, NCC which is the National Regulatory Authority for the telecommunications industry in Nigeria.[71]

Panoply of policies, regulations, strategies and statutory bills exist underpinning Nigeria's cybersecurity infrastructure. Some of these efforts, as earlier stated, include the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015; National Child Online Protection Policy; Nigeria Data Protection Regulation(NDPR), 2019; National Cybersecurity Policy & Strategy; Data Protection Bill, 2020; Nigeria National Cybersecurity Framework; and, the National Plan for the Implementation of National Cybersecurity Strategy.

Children in Nigeria also benefit from favourable provisions on their rights under various international covenants, conventions and other instruments either jointly with adults or separately.

Guided by the best interests of the child, public obligations and private responsibilities should be governed by a set of general principles that put children's rights in context to wit: (1) Children have the right to privacy and the protection of their personal data. (2) Children have the right to freedom of expression and access to information from a diversity of sources. (3) Children have the right not to be subjected to attacks on their reputation. (4) Children's privacy and freedom of expression should be protected and respected in accordance with their evolving capacities. (5) Children have the right to access remedies for violations and abuses of their rights to privacy and free expression, and attacks on their reputation.

[68] African Charter – Article 4:1
[69] https://www.cert.gov.ng/
[70] https://nitda.gov.ng/mandate/
[71] https://www.ncc.gov.ng/the-ncc/who-we-are

Table 12: Extant Acts, Policies and Legislation around Children in Nigeria

Extant Act / Policy	Purpose	Drawback
The Child Rights Act 2003 (CRA).	Nigeria adopted the Child Rights Act to domesticate the Convention on the Rights of the Child. The Act provides for the protection of child's rights (most specifically right to survival and protection). Makes provisions to provide and protect the rights of a Nigerian child and for other related matters.	Although this law was passed at the Federal level, it is only effective if State Assemblies also enact it as only international treaties that have been domesticated into Nigerian law, have the force of law in the country;[72] To date, only 25 of the country's 36 States have passed the Act into State law.[73]
NIMC Act No. 23 of 2007.	The Act established the National Identity Management Commission (NIMC).	NIMC operates and regulates matters of national identity in Nigeria with services covering National Identification Number (NIN) enrolment and issuance, National e-ID card issuance, identity verification as well as data harmonization and

[72] Section 12; Constitution of the Federal Republic of Nigeria, 1999

[73] The States that have adopted the CRA are: Abia, Akwa-Ibom, Anambra, Benue, Cross River, Delta, Ebonyi, Edo, Ekiti, Enugu, Imo, Jigawa, Kwara, Lagos, Nasarawa, Ogun, Ondo, Osun, Oyo, Plateau, Rivers, Niger, Bayelsa, Kogi and Taraba. While the States that are yet to adopt the Act are Adamawa, Bauchi, Borno, Gombe, Kaduna, Kano, Katsina, Kebbi, Sokoto, Yobe and Zamfara.

		authentication.
Digital Evidence ACT 2011.	Lawyers can rely on the provisions of this law, most especially, Section 84(5)C to prove that information via mobile phones and other gadgets/devices are admissible in court for prosecution.	Inadequacy of the extant laws to successfully prosecute child online abuse and exploitations.
Nigerian Child Online Protection Policy 2012.	The framework focused on the domestication of five strategic areas of the Child Online Protection Initiative under the ITU framework to wit: ▪ Legal measures. ▪ Technical and procedural measures. ▪ Organisational structures. ▪ Capacity building. ▪ International cooperation.	A weak institutional framework that cannot effectively handle the implementation of the guidelines and the policy framework on COP; Digital illiteracy among COP stakeholders; Dearth of intervention funding mechanism for COP.
The Cybercrime Prohibition Act 2015.	Made provisions for the prosecution and investigation of Child pornography offenders within the Global Cyber Security Agenda, which was launched in 2008. Provides an effective, unified and comprehensive legal, regulatory and institutional	Technical gaps in toolkits and resources to mitigate child risks exposure.

	framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria.	
The Office of National Security Adviser (ONSA) Development of the National Cybersecurity Policy and Strategy (2015).	With the inclusion of the Child Online Protection Initiative through National Security Intervention.	Advocates for the inclusion of Child Online Abuse and Exploitation protection strategy into the Framework for national cooperation but not implemented yet.
Trafficking in Person (Prohibition), Enforcement and Administration Act 2015.	Establishing National Agency for the Prohibition of Trafficking in Persons (NAPTIP) including child labour, abuse and exploitation or trafficking aided through any channel including the Internet.	Absence of sustainable local multi-stakeholders platform on public awareness.
The Freedom of Information Act (FOI) 2011.	Grants an individual the statutory right to request access to information in the custody or possession of a public official, agency or institution.	Has a lot of exemptions to access to information; poor culture of record keeping/retrieval in many public institutions, frustrating and time consuming bureaucracy in the public service, high level of ignorance about the provisions of the Act among the work force in the

		public sector.
The Data Protection Bill 2017.	Seeks to make provisions for the regulation of information relating to children.	Bill stuck in the National Assembly yet to be passed into law.
The National Information Technology Development Agency (NITDA) Draft National Guidelines on Data Protection 2013.	Covers the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.	At the time of this Study, the Guidelines are still in draft, and yet to come into force.
Convention on the Rights of the Child (CRC).	CRC is the foremost International Instrument for protecting children's rights. Article 3(1) provides for the best interests of the child to be the basic principle guiding all institutions and authorities, including courts of law in all actions concerning children.	Domesticated in Nigeria as The Child Rights Act, 2003 but not yet passed into law in several States.
African Charter on the Rights and Welfare of the Child (ACRWC).	To formulate and lay down principles and rules aimed at protecting the rights and welfare of children in Africa.	The omission of a provision which requires countries to fully commit and use their resources means that the Children's Charter has no way to ensure or force states to provide resources to ensure the realisation of

		children's rights; There is also some confusion regarding Article 31 that deals with children's responsibilities. Children are required to respect parents, superiors and elders at all times which could conflict with the child's right to participate in decisions that affect them.
Children and Young Persons Act (CYPA) later adopted by States as Children and Young Persons Law (CYPL).	Prior to the enactment of the CRA, the CYPA was the major piece of legislation dealing with children's rights.[74]	Out-dated and not consistent with the current standard on child justice.

To attempt an assessment of the effectiveness of these extant policies and enactments in offering an adequate level of protection to children online in Nigeria, it is necessary to benchmark them on these seven key principles of Europe's General Data Protection Regulations (GDPR):[75]

1. Lawfulness, Fairness and Transparency

Children should be provided with information as to the purpose of the processing and the identity of the data controller, and other information insofar as this is necessary to ensure fairness (Article 12 of the GDPR).

[74] **Abdulraheem Mustapha**; Child Justice Administration in the Nigerian Child Rights Act: Lessons from South Africa. African Human Rights Law Journal, 16, 435-457.
[75] **GDPR -** the core of Europe's digital privacy legislation, universally accepted as the Magna Carta of digital privacy legislation

2. Purpose Limitation

Data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of collection (Article 5 (1) (b) of the GDPR).

3. Data Minimisation and Accuracy

Data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed (Article 5 (1) (c) and Article 5 (1) (d) of the GDPR).

4. Storage Limitation

Children should have a right to obtain a copy of all data relating to him or her that are processed, and a right to rectification of those data where they are shown to be inaccurate (Articles 5 (1) (d), 12, 16, 17, 18, 19, 20 and 21 of the GDPR).

5. Integrity and Confidentiality (Security)

Technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing (Article 5 (1) (c) of the GDPR).

6. Accountability

Further transfers of the personal data by the recipient of the original data should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection (Article 45 of the GDPR).

Additional principles in appropriate types of processing, such as those concerning (i) sensitive data, (ii) direct marketing and (iii) automated decisions:

i. **Sensitive Data:**
   Where 'sensitive' categories of data are involved — such as personal data revealing racial or ethnic origin, political

opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life — additional safeguards should be in place, such as a requirement that the data subject gives his/ her explicit consent for the processing (Article 9 (2) (a) of the GDPR).

ii. **Direct Marketing**:
Where data is transferred for the purposes of direct marketing, the individual should be able to 'opt-out' from having his/her data used for such purposes at any stage (Article 21 (2) – (3) of the GDPR).

iii. **Automated Individual Decision**:
Where the purpose of the collection is the taking of an automated decision which entails the automated processing of data intended to evaluate certain personal aspects relating to the data subject, such as his/her performance at work, creditworthiness, reliability, conduct, etc., the data subject should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest (Article 22 (4) of the GDPR).

7. Enforcement Mechanisms

The objectives of a good data protection framework or a well-developed privacy policy are essentially threefold:

1. To deliver a good level of compliance with the rules (Articles 82 – 84 of the GDPR).

2. To provide support and help to children in the exercise of their rights (Articles 77 – 79 of the GDPR).

3. To provide appropriate redress to the injured party where rules are not complied with (Article 77 of the GDPR).

The NITDA Guidelines appear to contain all the content principles and enforcement mechanisms of the GDPR. However, the major flaw with the NITDA Guidelines is that they are yet to acquire the force of law.[76]

Technically, none of the existing frameworks contain the full complement of the core data protection principles as contained in the GDPR and thus, cannot guarantee an adequate level of protection to the data subject in Nigeria.

Increasingly, certain rights enshrined in the United Nations Convention on the Rights of the Child (CRC) are being realized or put at risk with the advancement of digital technologies. These rights need to be translated and applied to the digital age.

The rights most affected by the digital age include: The right to protection against all forms of discrimination (Article 2); The right to express views and the right to be heard (Article 12); The right to freedom of expression, including the freedom to seek, receive and impart information (Article 13); The right to freedom of association and peaceful assembly (Article 15); The right to privacy, family, home or correspondence and against unlawful attacks on honour and reputation (Article16); The right to information (Article 17); The right to education (Article 28), health (Article 24); and participation in artistic and cultural activities (Article 31); The right to protection from all forms of violence and abuse (Article 19); The right to protection from all forms of sexual exploitation and sexual abuse (Article 34); and, The right to protection from sale, trafficking or abduction (Article 35).

3.62 Making a Case for Child Online Protection Law in Nigeria

Despite copious provisions in Nigerian laws and international instruments on the rights of the child, there appears to be a gap between law and practice resulting in gross inability of the child to realize these rights at present. Organisations, parents and stakeholders are still abandoning their responsibilities towards the children despite the provisions of the law.

[76] http://webfoundation.org/docs/2018/03/WF_Nigeria_Full-Report_Screen_AW.pdf

Gaps in the table below represent either a lack of one or more content principles of data protection or a total lack of an enforcement mechanism to enforce data protection breaches or to provide redress to the data subject.

	Lawfulness, Fairness and Transparency	Purpose Limitation	Data Minimisation and Accuracy	Storage Limitation	Integrity and Confidentiality (Security)	Accountability	Enforcement Mechanisms
Child Rights Act	-	-	-	-	-	-	-
National Identity Management Commission Act, 2007	-	Section 15	-	-	-	-	-
Digital Evidence Act, 2011	-	-	-	-	-	-	-
Nigerian Child Online Protection Policy 2012	-	-	-	-	-	-	-
Cybercrime Act, 2015	-	Section 38(4)	Section 39	-	Section 38(5)	-	-
Development of National Security Policy, 2015	-	-	-	-	-	-	-
Trafficking in Persons Prohibition Enforcement Act, 2015	-	-	-	-	Part VII (46-47)	-	Part V (36)
Freedom of Information Act	-	-	-	-	-	-	-
Data Protection Bill 2017	Clause 2(1)	Yes. Clause 1(b)	Clauses 3(1) & 7(1)	Clause 1(4)	Clause 1(2)	Clause 1(3)	-
NITDA Guidelines	Paragraphs 2.2(1)(a); 2.2(2)(a); 3.1.1	Paragraphs 2.1(3); 2.2(1)(a); 3.1.1	Paragraphs 2.2(1) (b); 2.2(1)(d); 3.1.3; 3.1.4; 3.1.5	Paragraphs 2.3(4) – (5); 3.1.8	Paragraphs 2.4; 3.1.7	Paragraphs 2.2 (3); 3.1.6	Paragraph 2.3(6)
Convention of the Rights of the Child (CRC)	-	-	-	-	-	-	-
African Charter on the Rights and Welfare of the Child	-	-	-	-	-	-	-
Children and Young Persons Law	-	-	-	-	-	-	-
BVN Policy	CBN Circular 16/003 and CBN Circular 01/015	Yes	-	-	CBN Circular 16/003 and CBN Circular 01/015	-	-

Table 13: Comparison of Extant Acts in Nigeria with the GDPR

There is need for more political will and economic power on the part of the Government to implement these laws in the interest of the Nigerian child. It is recommended that all stakeholders must be properly educated and enlightened on these rights. Parents, children, families, and the Government should be alert to their responsibilities under these laws and pay greater attention to their implementation.

Nigeria needs an online privacy protection law for children. The law will seek to protect the personal information of children on websites, online services and applications. The law will be binding on online service providers that collect the personal data of children.

Service providers will need the consent of the parents or guardians if the data collection affects a child below the established age. A child according to Nigeria's Child Rights Act is anyone below the age of 18. The law will guide the age of consent, the definition and provision of rights, retention period of such data and the obligations of service providers.

The law should provide for transparency and accountability mechanisms on the use of personal data. Internet Service Providers and Electronic Service Providers with products targeting children must be mandated to display children friendly privacy notice.

There should be an independent body to administer enforcement and compliance with the provision of the law and to address complaints from those seeking redress.

Service providers need to ensure their platforms are secure and do not put children at risk. They should implement privacy and security by design and default. They will have to do more, to create and ensure age-appropriate contents by managing content and dealing effectively with abuse, misuse of their platform and illegal contact with children.

Data collection should not be excessive but limited to what is required for the services provided to the child. Consent management has to be transparent and verifiable. Companies providing services that affect

children need to exercise a duty of care and be more transparent about how they capture data relating to children and their use.

Further, regulators have to understand that “children have different capacities to understand privacy and different needs which cannot be explained entirely by age."[77]

The legal framework alone cannot guarantee complete protection for the Nigerian child. Excessive regulation will stifle children's participation and access to the immense benefits of the Internet. There is a need for increased digital literacy for both children and their parents and guardians. This will ensure children implement best privacy preferences, understand the implication of oversharing, and have good online behaviour.

Parents or guardians can also utilise safety tools on their wards' devices. The tool protects children from inappropriate online contents, prevents disclosure of personal information and assists parents and guardians to manage time spent on the devices.

[77] **LSE;** https://blogs.lse.ac.uk/medialse/2018/11/08/privacy-data-protection-and-the-evolving-capacity-of-the-child-what-the-evidence-tells-us/

3.70 Objective Seven – Penetration Level of Digital Technology

7. What is the current penetration level of digital technology in relation to youth population across the 36 States of the Federation and the FCT?

3.71 Key Findings

Children and young people are major beneficiaries of the Internet and related digital technologies. These technologies are transforming the way they communicate with each other and have opened many new ways to play games, enjoy music and engage in a vast array of cultural activities thereby dissolving many barriers. Children broaden their horizons online by taking advantage of opportunities to gather information and nurture relationships.

The teeming army of young people in Nigeria has access to assortment of digital technologies. As found by this study, more than two-thirds of the 5681 children who participated in the survey own mobile phones and the rest have access to either a shared smartphone or a simple feature phone through their siblings and friends.

Their use of and access to other digital devices such as television, games console, radio, computer, laptop and tablet is also significant although the youngsters rely heavily on mobile phones for connecting with their friends and peers, meeting new people, doing school assignments and finding information.

One significant finding of the study is the apparent dissimilarity between urban and rural children in terms of their need of the Internet and digital technologies. Both sets of children desire to stay connected with friends and family; communicate with their teachers and fellow students; and generally partake of the many benefits of being online.

The survey discovered that children in Nigeria have access to and use of a wide variety of digital technologies. Radio, mobile phone and television dominate by ubiquity as outlined in the table below.

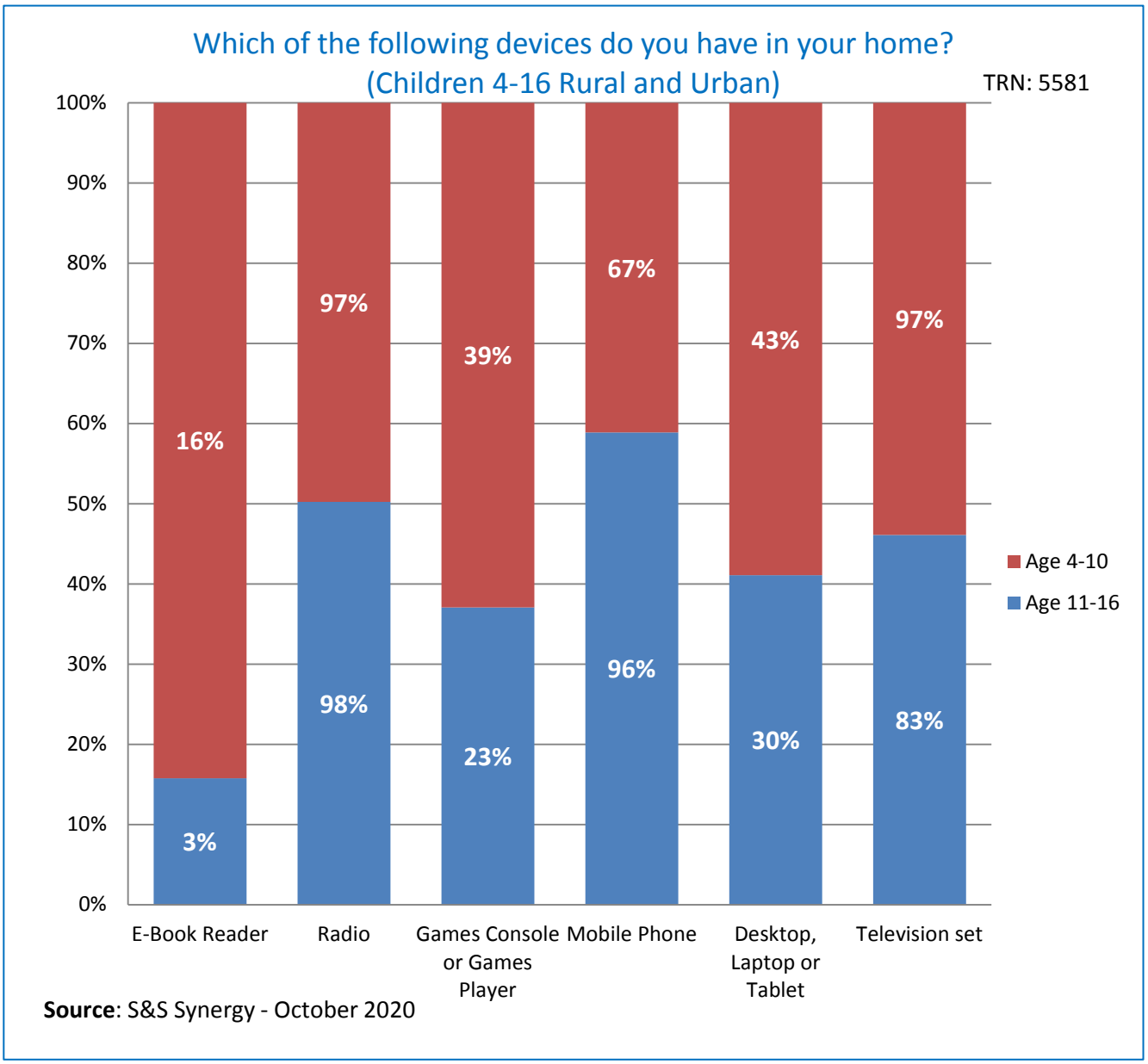


Figure 32: Availability and Access to Digital Technology At Home

Sociological and economic factors influence pattern of digital technology use among Nigerian children. The effect is that certain groups of children benefit more from their various uses of digital technology than others. Children who live in cities are poised to participate more in society through digital means than those in rural or poor areas especially on account of access to regular electricity.

3.72 Availability and Source of Electricity

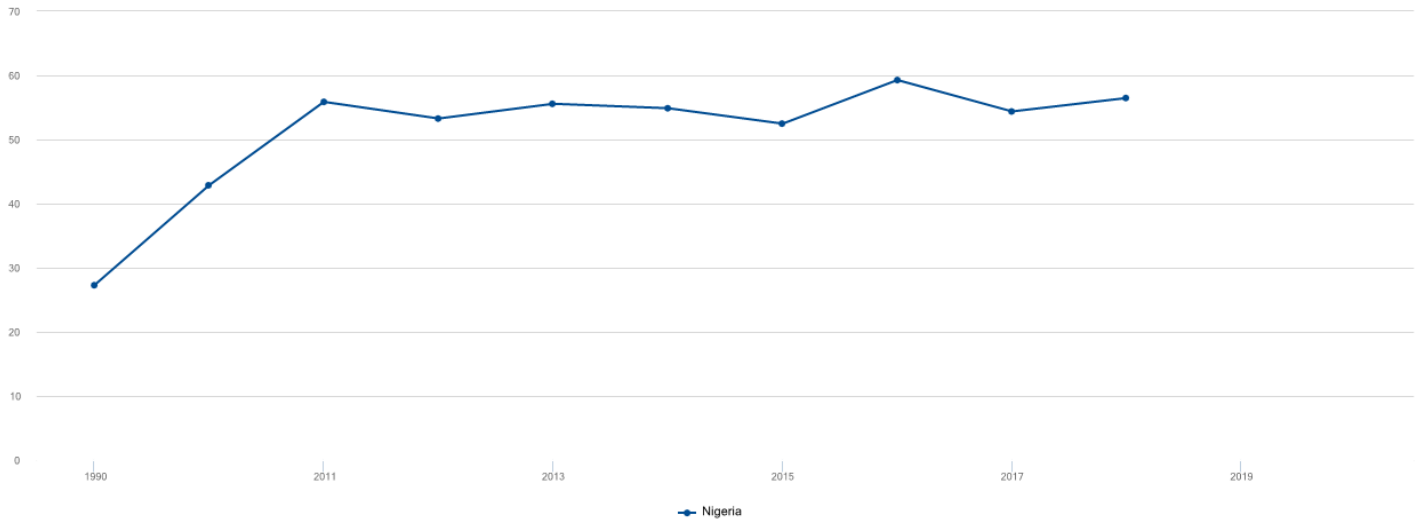
Electricity is a key driver of digital technology and therefore, the survey sought to establish the extent to which its availability (or lack thereof) affects the penetration of digital technology in the country.

Connection through the grid is the main source of electricity in Nigeria with 83.6% of the urban population having access while only 39.1% of the rural population does. Similarly, the connection rate ranges from 26.7% in the northeast to 82.4% in the south-south zone[78].

Access to electricity (% of population)

	2013	2014	2015	2016	2017	2018
Nigeria	55.6	54.9	52.5	59.3	54.4	56.5

Source: World Bank



Series : Access to electricity (% of population)
Source: World Development Indicators
Created on: 10/04/2020

[78] https://www.businessamlive.com/nigeria-ranked-2nd-largest-electricity-access-deficit-in-world-as-80m-homes-live-without-power/

The rationale for this question is to establish the availability of electricity in the first instance as it is a key enabler for digital technology. Of the 4-10 year-old respondents in the urban areas, 83% has access to electricity ranging from all the time to most of the time and some of the time while 44% of 11-16 year-olds reported having no access to electricity at all in the rural areas where they live.

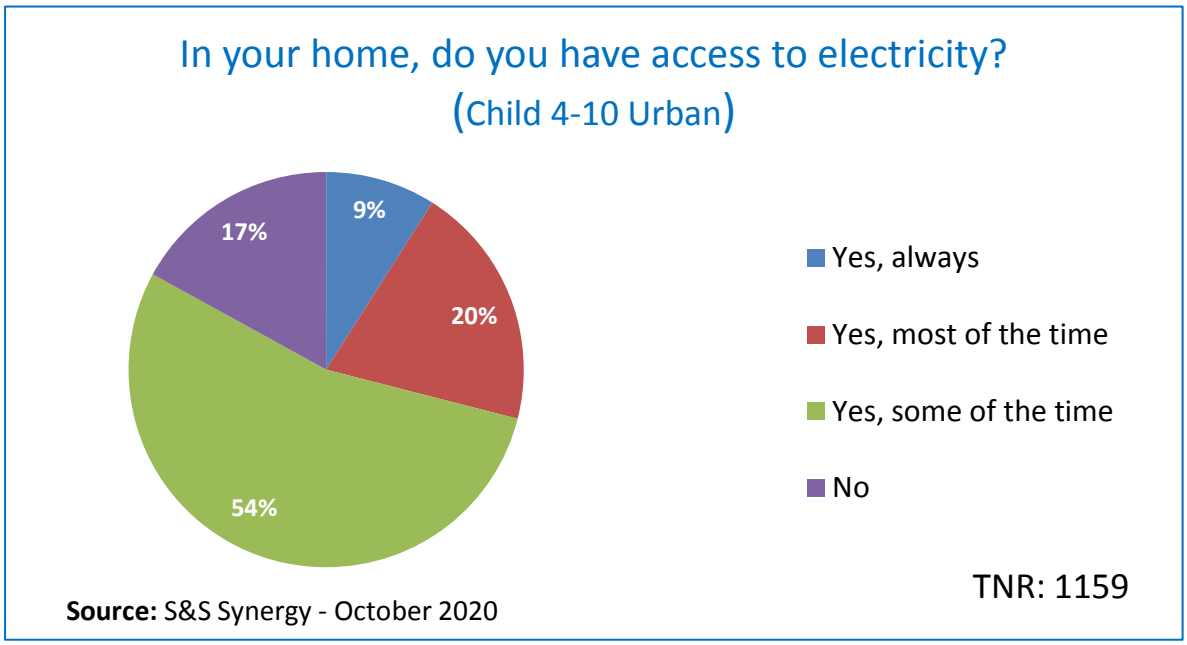


Figure 33: Access to Electricity Urban Area

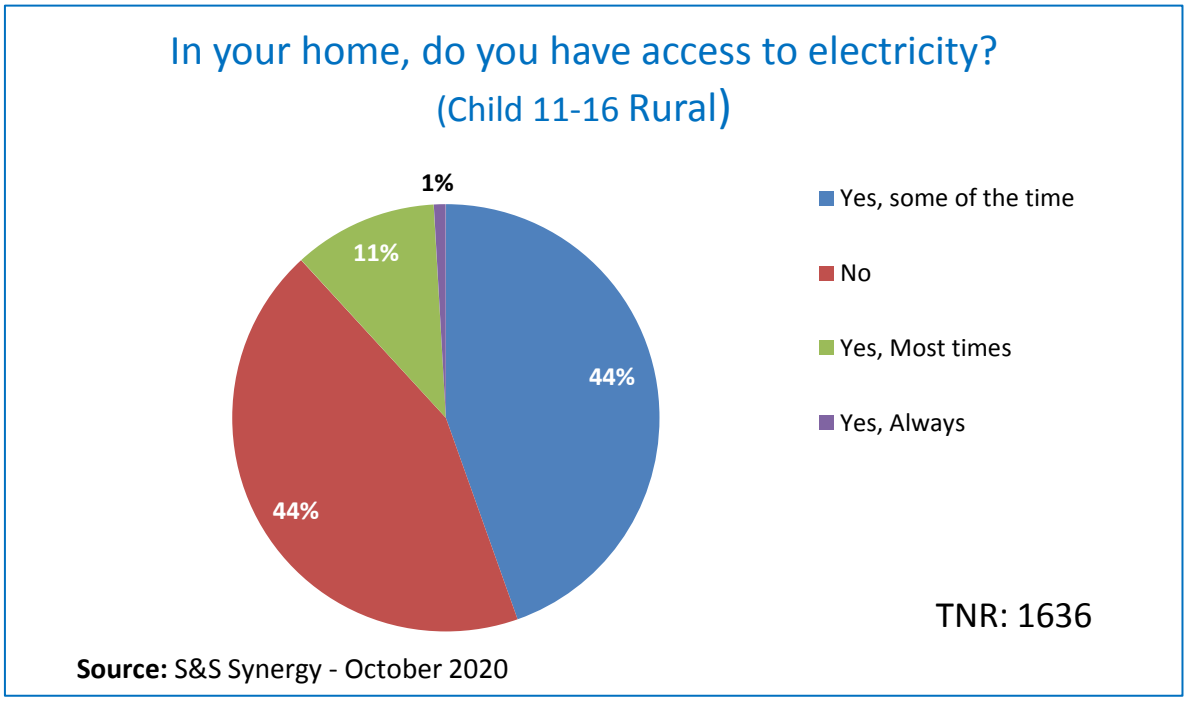


Figure 34: Access to Electricity Rural Area

3.73 Availability and Penetration of Mobile Phones

According to figures from the Nigerian Communications Commission, there are around 198.4 million mobile phone subscriber connections[79] placing Nigeria among the top 10 African countries with the highest number of connections.

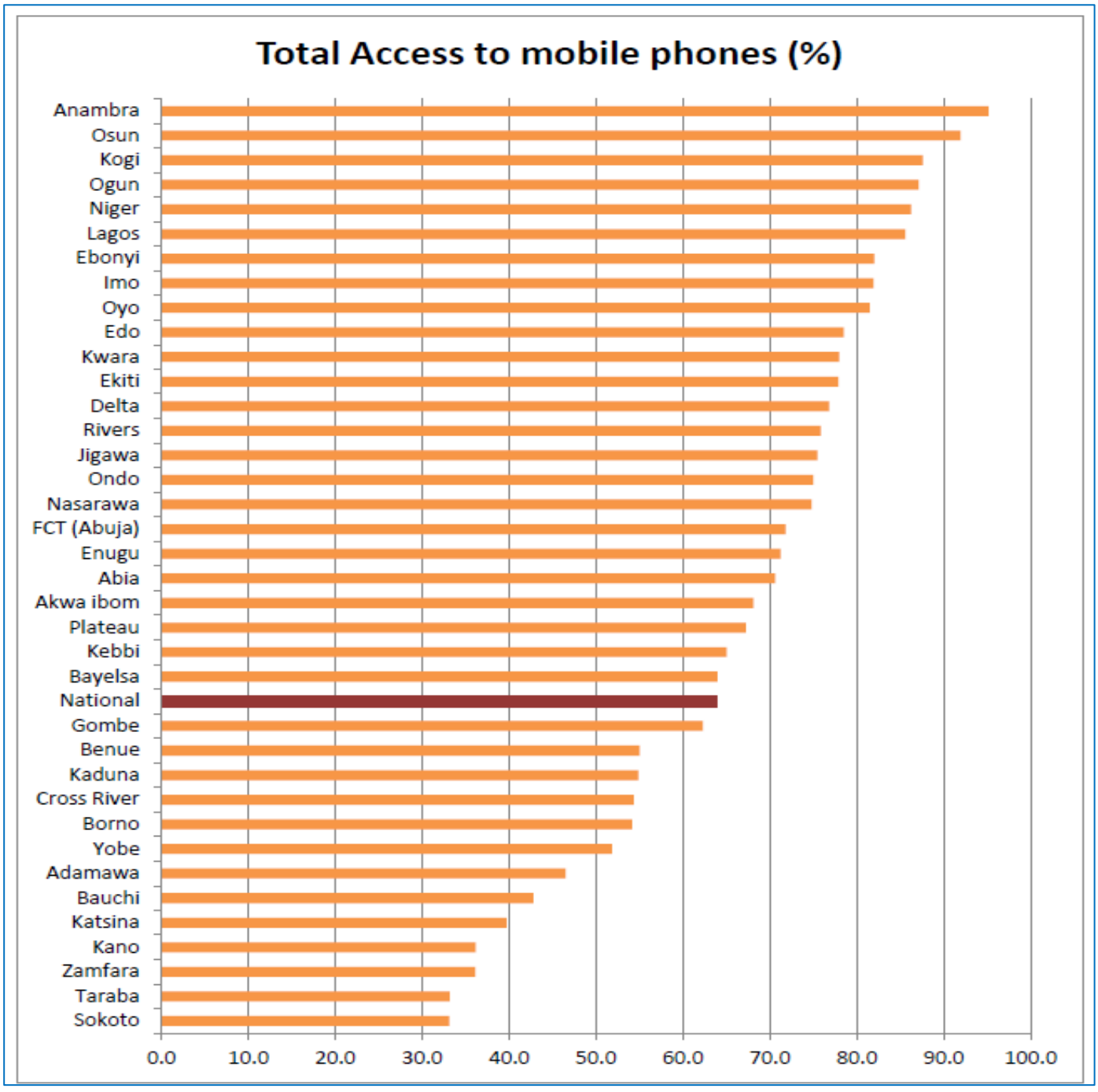


Figure 35: Schedule of Access to Mobile Phones Nationwide; Source: NBS

[79] NCC; https://www.ncc.gov.ng/statistics-reports/subscriber-data

3.74 Overall Internet Penetration

Nigeria has a multi-SIMs culture, which has fuelled the exponential growth in telephone connections in the country in the last one and a half decade. As at Q1, 2020 Nigeria has about 205.2million active lines; teledensity of 107.5% (calculated based on a population estimate of 190million); and, a total of 151.1million active Internet connections according to NCC.[80]

Based on the percentage of children using the Internet, the number of fixed-broadband subscriptions (per 100 inhabitants), and the number of cellular subscriptions (per 100 inhabitants), Nigeria came second from the bottom on the COSI connectivity access rankings.

Overall Internet penetration in Nigeria as at June 2019 stood at 45.43% of the population, compared to the global average of 57%. Mobile subscriptions grew by 7.4%; Internet users grew by 13.8%; active social media users grew by 26%; and, active mobile social media users expanded by a whopping 35% according to statistics from WeAreSocial Inc.[81]

The study discovered that the number one device for children to access the Internet is a mobile phone, followed by a family PC. More than 67% of the children own a personal mobile phone and access the Internet through their phone. Majority of them got their first phone by the time they reached 10 years of age.

Interestingly, radio appears to be the most widely available form of digital technology as evidenced by 98% of respondents reporting having one at home. Mobile phones came in at a close second position with 95% of respondents owning or having access to one.

E-Book readers are not as popular as Desktop Computers, Laptops or Tablets going by the paltry number of 7% that reported having one in their homes. Bulk of those who reported owing an E-Book also reported living in the City.

[80] NCC; https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview#view-graphs-tables-5
[81] https://wearesocial.com/global-digital-report-2019

Further interrogation of the data revealed some interesting statistics. For instance, 900 (39.6%) of the children in the 4-10 years-old bracket have access to Games Console or Games Player while only 791 (23.2%) of their 11-16 years-old contemporaries reported having access to one of those at their homes.

Similarly, the survey notes that more children in the 4-10 years-old category have access to E-Book Readers than among the 11-16 years-old.

The two groups are almost neck and neck on availability of Desktop Computers, Laptops and Tablets with 1031 (30%) and 987 (43%) numbers respectively.

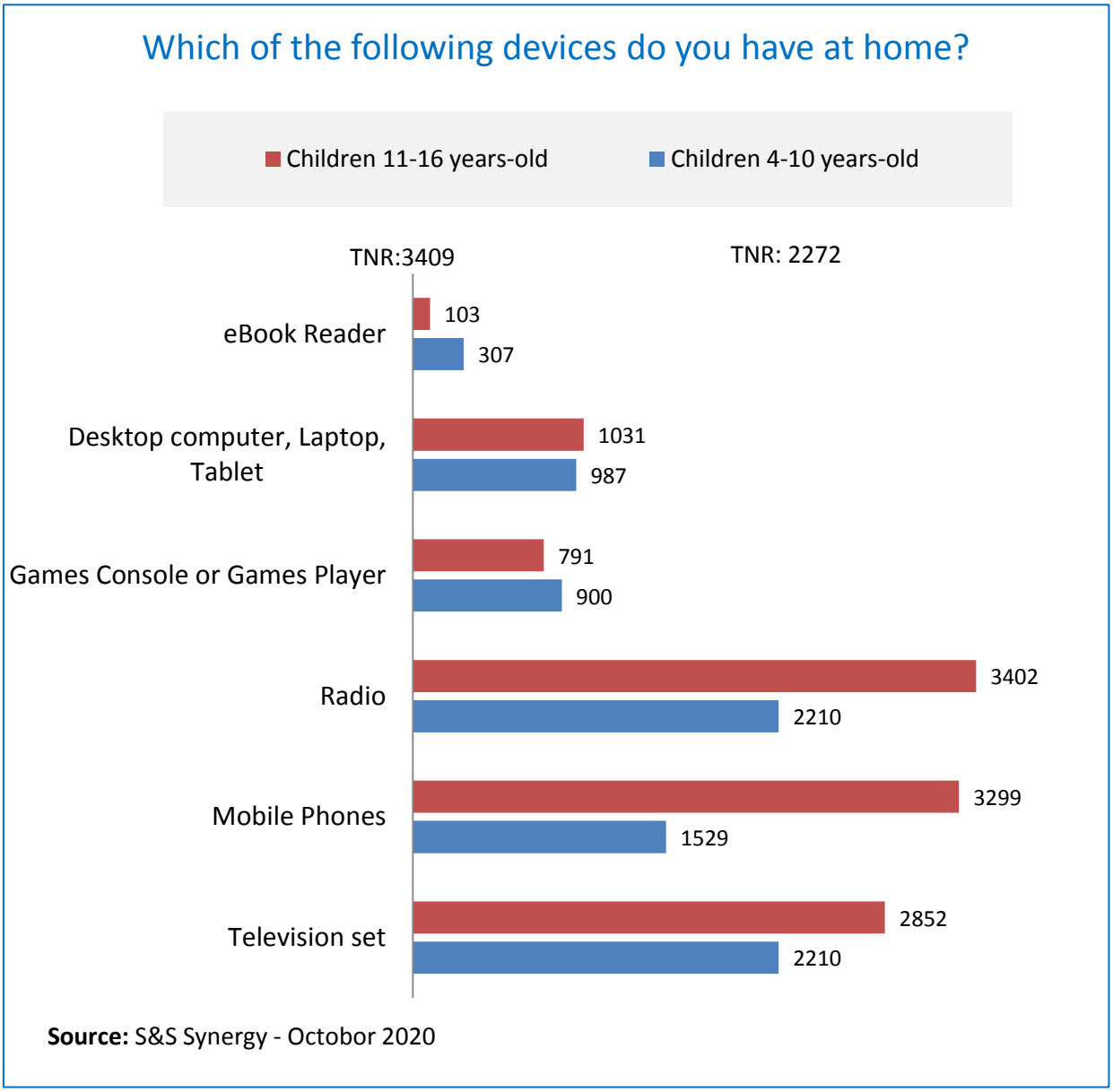


Figure 36: Digital Technology Available in Children's Homes

The gulf between the two groups concerning access to or ownership of mobile phones indicates that those in the 11-16 years-old group readily have more access to mobile phones than the 4-10 years-old.

3.75 Mobile Phone Ownership for Children

Some 700 million new mobile subscribers from various countries across the world will push the total number of global mobile subscribers to 6 billion by 2025.[82] Nigeria has been identified among these countries, with others being India, China, Pakistan, Indonesia, USA, and Brazil.

It is predicted that Nigeria will contribute 4% of the estimated 700 million new global mobile subscribers, making it one country in Africa marked with a significant contribution to increasing mobile penetration in the world. It is expected that 28 million new mobile subscribers will emerge from Nigeria between 2019 and 2025, that is, an average of 7 million new mobile subscribers annually.[83]

Figure 37: Nigeria's ranking on Mobile Ownership for Children

[82] Mobile Market Trends; https://www.jumia.com.ng/sp-mobile-report/
[83] Ibid

3.76 Connectivity Speed

Another major issue confronting children and digital technology in Nigeria is the lethargic speed of their Internet connection compounded by the rather high cost of voice/data bundles. Nigeria was ranked 114th in the world for mobile speeds and 148th for fixed broadband speeds during August 2020.[84] Nigeria's Internet download speed has also gone from bad to worse as a report from a major price comparison website revealed that the country's Internet download speed is one of the slowest in the world[85].

The Internet user in Nigeria accesses the Internet at an average speed of 15.3-megabits per second (Mbps) which is two times below the worldwide average at 34.7Mbps[86]. Confirming the rankings by almost all the speed graders, the DQInstitute in its 2020 Child Online Support Index placed Nigeria at the bottom of the table on Internet connection speed.

Figure 38: Ranking of Nigeria's Internet Connectivity Speed

[84] https://www.speedtest.net/global-index/nigeria
[85] https://nairametrics.com/2019/07/08/nigerias-internet-download-speed-ranks-one-of-slowest-in-the-world/
[86] https://businessday.ng/exclusives/article/nigerias-internet-speed-crawls-behind-global-average-as-uk-japan-set-world-record/

3.80 Objective Eight – Children's Safe Interaction with Technology

8. What suggestions and recommendations may improve the safe interaction between young people and digital technology?

3.81 Key Findings

Technology can create great benefits for children in numerous areas of their needs ranging from education to entertainment, shopping, health and many more. It is empowering in its ubiquity with children in rural areas and their counterparts in the urban areas collaborating, sharing information and new maintaining social connectivity.[87]

Technology can foster entrepreneurial thinking, helping children develop good citizenship norms when they engage in social activism through digital platforms. To unlock most of the best benefits from the digital world children should be equipped with a comprehensive set of digital citizenship skills to imbue them with critical reasoning for discernment while navigating the cybersphere.

Moreover, they also need to be able to evaluate and choose good digital services and products as conscious consumers and to become good users and creators of technology.[88]

With the understanding of the cyber-risk pandemic facing children, the Government should consider implementing digital citizenship education as part of the national curriculum for primary and secondary schools as a first priority. Empowering children with digital intelligence is only the start. Building a safe support network for children is crucial – from caring parents and capable teachers to supportive communities. At a

[87] **UNICEF** - The State of the World's Children 2017
[88] **Yuhyun Park**; 8 Digital Skills We Must Teach Our Children

national level, all stakeholders in the digital ecosystem should put their efforts together to develop an ethical digital ecosystem where every child is safely and securely protected, all children have their Rights of the Child respected, and every child has equal opportunities to thrive in their digital future.

To achieve this goal, all aspects of the digital lives of children – from Internet access points, networks, family digital culture, school education, ICT business practices, civic sector supports and Government policies in the digital ecosystem – should have proper principles and tools in place to ensure the safe, responsible and ethical use of technology.

Specifically, comprehensive digital citizenship education should teach children how to:

- Discipline their usage of digital media and technology;
- Understand the basic nature of online communication;
- Develop cognitive critical reasoning about online information, contents and contacts;
- Protect themselves proactively from cyberrisks;
- Cultivate healthy social-emotional relationships with others; and
- Develop a strong identity as responsible digital citizens.

Generally, there is need to:

- Incorporate the rights of the child into national broadband strategy and all other relevant areas of national policy.
- Cooperate across borders to create internationally valid standards and terminology for defining and measuring the state of children's rights and protection online.
- Ensure products and services designed for children by public or private sector has children's rights at the heart of their operating principles.
- Work with private-sector, civil society, subject matter experts and partners in developing online children's rights standards.

- Develop ways to engage relevant local stakeholders in campaigns against harms such as child exploitation and other online children's rights issues.
- Use new and innovative technologies such as AI, data analytics, and data motifs, to prevent networks and services from being used by offenders.
- Make measurable progress toward blocking upload of child sex abuse materials and other non-sexual child-abuse or child-harm materials in the services and products under their respective domains.
- Commit to cooperating cross-border with relevant partners to detect, stop and where possible prevent harm to children online.

There are many ways in which the private sector can contribute to positive child online protection starting with the following six:

1. By ensuring that their systems and services for children are safe by design;
2. By having prominent, well-resourced reporting and moderating functions;
3. By providing programming and engineering talent to develop anti-abuse technology;
4. By working closely with law enforcement to tackle abuse as quickly as possible;
5. By working with financial regulators and investigators to track the flow of money from abuse; and
6. By deploying their corporate social responsibility (CSR) to educate teachers, parents and guardians to help them keep children safe from harm online.

3.82 Respondents' Recommendations for Government

Invited to choose as many as they like from a bouquet of suggestions/ recommendations to the Government, 93% of the 4-10 years-old and 85% of the 11-16 years-old children rated the creation and implementation of education programmes for children on the consequences of their Internet use as top on their wish list.

The teachers on the hand were desirous of education programmes for all stakeholders with 91% and 86% of them voting for education programmes for children and training for parents/guardians, teachers and school staff respectively.

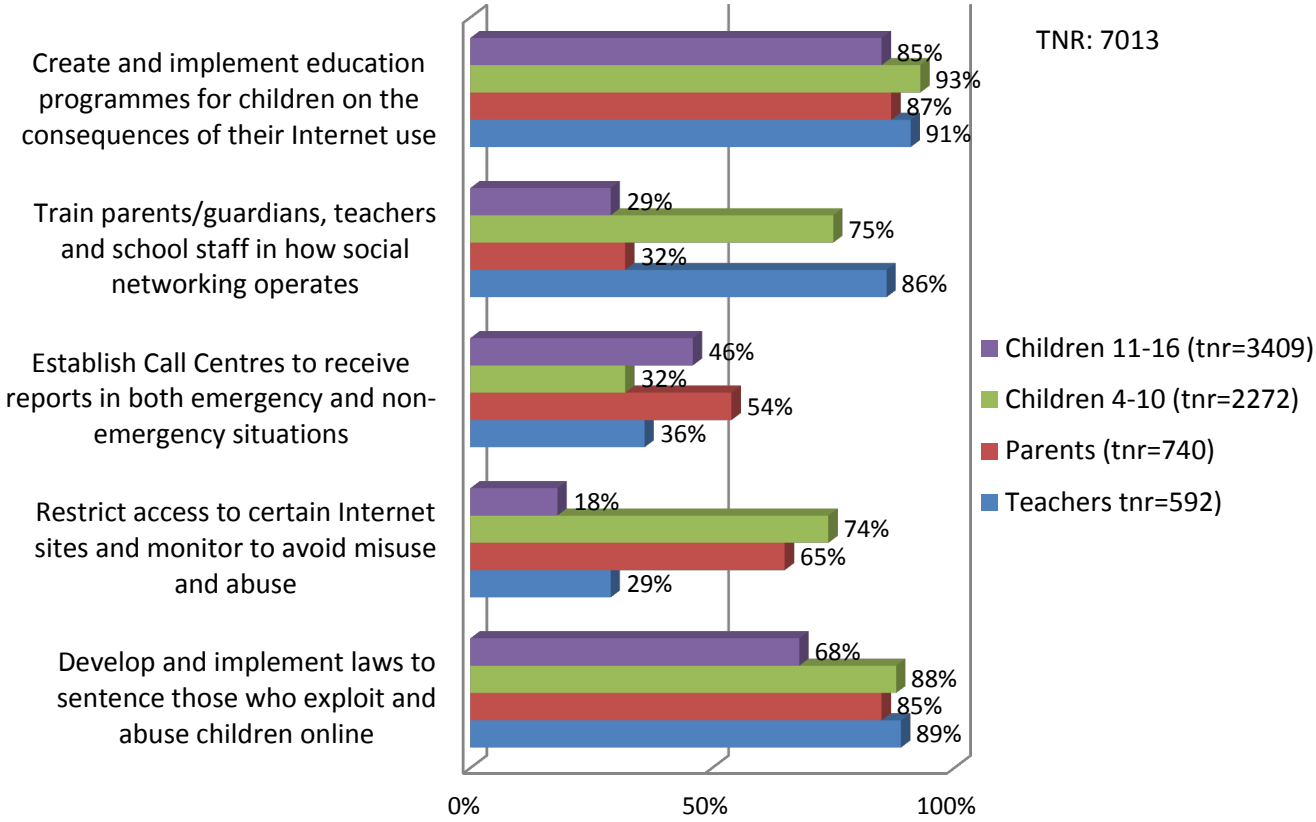


Figure 39: Survey Respondents' Recommendations for the Government

3.83 Insights from Focus Group Discussions with selected Policymakers

The discussions with selected Industry stakeholders revealed that Child Online Protection is an area in which many organisations and policymakers are lacking both in terms of confidence and competence. Not only is it an area in which their knowledge may be limited but it is also an area where awareness of the risks is developing at a pace slower than the risks themselves.

The study discovered that not many organisations have online safety and children's rights integrated into their existing policies and processes; many organisations and policymakers work mainly in silos with little or no structured collaboration with other players in the child protection ecosystem.

The key challenges in the online world that majority of the organisations identified include how to ensure that children have a safe and constructive experience online; how to promote digital inclusion and ensure adequate child protection.

They rated integrating children's rights considerations into corporate policies and management processes; supporting government, law enforcement agencies, civil society, and other stakeholders to tackle online abuse of children as online safety priorities.

Prompted to identify which actions the government should take to make the Internet safer, majority of the organisations highlighted the training of parents, guardians, teachers and school staff on how social networks operate and education programmes for children on the consequences of their Internet use as key recommendations.

The policymakers were unanimous about the merits of developing and implementing laws to sentence those who exploit/abuse children online. They also expressed enthusiasm around the prospect of establishing call centres to receive reports in both emergency and non-emergency online issues.

CHAPTER FOUR

CONCLUSION AND RECOMMENDATIONS

4.10 Conclusion

The survey came up with the following key conclusions:

- Children in Nigeria grow up being technology savvy. They are in contact daily with a wide range of digital tools;

- Digital technologies are an important but not dominant part of children's lives. Even though children love playing digital games or watching videos, they also enjoy performing other non-digital activities. Digital activities support their offline life interests and they use them as an enlargement of those activities;[89]

- Children in Nigeria are digital natives, but only to some extent. The reading and writing skills influence the quality of their digital interactions. Most children have basic operational skills while some have acquired more advanced online competencies; few use digital technologies not only as passive consumers but also in a creative way. Yet, they do encounter situations that they cannot manage, for which they have to ask for help. Their capabilities are limited by their state of cognitive development;

- When asked, children aged 4-10 have little comprehension of the risks and threats the Internet inherently embodies; their favourite activities are gaming and video watching on a variety of devices that sometimes are Wi-Fi connected. In general children this age have limited or no perception of online risks, although some of them have already encountered inappropriate age content. Many children mentioned digital activities as help for their studies;

- Children learn from observation. In most cases, children learn from observing others, parents and other family members at first,

[89] **Stéphane Chaudron**; Young Children (0-8) and Digital Technology

but they also learn from older siblings and extended family members or peers that usually have a more active mediation. Interestingly, parents seem in most cases not aware of their children mirroring their behaviour;

- Children use digital technology mainly individually rather than socially while watching videos, gaming, browsing for information or being more creative with pictures. The shared activities reside more in communicating via online video conference such as Zoom and WhatsApp;

- Mobile phones followed by Tablets are the children's favourite devices. When available, children show a strong preference for these devices. The size of their screens, portability and ease of use are the main assets of these devices for child use;

- Smartphones are the melting pot devices as they are versatile in their use bringing the ease to watch videos, play games, send messages, take pictures, and make video-calls and phone-calls. In most cases, younger children use their parents' devices equipped with free-apps for different activities but recurrently for filling gaps in the day, to keep the children occupied in waiting times or when parents need time for themselves;

- The child online protection advocacy is neither unified nor pursued in a way that is consistent across all 36 States of the Federation and the FCT;

- There is a palpable lack of political will to enforce regulations and laws that hold service providers accountable for materials hosted on their platforms;

- Children spend a lot of time online often unsupervised, un-moderated and in sometimes unsafe spaces such as social media, messaging platforms, live-streaming apps, virtual spaces, interactive games etc.;

- The rise of new technologies such as affordable smartphones equipped with high-resolution cameras and video, picture messaging, live streaming and encryption capabilities may exacerbate the proliferation of unwholesome content and make curbing online child abuse even harder;

- Most digital technology devices are often designed with limited or no consideration of their impact on the well-being of the child;

- The slow, even reluctant, uptake and use of the tools designed to detect and tackle online harm and exploitation of children as well as the duplication of efforts in developing and applying such tools makes it harder to have collaborative and focused action on the issue;

- There is a clear and pressing need for the sharing of good evidence-based best practices among child protection stakeholders that can help prevent and reduce offending;

- Some social attitudes, cultural nuances and other environmental factors, varying from State to State, may make it easier for abusers to victimize children and go undetected and therefore, unpunished;

- There exists a wide digital gap between parents, guardians, educators, and policymakers who themselves are often ill-equipped to understand the digital lives of children or to help them understand and avoid digital technology risks;

- Children spend time online in a national average of 32 hours of screen time per week. Half of them access the Internet through their own mobile phones. The majority of children use social media;

- Children who own mobile phones are twice more likely to actively engage in various social media platforms compared to those without mobile phones;

- Children who own mobile phones and actively engage in social media have 12 hours more screen time per week and have a 20% higher chance of becoming involved in cyberrisks compared to those without mobile phones;[90]
- Majority of parents feel their children spend too much time on their mobile devices;
- As parents spend more time at work leaving the upbringing of the children to teachers and house-helps, they inadvertently aid the sedentary lifestyle of their children through the proliferation of electronic gadgets such as televisions, computers, smartphones and tablets. Many children spend more time before screens than going outside to play. Some parents consider this as good news with the many dangers children face outside of the house;
- Children become occupied morning, noon and evening with television programs, little surprise that hardly anything more causes rifts among and between siblings and house-helps than the squabbles over who controls the TV remote control or the Xbox joysticks;
- There are gaps in parental knowledge relating to online risks. There is also reluctance on the part of parents to fully capitalise on the benefits of children's digital technology use.

[90] https://www.dqinstitute.org/wp-content/uploads/2018/08/2018-DQ-Impact-Report.pdf

Recommendations

4.11 Recommendation One

The Mobile Network Operators (MNO)

Should:

- Ensure content is classified in line with existing national standards of decency and appropriateness to identify content unsuitable for viewing by children;
- Provide appropriate means for parents and schools to control children's access to content classified as only suitable for adult customers in equivalent media;
- Work with relevant law enforcement agencies to combat illegal content on the Internet;
- Work to raise awareness and provide advice to parents on safer use of mobile services and ensure customers have ready access to mechanisms for reporting safety concerns;
- Provide advice and effective access to information regarding the use of mobile phone services and measures which can be taken by parents to ensure safer use by their children;
- Support awareness-raising campaigns designed to improve the knowledge of their customers and to encourage parents to become interested in the electronic media services used by their children;
- Give their support to the authorities in their fight against child pornography, and to organisations such as Save the Children in their efforts to report such content found on the Internet;
- Support the creation of appropriate legally authorised national take-down procedures for such illegal child image content, including a commitment to liaise with law enforcement agencies;
- Undertake not to insert promotional or advertising materials in the case of services targeted exclusively at children;
- Recognise the need to support parents and other guardians to ensure a safer mobile use by children.

4.12 Recommendation Two

The Parents and Teachers

This Study recommends the:

- Development of educational materials for parents and guardians on how they can support young children in learning and acquiring digital and critical thinking skills for a balanced life;
- Development and promotion of communication strategies outlining how parents can talk to young children about managing online risks and actively mediate their use;
- Development and promotion of information materials outlining the positive benefits of engagement with digital technology with a focus on positive content, educational, creative, communication and social outcomes;
- Encouragement for schools to take a more active role in promoting creative and educational uses of digital technologies as well as addressing safety matters at home with parents and guardians;
- Encouragement for schools to support teachers' lifelong learning, increase their digital skills and command for integrating the subject with ease in their teaching;
- Development and promotion of communication strategies outlining how parents and teachers can together reach the objective of digital literacy of the children;
- Development of content and services that empower children by designing and supporting children's rights online;
- Development of information materials for parents that will give them insights into the potentialities of the technology they choose for their children;
- Encouragement for dialogue with parents, schools and teachers to take a more proactive role in promoting creative and educational uses of digital technologies;
- Development of ethnographic and participatory investigative methods to capture young children's own opinions and experiences in more detail allowing children's voices and agency to inform the Study and recommendations.

Parents should:

- Set reasonable rules and guidelines for computer use by your children. Discuss these rules and post them near the computer as a reminder;
- Remember to monitor your children's compliance with these rules, especially when it comes to the amount of time your children spend on the computer. A child's excessive use of online services or the Internet, especially late at night, may be a clue that there is a potential problem;
- Remember that personal computers and online services should not be used as electronic babysitters or pacifiers for children;
- Consider keeping the computer in a family room rather than the child's bedroom. Get to know their online friends just as you get to know all of their other friends.

4.13 Recommendation Three

The Industry

Ought to focus on the:

- Introduction of corporate responsibility standards whereby Industry shares in the responsibility to ensure that children are afforded protection. Businesses may be required to show what procedures and special considerations they have undertaken to ensure child safety and respect for children's rights;
- Implementation of safety by design requiring that standards and codes of practice will be developed to require product designers, manufactures and service providers to uphold child protection values in the design and marketing of their products and services;
- Standardisation of codes of practice that aim to prevent children from seeing harmful or inappropriate content; to protect children's online privacy on the system or device-level;
- Application of consistent age-rating and classification of commercial content which will offer a transparent and effective

approach to manage content and services accessed by children. This could be made a mandatory requirement for relevant goods and services;

- Introduction of flagging systems and mechanisms to identify and report upsetting or unsuitable content by the service providers. Transparent and robust monitoring systems ought to be in place for all digital services;
- Provision of a free public hotline for reporting and accessing specialist support and advice and provision of takedown mechanisms;
- Protection of children from commercial pressures to include providing content filters, promoting safety-by-design, and raising awareness of the context in which children grow up;
- Certification of products and services that are offered to children and articulation of action that may be taken against purveyors of products and services that violate the dictates of the certification;
- Moderation or Internet surveillance requiring a deliberate effort to conduct surveillance of the Internet to detect content that is harmful to children; and
- Construction of a robust repository database of child abuse images and cases in Nigeria as a foundational tool to monitor and link cases to identify both the victims and criminals for appropriate legal action.

4.14 Recommendation Four

The Government

Is recommended to:

- Listen to young people's viewpoints through direct consultation or research and incorporate their thinking into policies, strategies and programmes designed to enhance their online well-being;
- Promote the development of digital content that is entertaining in nature but still educative. This will focus support on the creation of content, including peer-to-peer programs, designed to educate

through entertainment like games and puzzles that help children develop digital skills;

- Encourage the development of artificial intelligence (AI) which has the potential to help companies and law enforcement agencies process more suspected child-abuse content and accurately identify illegal material, abusers and victims more often and faster;
- Train teachers on child online protection matters and professional development should be encouraged to increase their knowledge to teach and monitor children's safety. Child online protection training should ideally form a mandatory part of teaching degrees/certificates.
- Balance digital safety messages with emphasis on the usefulness of the Internet in areas such as education, research and commerce.
- Encourage young people to use the Internet as a resource for also reporting online or offline abuse or other inappropriate behaviour.
- Create online and offline digital safety campaigns for placement on the full spectrum of traditional and digital media outlets such as television channels, radio shows, websites and social media platforms that young people commonly access and use.
- Foster young digital safety champions who can speak to their peers through digital media, audio and video spots on mass media and offline spaces like schools and universities.

4.15 Recommendation Five

The Children

Should:

- Never give out identifying information such as your home address, school name or telephone number in a public message such as group chats or newsgroup; and be sure you're dealing with someone both you and your parents know and trust before giving out this information via email or any other method;

- Think carefully before revealing any personal data such as age, or financial information;
- Not post photographs of yourself on web sites or in newsgroups that are available to the public;
- Consider using a pseudonym, avoid listing your name and email address in public directories and profiles, and find out about your ISP's privacy policies and exercise your options for how your personal information may be used;
- Get to know the Internet and any services you use. If you don't know how to log on, get your parent or teacher to show you;
- Never arrange a face-to-face meeting with anyone you first met online without your parents' permission. If a meeting is arranged, make the first one in a public place and be sure someone older accompanies you;
- Never respond to messages that are suggestive, obscene, belligerent, threatening or make you feel uncomfortable. If you would encounter such messages be sure to report them to a trusted adult or the police;
- Not click on any links that are contained in emails or chats from persons you don't know. Exercise caution clicking on links even from people you know unless you specifically requested for such a link;
- Remember that people online may not be who they seem. Because you cannot see or even hear the person, it would be easy for someone to misrepresent him or herself. Thus, someone indicating that "she" is a "12-year-old girl" could in reality be a 40-year-old man;
- Remember that everything you read online may not be true. Any offer that is too good to be true probably is.
- Be careful about any offers that involve you coming to a meeting, having someone visit your house or sending money or credit-card information.

APPENDICES

5.1 Appendix 1: Work Plan

	Work Activity	Description	Responsibility	KPI	Remarks
1	Inception Report	a) Review project objectives b) Draft and submit Inception Report	S & S SYNERGY NCC	Mobilisation to the field	Achieved ✓
2	Project inception	a) Set up strata PIU in Abuja, Ibadan, Jos and Calabar b) Arrange strata level logistics c) Procure required equipment – tablets, handheld devices, mobile devices and other project consumables	S & S SYNERGY	Harmonise project objectives with Work Plan	Achieved ✓
3	Articulation of survey questionnaire	a) Articulate, review and produce interview questionnaires b) Configure tablets and handhelds with survey apps and questionnaire accordingly	S & S SYNERGY	1. Printed questionnaire 2. Configured devices	Achieved ✓
4	Engagement of resource persons	a) Engage zonal coordinators b) Engage State coordinators c) Engage data collectors/ enumerators d) Plan for engagement of ancillary artisans, drivers, messengers, etcetera as required	S & S SYNERGY	Resource persons in place	Achieved ✓
5	Training	a) Execute train the trainer course for the four zonal coordinators b) Conduct training of State Coordinators by the zonal coordinators at the respective PIUs c) Organise training, orientation and	S & S SYNERGY	Resources persons trained and ready	Achieved ✓

		deployment of data collectors/ enumerators			

6	Identification of industry and sector resource partners	a) Populate the TSU cluster schedule with a comprehensive list of relevant sector resource partners b) Organise focus group discussions, workshops and meetings as required	S & S SYNERGY	1. Stakeholder mapping 2. Efficient matching of resource persons to TSUs	Achieved ✓
7	Desk review	a) Subject the NCOP to SWOT analysis b) Interrogate legacy archived materials on children's exposure to digital technology c) Review literature from leading institutions active in the ICT sector and in child online safety issues d) Research Internet resources and documented materials	S & S SYNERGY	Secondary data	Achieved ✓
8	Field Work	a. Mobilise resource persons to the field b. Conduct HH enumeration in urban area clusters and rural area clusters c. Conduct cluster level enumeration of primary schools and secondary schools d. Execute doorstep interview of PSU respondents e. Carry out survey meetings with SSUs and TSUs	S & S SYNERGY	Commencement of active field work across the country	Achieved ✓

9	Interim Report	Produce and submit progress report	S & S SYNERGY NCC	Interim Report Feed back to client	Achieved ✓
10	Monitoring and Evaluation (M&E)	a. Feedback on project performance b. M&E on processes and platforms c. M&E on performance of resource persons and other service providers	S & S SYNERGY	Continuous monitoring and evaluation of the project to ensure consistent alignment with the ToR	Achieved ✓
11	Data Analysis	a. Collate and analyse primary and secondary data b. Feed all data into the Zoho Analytics correlation engine	S & S SYNERGY	Policy recommendations, suggestions	Achieved ✓
12	Final Report	Submit Final Report Do a Presentation to Executive Management at client's site Conclude and submit the Final Report	S & S SYNERGY NCC	Produce a Final report on the Project	Achieved ✓
13	Executive Summary	Submit publishable Executive Summary	S & S SYNERGY NCC	Executive Summary of the Study	Achieved ✓
14	PowerPoint presentation to the Commission, Industry stakeholders and the public	TBA			

5.2 Appendix 2: Terms of Reference

Section 6. Terms of Reference

PROPOSAL FOR A CONSULTANCY STUDY ON "[YOUNG CHILDREN AND DIGITAL TECHNOLOGY: A SURVEY ACROSS NIGERIA]"

1.0 INTRODUCTION

Digital Technology is a contemporary phenomenon associated with the use of modern gadgets to simplify the daily activities of human beings. It is a phenomenon that is mostly associated with the learned populace of a society, although the unlearned part have also found ways of making use of digital technology due to the simplicity of their interfaces making most of them user friendly. It encompasses the use of internet resources, phones, tablets, computers, artificial intelligence, and so much more.

In this modern time, the world has become a global village due to the concept of globalization, as such access to digital technology has been made easy and an integral part of societal activities. Children have access to a wide array of filtered and unfiltered contents on the internet which can be integral in shaping the conduct of the children.

Despite the growing number of young children who go online and who are using a wide range of technologies, little is known about children's interaction with those technologies. The implementation of the Nigerian Child Online Protection (NCOP) framework has not made significant impact

yet. NCOP was developed through interagency collaboration in 2013 with extensive use of various local and international institutions.

NCOP focus areas are:

- Policy makers
- Parents – children and guardians
- Educators
- ICT industry
- Security and law enforcement agencies

Children use of technology is affected by the way parents introduce those technologies to them or what they allow them to do with them. Children's activities with digital technology is closely connected to their digital skills and level of cognitive development. The ways parents choose to control the use of technologies by children are connected to their general conviction and their perception of the technologies. Also, specific events that occur when using these technologies by children affect their perception and the way they use them afterwards. Those events also influence parents in their views and mediation.

Globally, there is an upsurge of exploitation and abuse of vulnerable groups (which young people fall under). Other areas of concern are the increased level of internet penetration and widespread use of social media where people were underserved before.

It is against such contending threats and previous efforts made, especially the NCOP framework, that this study is expected to extensively identify and

proffer possible regulatory remedies to checkmate the current challenges associated with the use of digital technology by young children across Nigeria.

2.0 OBJECTIVES/TERMS OF REFERENCE (TOR)

1. To identify issues of young people and digital technology in line with Child Online Protection Policy of the International Telecommunications Union (ITU).
2. To analyse issues such as risk, privacy, fraud, explicit content that are related to information and communication technology (ICT).
3. To establish effective online barriers without undermining the openness of the internet and its fundamental values.
4. To develop the childrens ability on how to deal with online insecurities and challenges.
5. To develop the feedback of consultation mechanisms for child online protection.
6. To determine how effective previous Child Online Protection Policies policies and guidelines have impacted the stakeholders (children, parents, policy makers etc).
7. To determine the current penetration level of digital technology in relation to youth population across the country.
8. To suggest/recommend ways of to improve the safe interaction between young people and digital technology.

3.0 SCOPE

The survey shall cover the period of year 2015 to year 2018. The study shall also cover thirty six (36) states of the Federation with equal emphasis on urban and rural areas with relevance to the following broad lines;

1. The level of availability and penetration of technological devices to children (4-16 years)
2. Identify and analyze challenges encountered by children.
3. Recommend regulatory actions to be taken.

4.0 DELIVERABLES

The Consultant will deliver the following documents in accordance with the agreed timelines as indicated in the work plan:

1. An Inception Report to be submitted within four weeks of acceptance of Letter of Award. This Inception Report will detail the study approach/methodology and work plans with timelines including review meetings, in-house or out of office trainings where necessary, presentation periods following the submission of draft interim/progress reports and draft final reports.
2. In the event that the Inception report is unacceptable, the Commission reserves the right to cancel the award.
3. Interim/Progress report before and after completion of field survey.
4. Draft final report.
5. Final report.
6. The Consultant shall submit five (5) copies of each of the approved final report and two electronic copies in Microsoft Office software format.

7. A publishable Executive summary of the Final Report.

5.0 TIME FRAME (or DURATION)

The study shall be executed within twenty weeks (20) effective from the date of award. An Inception Report must be submitted within four weeks of acceptance of Award.

6.0 PAYMENT

1. 25% of agreed consulting project sum as first installment upon acceptance of Inception Report.
2. 40% of agreed consulting project sum as second installment on submission of Interim/Progress Report after completion of field survey and the Draft final report.
3. 35% being full and final payment of the greed consulting project sum on acceptance of the Final Report.

7.0 ADMINISTRATIVE ARRANGEMENTS AND RESPONSIBILITIES

While this study is underway the Consultant shall;

Report directly to the Research and Development Department of the Commission and shall be responsible for alerting the Commission on all major issues pertinent to the successful execution and completion of the study.

The Consultant is expected to be available until the completion of the studies.

8.0 CONDUCT OF THE CONSULTANT

1. The Consultant shall be expected to carry out the assignment with the highest degree of professionalism and integrity.
2. The Consultant shall conduct their duties in an open and transparent manner and shall not hinder nor prevent the Commission from executing this or any other transaction included as part of industry development.
3. The Consultant will study all the guidelines and policies of the Commission with respect to the Industry development initiatives and will be expected to ensure that the transaction is concluded with very strict adherence to such policies and regulations.
4. The Consultant shall not take any material decision pertinent to this study without the express permission of the Commission.
5. The Consultant shall not discuss, publish, or reveal any information regarding the study without the Commission's approval.

5.3 Appendix 3: Survey Questionnaire for Children

Child Online Protection Survey

Questionnaire for Children

This survey is conducted by S&S Synergy Ltd

1. Are you?

Mark only one oval.

- ◯ Male
- ◯ Female

2. What is your age group?

Mark only one oval.

- ◯ 4 -10
- ◯ 11-16

4. Do you live in a?

Mark only one oval.

- ◯ City (Urban area)
- ◯ Village (Rural area)

3. In which State do you live?

Mark only one oval.

- Abia
- Adamawa
- Akwa Ibom
- Anambara
- Bauchi
- Bayelsa
- Benue
- Borno
- Cross River
- Delta
- Ebonyi
- Edo
- Ekiti
- Enugu
- FCT
- Gombe
- Imo
- Jigawa
- Kaduna
- Kano
- Katsina
- Kebbi
- Kogi
- Kwara
- Lagos
- Nassarawa
- Niger
- Ogun
- Ondo
- Osun
- Oyo
- Plateau
- Rivers
- Sokoto
- Taraba
- Yobe
- Zamfara

5. Do you go to school?

Mark only one oval.

- ◯ Yes
- ◯ No

6. In your home, do you have access to electricity?

Mark only one oval.

- ◯ Yes, always
- ◯ Yes, most of the time
- ◯ Yes, some of the time
- ◯ No

7. Which of the following devices do you have in your home?

Check all that apply.

- ☐ Television set
- ☐ Desktop Computer, Laptop, or Tablet
- ☐ Mobile Phone
- ☐ Games Console or Games Player
- ☐ Radio
- ☐ E-Book Reader

8. How often do you go online?

Mark only one oval.

- ◯ Daily
- ◯ Weekly
- ◯ Monthly
- ◯ Never

9. How much time do you spend online each day?

Mark only one oval.

- ◯ Less than 1 hour
- ◯ 1-5 hours
- ◯ 5-10 hours
- ◯ More than 10 hours

10. How do you access the Internet?

Check all that apply.

- ☐ Parent's/Guardians' Computer/Laptop or Mobile Device
- ☐ Your own Computer/Laptop or Mobile Device
- ☐ Other Family Members' Computer/Laptop or Mobile devices
- ☐ Friends' Computer/Laptop or Mobile Device
- ☐ School
- ☐ Internet Café

11. Do your parents or guardians have rules about your Internet use?

Mark only one oval.

- ◯ No
- ◯ Yes, my parents restrict my access
- ◯ Yes, my parents have time limits
- ◯ Yes, both

12. How do you and your parents/guardians talk about the Internet?

Mark only one oval.

- ◯ We talk openly and regularly about what I do online
- ◯ We sometimes talk about what I do online
- ◯ We rarely talk about what I do online
- ◯ We never talk about what I do online

13. How often do you do any of the following?

Mark only one oval per row.

	Every day	Once or twice a week	Once a month	Never
Use the Internet for school work	◯	◯	◯	◯
Watch video clips (e.g. on YouTube)	◯	◯	◯	◯
Download music or films	◯	◯	◯	◯
Read/watch the news online	◯	◯	◯	◯
Play games with other people online	◯	◯	◯	◯
Sent/received email	◯	◯	◯	◯

14. Which of the following products and services do you use regularly (i.e. daily)?

Check all that apply.

- [ ] Facebook
- [ ] YouTube
- [ ] Instagram
- [ ] WhatsApp
- [ ] Zoom
- [ ] SnapChat
- [ ] Online Games
- [ ] Email

Other: [ ] _____

15. Do you feel safe online? Please choose the statement that best applies to you.

Mark only one oval.

- ◯ Yes, I have never come across any threat or nuisance
- ◯ Yes, I feel I can handle any threat or nuisance that comes my way
- ◯ Sometimes, although I have heard of people having bad experiences
- ◯ Sometimes, because I have had bad experiences that make me aware of the dangers
- ◯ No, I never feel safe online and am always thinking about the dangers

16. Does your social media account profile include any of the following?

Check all that apply.

- [ ] A photo that clearly shows your face
- [ ] Your full name
- [ ] Your address
- [ ] Your school
- [ ] Your phone number
- [ ] Your correct age
- [ ] An age that is not your real age
- [ ] None of the above

17. Has any teacher at your school ever done any of these things?

Mark only one oval per row.

	Yes	No
Talked to you about what you do on the Internet	◯	◯
Helped you when you found something difficult to do or find on the Internet	◯	◯
Explained why some websites are good or bad	◯	◯
Suggested ways to use the Internet safely	◯	◯
Suggested ways to behave towards other people online	◯	◯
Made rules about what you can do on the Internet at school	◯	◯
Helped you in the past when something has bothered you on the Internet	◯	◯
In general, talked to you about what you would do if something on the Internet bothered you	◯	◯

18. What do you think is the biggest threat to you when you go online?

Check all that apply.

- ☐ Bullying or harassment by friends and acquaintances
- ☐ Unwanted sexual approaches in a chat room, social networking site or on email
- ☐ Coming across sexual images or content
- ☐ Being sent sexual images or content
- ☐ Someone using my photos in an inappropriate way
- ☐ Someone taking unwanted photos of me and circulating them

Other: ☐ _____

19. If you would feel threatened, who would you turn to for help?

Check all that apply.

- [ ] A friend
- [ ] My parents/guardians
- [ ] My teacher
- [ ] The police
- [ ] Religious/traditional/community leader
- [ ] Nobody
- [ ] Other: _____

20. Have you experienced any of the following online? Please choose all that apply.

Check all that apply.

- [ ] Pressure from friends to do things online that I did not want to do
- [ ] Bullying or harassment by friends or acquaintances
- [ ] Unwanted sexual approaches in a chat room, social networking site or an email
- [ ] Coming across sexual images or content
- [ ] Being sent sexual images or content
- [ ] Someone using my photos in an inappropriate way
- [ ] Someone taking unwanted photos of me and circulating it
- [ ] None of the above
- [ ] Other: _____

26. As a boy/girl are there specific issues you would like to share?

_____

21. How many times have you?

Check all that apply.

	0	1	2-5	5-10	More than 10 times
Added a stranger to Instant Messenger contacts list	☐	☐	☐	☐	☐
Added a stranger to social networking friends list	☐	☐	☐	☐	☐
Spoken on the phone to someone you met online	☐	☐	☐	☐	☐
Met in person with someone you met online	☐	☐	☐	☐	☐
Talked (chat or phone) about sex with someone you met online	☐	☐	☐	☐	☐

22. Have you ever shared any of the following information with a stranger?

Check all that apply.

	Face to face (offline)	Online
Name	☐	☐
Age	☐	☐
Email address	☐	☐
Home address	☐	☐
Mobile phone number	☐	☐
Where I go to school	☐	☐
Where I go after school	☐	☐
Photos of myself	☐	☐
Prefer not to say	☐	☐
None of the above	☐	☐

23. What do you think about the following protection measures?

Mark only one oval per row.

	Report Abuse buttons	Social networking sites privacy settings
They are good and play a big part in making me feel safer online	◯	◯
They are ok but more protection would make me feel safer	◯	◯
I don't think most of them are that effective in protecting young people	◯	◯
I don't know - I'm not aware of any protection measures in place	◯	◯

24. Do you think the government and organisations are listening to young people about safety issues they face online?

Mark only one oval.

- ◯ Yes, I feel young people have a strong voice on the main issues
- ◯ Sometimes, but I think they could listen more to what young people have to say
- ◯ No, I don't feel young people have enough say on the issues that affect them online
- ◯ Don't know

25. Which actions do you recommend the government should take to make the Internet safer?

Check all that apply.

- ☐ Develop and implement laws to sentence those who exploit/abuse children online
- ☐ Restrict access to certain Internet sites and monitor to avoid misuse and abuse
- ☐ Establish call centres to receive reports in both emergency and non-emergency
- ☐ Train parents/guardians, teachers and school staff on how social network operates
- ☐ Education programmes for children on the consequences of their Internet use

Other: ☐ _____

5.4 Appendix 4: Survey Questionnaire for Parents and Teachers

Child Online Protection

Questionnaire for Parents and Teachers

This Survey is conducted by S&S Synergy Ltd

1. In which State do you live?

_____

2. Do you live in a?

Mark only one oval.

- ◯ City
- ◯ Village

3. Gender of the child

Mark only one oval.

- ◯ Male
- ◯ Female

4. The age group of the child

Mark only one oval.

- ◯ 4-10
- ◯ 11-16

5. Does the child have access to the Internet at home?

Mark only one oval.

- ◯ Yes
- ◯ No

6. In your home, do you have access to electricity?

Mark only one oval.

- ◯ Yes, always
- ◯ Yes, most of the time
- ◯ Yes, some of the time
- ◯ No

7. Which of the following devices do you have in your home?

Check all that apply.

- ☐ Smart TV set
- ☐ Standard TV set
- ☐ Digital Video Recorder/ DVR (such as DSTV or Freeview+.)
- ☐ Desktop computer / laptop/ netbook– with internet access (Access to websites)
- ☐ Tablet computer – like an iPad, Kindle Fire, Samsung Galaxy Tab, Google Nexus
- ☐ Any mobile phone, including Smartphone – (iPhone/ Samsung Galaxy/ BlackBerry etc.)
- ☐ Portable media player – like an iPod Touch – that can be used to go online
- ☐ Games console or games player – like a PlayStation, Xbox, Wii, Nintendo
- ☐ Radio (whether FM/ AM or digital DAB)
- ☐ E-Book reader - like a standard Kindle, Kobo eReader or Nook eReader

8. What technology does the child have in their bedroom?

Check all that apply.

- [ ] Television/DVD Player
- [ ] Games console
- [ ] Music player (CD, iPod)
- [ ] Mobile phone
- [ ] None of the above

Other: [ ] _____

9. I feel I know enough to help my child to manage online risks

Mark only one oval.

- ◯ Strongly disagree
- ◯ Slightly disagree
- ◯ Neither agree nor disagree
- ◯ Slightly agree
- ◯ Strongly agree
- ◯ Don't know

10. Have you looked for or received information or advice about how to help your child manage online risks, from any of these sources or in any other way?

Check all that apply.

- [ ] The child's school
- [ ] Family or friends
- [ ] The child him/her self
- [ ] Government or local authority
- [ ] Manufacturers or retailers selling the product
- [ ] Internet service providers/ ISPs
- [ ] TV, radio, newspapers or magazines
- [ ] Websites with information about how to stay safe online
- [ ] No, have not looked for or received any information or advice

11. How does your child access the Internet?

Check all that apply.

- [ ] Parent's/guardian's computer at home
- [ ] Own computer at home
- [ ] Own laptop or notebook or tablet
- [ ] Own mobile phone
- [ ] Internet cafe
- [ ] Games console
- [ ] School
- [ ] Friend's house / Friend's mobile phone

12. Do you have rules about the child's Internet use?

Mark only one oval.

- ◯ No
- ◯ Yes, restriction of access
- ◯ Yes, set time limits
- ◯ Yes, both

13. What do you think is the biggest threat to children online?

Check all that apply.

- [ ] Bullying or harassment by friends and acquaintances
- [ ] Unwanted sexual approaches in a chat room, social networking site or on email
- [ ] Coming across sexual images or content
- [ ] Being sent sexual images or content
- [ ] Someone using their photos in an inappropriate way
- [ ] Someone taking unwanted photos of them and circulating them

Other: [ ] _____

14. Has the child experienced any of the following online?

Check all that apply.

- [ ] Pressure from friends to do things online he or she doesn't want
- [ ] Bullying or harassment by friends or acquaintances
- [ ] Unwanted sexual approaches in a chat room, social networking site or an email
- [ ] Coming across sexual images or content
- [ ] Being sent sexual images or content
- [ ] Someone using their photos in an inappropriate way
- [ ] Someone taking unwanted photos of them and circulating it
- [ ] None of the above
- [ ] Other: _____

15. Do you think the government and organisations are listening to young people about safety issues they face online?

Mark only one oval.

- ◯ Yes, I feel young people have a strong voice on the main issues
- ◯ Sometimes, but I think they could listen more to what young people have to say
- ◯ No, I don't feel young people have enough say on the issues that affect them online
- ◯ Don't know

16. Which actions do you recommend the government should take to make the Internet safer?

Check all that apply.

- [ ] Develop and implement laws to sentence those who exploit/abuse children online
- [ ] Restrict access to certain Internet sites and monitor to avoid misuse and abuse
- [ ] Establish call centres to receive reports in both emergency and non-emergency
- [ ] Train parents/guardians, teachers and school staff in how social networking operates
- [ ] Education programmes for children on the consequences of their Internet use
- [ ] Other: _____

Thank you very much for taking part in this survey.

5.5 Appendix 5: Questionnaire for Industry and Policymakers

Child Online Protection Survey

Questionnaire for Industry and Policymakers

This survey is conducted by S&S Synergy Ltd

1. Name of Organisation

2. To what extent are online safety and children's rights your responsibility?

3. How are online safety and children's rights integrated into your organisation's existing policies and processes?

4. To what extent is online safety covered within existing legislation?

5. What are your organisation's online safety priorities?

6. What activities does your organisation have to support online safety?

7. How does your organisation work with other agencies and organisations to improve/progress online safety?

8. Can children/parents report online safety concerns or issues to your organisation?

9. What are your organisation's three key challenges in the online world?

10. What are your organisation's three key opportunities in the online world?

11. Which actions do you recommend the government should take to make the Internet safer?

Check all that apply.

- [ ] Develop and implement laws to sentence those who exploit/abuse children online
- [ ] Restrict access to certain Internet sites and monitor to avoid misuse and abuse
- [ ] Establish call centres to receive reports in both emergency and non-emergency
- [ ] Train parents/guardians, teachers and school staff on how social network operates
- [ ] Education programmes for children on the consequences of their Internet use
- [ ] Other: _____

Thank you very much for taking part in this survey.

5.6 Appendix 6: List of Stakeholders/Policymakers

S/N	Organisation	Relevance
1	The Child Protection Sub-Sector (CPSS) Federal Ministry of Women Affairs and Social Development	The CPSS brings together relevant Government ministries and agencies, NNGOs, INGOs, UN agencies and other relevant actors with child protection technical and operational relevance
2	Public Enlightenment Department National Agency for the Prohibition of Trafficking in Persons (NAPTIP)	NAPTIP is committed to the prevention of all forms of human degradation and exploitation through the coordinated use of the Nation's crime prevention and law enforcement resources to stamp out human trafficking and to liberate and uplift the vulnerable, especially children
3	Education and Youth Development (EYD) Federal Ministry of Youth and Sports Development (FMYSD)	FMYSD is a youth centric Ministry charged with the all-round development Nigeria's youth population
4	Research & Development Department Nigeria Police Force (NPF)	NPF is the central law enforcement agency of the Federal Government of Nigeria
5	Basic and Secondary Education Department Federal Ministry of Education and Youth Development (FMEYD)	FMEYD is in charge of policymaking for the education of Nigeria's children
6	Planning Research and Policy Analysis Federal Ministry of Science and Technology	Key Policymaker
7	Standard Guidelines and Frameworks Department National Information Technology Development Agency	Key Policymaker

8	Federal Ministry of Justice	Key Policymaker
9	Save the Children Nigeria	Save the Children has programmes that work from the community to the national level to promote children's rights and protection ensuring that children are protected from all forms of violence, especially girls, orphans, vulnerable children and children affected by conflict
10	MTN	Mobile Network Operator and Internet Service Provider
11	Airtel	Mobile Network Operator and Internet Service Provider
12	Nigeria Computer Society (NCS)	NCS is the umbrella organization of all Information Technology Professionals, Interest Groups and Stakeholders in Nigeria
13	Nigeria Internet Regulatory Agency (NiRA)	NiRA is a not-for-profit, Non-Governmental self-regulating body and managers of the .ng national resource, the country code Top Level Domain name space in the public interest of Nigeria and global internet communities

5.7 Appendix 7: Definitions

Term	Meaning
Access	The right, opportunity, and/or means of finding, using or retrieving information.
Airtime	The time during which a cellular phone is in use, including calls made and received.
Blog	A Web site on which an individual or group of users record opinions, information, etc. regularly.
Broadband	A transmission capacity with sufficient bandwidth to permit the combined provision of voice, data and video, with no lower limit. Broadband is implemented mainly through ADSL, cable modem or wireless LAN (WLAN) services.
Chatroom	An online discussion forum. Everyone who is logged into a Chatroom sees what everyone else is typing, although two people can decide to break off and have a private chat.
Computer	Information technology systems and devices.
Cyberbullying	Wilful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices.
Distributed denial of service attack (DDoS)	Aim to disrupt a computer network by flooding the network with superfluous requests to overload the system and prevent legitimate requests being fulfilled.
Digital Behaviour	The process whereby an individual behaves and interacts with other users online and in groups.
Digital Divide	The gap between individuals, households, businesses and geographic areas at different socio-economic levels with regard to their opportunities to access information and communications technologies.
Digital Literacy	The interest, attitude and ability of individuals to

	appropriately use digital technology and communication tools to access, manage, integrate and evaluate information, construct new knowledge, and communicate with others.
Digital Media	Digitized content that can be transmitted over the internet or computer networks. This can include text, audio, video, and graphics.
DVD	A high-density videodisc that stores large amounts of data, especially high-resolution audio-visual material.
E-mail	Electronic mail – a computer-based form of sending and receiving messages via the Internet.
Follow	"Following" someone means you will see their updates in your timeline.
Friend	With the popularity of the Facebook concept of *friending*, young participants use the word "friends" to refer to friends from their school, neighbourhoods, or other parts of their offline lives, as well as friends they have met online.
Friending	Adding someone to a list of contacts associated with a social networking Web site.
Internet	A linked global network of computers in which users at one computer can get information from other computers in the network.
Internet subscribers	People who pay for access to the Internet.
MITM	Man-in-the-middle attack is when an attack relays and possibly alters the communication between two parties who believe they are communicating with each other.
Malware	Software that does malicious tasks on a device or network such as corrupting data or taking control of a system.
Microblogging	A broadcast medium in the form of blogging. Content is typically smaller in both actual and aggregated file size.
Multimedia Messaging Service	A system that enables mobile phones to send and receive pictures and sound clips as well as text

	messages.
Mobile Phone	Portable telephone device that does not require the use of landlines.
Mobile Internet	Internet accessed via mobile devices such as mobile phones.
Offline	Not controlled by or directly connected to a computer or external network.
Online	A resource that is available over the Internet or a network.
Online Content	Information that is available online.
Penetration	A measurement of access to telecommunications, normally calculated by dividing the number of subscribers to a particular service by the population and multiplying by 100.
Personal computers	Self-contained computers designed to be used by a single individual.
Phishing attacks	When a cybercriminal attempts to lure individuals into providing sensitive data such as personally identifiable information (PII).
Population	The number of all residents in a country, regardless of legal status or citizenship.
Post	To publish a message (text, audio, and video) in an online forum, social media platform or newsgroup.
Private Chat	An online discussion between two users via the keyboard on a computer or mobile device such as a phone.
Ransomware	A type of malware that denies access to a computer system or data until a ransom is paid.
SIM (card)	A small printed circuit board inserted into a GSM-based mobile phone. It includes subscriber details, security information and a memory for a personal directory of numbers.
Smartphone	A smartphone is a mobile phone built on a mobile operating system, with more advanced computing capability and connectivity than a basic feature phone.

Media Profile	An established user profile using a social media platform.
Social Network Site	A web-based service that allows individuals to set up profiles and share information.
Software	The programs or other "instructions" that a computer needs to perform specific tasks.
Spyware	A form of malware that hides on a device providing real-time information sharing to its host, enabling them to steal data like bank details and passwords.
Tablet	A complete computer contained entirely in a flat touch screen that uses one or more physical context-sensitive buttons; tablets customarily offer a screen diagonal greater than 7 inches (18 cm), differentiating themselves through size from functionally similar to smartphones.
Trojans	Creates a backdoor in your system, allowing the attacker to gain control of your computer or access confidential information.
Unfriending	Removing a person from a friend list on a social media platform. This means he or she will no longer be able to view a profile or information associated with it.
Video Game	A game played by electronically manipulating images produced by a computer program on a television screen or display.
Wireless	A generic term for mobile communication services which do not use fixed-line networks for direct access to the subscriber.
World Wide Web	The complete set of electronic documents stored on computers that are connected over the Internet and are made available by the protocol known as HTTP.

5.8 Appendix 8: Acronyms

CBN	Central Bank of Nigeria
Covid19	Corona Virus Pandemic
CIA	Central Intelligence Agency
COP	Child Online Protection Policy
CRA	Child Rights Act
CRC	Child Rights Charter
CSAM	Child Sexual Abuse Material
CSR	Corporate Social Responsibility
DDoS	Distributed Denial of Service attacks
DVD	Digital Versatile Disc
DVR	Digital Video Recorder
EFCC	Economic and Financial Crimes Commission
ESP	Electronic Service Provider
Et Al	And others
EU	European Union
FCT	Federal Capital Territory
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GSMA	The GSM Association worldwide
HH	Households
ICT	Information Communication Technology
INGO	International Non-Governmental Organisation
ISP	Internet Service Provider
ITU	International Telecommunications Union
IWS	Internet Watch Stats
KPI	Key Performance Indicators
M&E	Monitoring and Evaluation
MDA	Ministry, Department, Agency of Government
MNO	Mobile Network Operator
MMS	Multimedia Messaging Service,
NAPTIP	National Agency for the Prohibition of Trafficking in Persons
NBS	Nigerian Bureau of Statistics
NCC	Nigerian Communications Commission
NCDC	Nigerian Centre for Disease Control
NCOP	Nigerian Child Online Protection

NGO	Non-Governmental Organisation
NIMC	National Identity Management Commission
NITDA	National Information Technology Development Agency
NPF	Nigeria Police Force
NSA	National Security Adviser
NYSC	National Youth Service Corps
OEM	Original Equipment Manufacturer
PC	Personal Computer
PII	Personal Identification Information
PIU	Project Implementation Unit
PSU	Primary Survey Unit
PVR	Personal Video Recorder
CSAM	Child Sex Abuse Material
SM	Social Media
SIM	Subscriber Identity Module
SMS	Short Message Service
SNS	Social Network Site
SSU	Secondary Survey Unit
SWOT	Strength Weaknesses Opportunities and Threats
TBA	To Be Advised
TNR	Total Number or Respondents
ToR	Terms of Reference
TSU	Tertiary Survey Unit
TV	Television set
UN	United Nations
UNICEF	United Nations Children's Fund
WWW	World Wide Web

5.9 Appendix 9: Bibliography

1) **OECD** (2016); Trends Shaping Education 2016, OECD Publishing Paris: https://dx.doi.org/10.1787/trends_edu-2016-en.

2) **Hopkins, L., F. Brookes and J. Green** (2013), "Books, Bytes and Brains: The Implications of New Knowledge for Children's Early Literacy Learning", Australasian Journal of Early Childhood, Vol. 38/1, pp. 23-28.

3) **E. L Anderson, Et Al;** "Internet Use and Problematic Internet Use: A Systematic Review"

4) **Viswanath Venkatesh, Et Al;** "Children's Internet Addiction, Family-to-Work Conflict and Job Outcomes"

5) **Emmanuel Olagunju Amoo;** Effects of Adolescents Exposure to Sexual Contents on Social Media in Nigeria

6) **Professor Sonia Livingstone**; LSE; Children's online activities, risks and safety

7) **Marika Lüders, Et Al**; Online Opportunities and Risks for Children (pp.123-134)

8) **Shawn M Bergman, Et Al**; Millennials: https://doi.org/10.1016/j.paid.2010.12.022

9) **Larry Rosen, Et Al**; "iDisorders" https://psycnet.apa.org/record/2013-00251-001

10) **Shamael Ali**; Relationship between Technology Use and Development of Social Skills

11) **Heather C Woods, Et Al**; Sleepyteens: https://pubmed.ncbi.nlm.nih.gov/27294324/

12) **Larry Rosen, Et Al**; Sleep Health: Journal of the National Sleep Foundation

13) **Douglas A. Gentile, Et Al**; Bedroom Media: One Risk Factor for Development

14) **Hugues Sampasa-Kanyinga, Et Al**; Cyberpsychology, Behaviour, and Social Networking

15) **Mitch Van Geel**; Cyber-bullying: https://jamanetwork.com/journals/jamapediatrics/fullarticle/1840250

16) **Larry Rosen, Et Al;** Computers in Human Behaviour, 35, 364-375

17) **Helsper, E.** and **R. Eynon (2010),** "Digital Natives: Where Is the Evidence?" British Educational Research Journal, Vol. 36/3, pp. 503-520, http://dx.doi.org/10.1080/01411920902989227.

18) **Sue Scheff**; Shame Nation: The Global Epidemic of Online Hate

19) **Marcello Russo, Et Al**; https://sloanreview.mit.edu/article/surviving-a-day-without-smartphones/

20) **Danah Boyd**; Privacy and Publicity in the Context of Big Data

21) **David Siesage**; The Internet Never Forgets, So Be Careful What You Put On It

22) **Joseph B Walther**; Theories of Computer-Mediated Communication and Interpersonal Relations

23) **Allen Nnanwuba A**; The Displacement Effect of Screen Time among In-School Adolescents in Nigeria

24) **Rachel Buchanan**; How to Help Children Build a Positive Presence Online: https://www.weforum.org/agenda/2018/01/why-children-should-be-taught-to-build-a-positive-online-presence

25) **Cassandra Liem, Et Al**; The Economic Value of Personal Data for Online Platforms, Firms and Consumers; http://bruegel.org/2016/01/the-economic-value-of-personal-data-for-onlineplatforms-firms-and-consumers/

26) **Paul M. Schwartz**; 'Data Protection Law and the Ethical Use of Analytics'

27) **DQ Institute**; "What is DQ (Digital Intelligence)?"

28) **Yuhyun Park**; "DQ Global Standards Report 2019" (PDF) DQ Institute

29) **Abdulraheem Mustapha**; Child Justice Administration in the Nigerian Child Rights Act: Lessons from South Africa. African Human Rights Law Journal, 16, 435-457.

30) **UNICEF** - The State of the World's Children 2017

31) **Yuhyun Park**; 8 Digital Skills We Must Teach Our Children

32) **Stéphane Chaudron**; Young Children (0-8) and Digital Technology

33) **Livingstone, S**. Et Al. (2011), Risks and Safety on the Internet: Full Findings and Policy Implications http://eprints.lse.ac.uk/33731/.