JRIIE Journal of Research Innovation and Implications in Education

ISSN: 2520-7504

Center for Research Implications & Practice

Website: www.jriie.com ISSN 2520-7504 (Online) Vol.4, Iss.3, 2020 (pp. 209-219)

Stakeholders' Awareness Creation on Online Child Abuse among Primary School Children in Langata Sub-county, Nairobi County in Kenya

Wilkins Ndege Muhingi[1], Johnson Nzau Mavole[2], and Mumo Nzau[3]
[1, 2] The Catholic University of Eastern Africa
[3]University of Nairobi

Corresponding Author: wilkndege@gmail.com

Received September 6, 2020; Revised September 17, Accepted September 18, 2020

Abstract: *There exist several technical mechanisms to protect children on the internet. However, children continue encountering problems emanating from sexting, pornography, fraud, among others. The objective of this study was to examine how stakeholders' awareness creation influenced online child abuse among children in primary schools in Langata sub-county in Kenya. Adopting a cross-sectional descriptive design, this study was informed by Godden's formula, targeted 423 children, 9-17 years from private and public primary schools, teachers, parents, and policymakers within the DCS and DCI. Key Informant Interviews were carried out using simple random, stratified purposive, stratified, convenience, and purposive sampling designs. The study employed interview guides, questionnaires, and FGD (5) schedules to collect data. Quantitative data were analysed using descriptive statistics with the help of SPSS version 22. Quantitative data were analysed using descriptive and inferential statistics presenting findings using graphs, frequencies, and tables. Qualitative data were analyzed using content analysis utilising Nvivo version 12 and presented in narratives. The study showed that traditional awareness delivery methods, particularly activities and posters were used in schools to raise awareness of cyber-safety. School teachers also used video-based, game-based, social media online method, and lecture method to instruct children on internet use. The study concluded that a multi-level approach would be used to enhance awareness creation by having each stakeholder take the responsibility to address child online abuse. The study recommended stakeholders to work in collaboration, prepare materials, and plan to use through awareness creation on online child protection issues.*

Keywords: *Stakeholders, Awareness interventions, Online child abuse, Langata, Kenya*

How to reference this article (APA):

Muhingi, W. N., Mavole, J. N. & Nzau, M. (2020). Stakeholders Awareness Creation on Online Child Abuse among Primary School Children in Langata Sub Country, Nairobi County, Kenya. Journal of *Research Innovation and Implications in Education, 4*(3), 210 – 213.

1. Introduction

Nowadays, children have access to the new technologies which have become part of their life since they use them in school spaces as well as their homes for their known reasons (Herrero et al. 2018; Kritzinger 2016). The various technologies influence and transform economic, political, social, and cultural structures (Romero-Ruiz et al., 2017). The Internet gives children access to information, play, and leisure that are central to children's lives and rights. More importantly, children use these technologies for course education (Asongu & Odhiambo 2019; Islam et al. 2019; Nath, 2019; Wu et al. 2019; Semerci & Aydin 2018; McFarlane & Sakellariou, 2002). It is no doubt that as Goodstein (2007) and Myers et al. (2011) observed, cyber-risks and threats have reached schools, schoolyards, and children's and youth homes.

The encryption mechanisms applied to technologies ensure that users, including children, are fully protected from harm while accessing the internet. However, children continue encountering problems emanating from sexting, pornography, fraud, among others (Ong'ong'a, 2020). The emergence of online social media networks has greatly increased children's vulnerability (Nikolovska, 2020). Furthermore, the Internet is now revolutionizing children's sexual exploitation, including child prostitution and child trafficking, making it an online activity hence enabling it to be streamed and watched live, in real-time, and even allowing "clients" to direct abuse through customized requests (Dushi, 2020).
Stakeholder awareness creation interventions according to this research broadly refers to the establishment of ICT security skills and knowledge to protect users from physical, psychological, and intellectual harm. According to Mashiane, Dlamini, and Mahlangu (2019), awareness is a form of security training to inspire, stimulate and building skills and knowledge to system users." School learners can become cyber victims if they are not educated in the dangers of cyber risks and threats and in the correct way of protecting themselves and their information (Kritzinger, 2017).

Internet technology is popularly used all over the world in these modern days, so users need to be aware of the safe usage of the internet to avoid an unforeseen online accident (Karabulut, 2017, as cited in Elgharnah, 2020). Methods of awareness creation intervention revealed by a more recent study by Mabitle and Kritzinger (2020) included: traditional, game-based, instructor-led, online, simulation-led, and video-based. This was a categorization informed by previous studies by Abawajy (2014) and Wilson and Hash (2003), whose study classified awareness methods around award programs, activities, flyers or leaflets, mousepads, newsletters, posters, stationery, crossword puzzles, video games, seminars, structured presentations, animation, blogging, e-learning, email, mLearning, screensavers, social media, and simulations.

Citing Kortjan and Von Solms (2014), Kritzinger (2015) asserts that cybersecurity is a critical problem in various (developing) African countries. According to Kritzinger (2015), teachers and schools are ill-equipped to deal with cyber accidents. As stated by Marsh et al., (2015) foreign findings, parents should be mindful of taking more care to prevent and get rid of hazardous content (Bakó, R. K., & Tőkés, G. E. (2018). Besides, language, access to technological infrastructure, and geographic location impact directly on South Africa's cybersecurity and other parts of Africa and the developing countries. There are limited studies in Africa, especially in Kenya on stakeholders' interventions on, particularly awareness creation interventions among primary school children. This study aimed at filling that gap in knowledge.
What research questions did this study set to answer?

2. Literature Review

The aim of creating awareness is to educate the users of technology on the potential risks that are faced when using Internet communication tools, such as the social media, chat rooms, online gaming, email, and instant messaging on various devices, including smartphones (Breitinger, Tully-Doyle, & Hassenfeldt, 2020; Microsoft, 2014; Rahman, Sairi, Zizi & Khalid, 2020). Although the degree to which users are being taught about the risks the Internet holds is unclear (Ey & Glenn Cupit, 2011). In agreement, Kritzinger (2017) asserts that school learners can become cyber victims if they are not educated in the dangers of cyber risks and threats and in the correct way of protecting themselves and their information. He further notes that it is vital that school learners be educated about all the possible online risks and how to protect themselves (Kritzinger, 2014). However, schools are facing various challenges when implementing cybersecurity education, which includes a lack of expertise, funding, and resources. Teachers lack knowledge and know-how on cyberspace. Moreover, schools and governments, particularly police departments, may lack the tools and facilities for cybersecurity education (Rahman, Sairi, Zizi & Khalid, 2020).

Online safety, including child online safety, particularly cybersecurity is widely acknowledged as a national priority in many nations across the globe (Center for Strategic and International Studies, 2011). Countries, Labuschagne & Eloff (2014) observe that they need to have a long-term commitment, and several initiatives aimed at enhancing awareness regarding cyber safety. Failure to enhance cybersecurity was found to cripple the economy of nations (Sharma, 2012). Since children and teenagers form a large portion of Internet users, they are the focus of many recent statutory attempts to enhance online safety. Developed countries have already included cyber-safety in their school curricula because they cannot do without the internet and there has been rapid growth in Internet demand across Africa in the last decade (Von Solms & Von Solms, 2015).

The United Kingdom government agreed to educate on cybersecurity to school students aged 11 to 14 (Farrell, 2014). Australia has put in place a range of cyber-safety measures to protect its learners (Communications and Arts Department, Australia, 2014). Other developed countries involved in teaching cyber-security knowledge are the United States of America, New Zealand, and Canada (Kortjan & von Solms, 2014). Studies have shown that it is possible to ensure information security by increasing people's awareness and using safety tools at the right time and place (Güldüren & Keser, 2015). It is, therefore, important to share out information on security to the youths before it is too late.

Research on the internet activities of children in Turkey by "EU Kids Online," the threats they face, and the concern of their parents about the internet experience of their children in Europe and Turkey were recorded (Kaşıkcı et al., 2014). The study found that the majority of the students do not have enough skills to use the internet and they are under online risks. Information is needed to ensure that parents can decide, with their child, what is appropriate and safe for their use (ENISA, 2011). The purpose of awareness education is basically to draw attention to security (Wilson & Hash, 2003), therefore the families who are not aware of information security enough will fail to help both children and themselves. Examining the information security awareness of primary and secondary school students in Maraş Province, Turkey, the results revealed that the information security awareness of ethical issues among students is adequate while their level of awareness of the rules and knowledge-required issues was low (Tekerek & Tekerek 2013).

It was remarked that in ensuring the information security of the users on the internet, it is important to raise awareness of the users rather than blockings, bans, obligations (Chou & Peng, 2011; Cole, 2014; Valcke, Schellens, Van Keer, & Gerarts, 2007; Yan, 2009). For instance, Vicks (2013) examines the use of internet filters in schools to ensure students' safe internet and computer use and finds out that extreme policies limiting user access might impede accessing educational resources. Vicks suggests that instead of implementing restrictive policies, it is important to foster a culture of the appropriate use of the internet and raise the information security awareness of the students. From this point of view, it could be inferred that some stakeholders including parents need to work with the students in a partnership to ensure information security.

Regarding parents, there is an abundance of evidence that they often lack the awareness, competence, will, time and resources, or the understanding, to protect and empower their children online – and this applies even more in the Global South than the North (Barbosa 2014; ITU 2013; Livingstone and Byrne 2015). According to the researchers, there is a need to undertake new studies on secure Internet and computer use knowledge of children and young people coping with different variables such as age groups, information security policies of the school and the state of use of technology, parental and environmental conditions (Berrier, 2007; Harshman, 2014; Vicks, 2013). As reported by Marsh et al. , (2015) International findings, parents should be more vigilant in preventing and getting rid of hazardous material (Bake & Tokes, 2018).

Continents such as Africa, considered a set of developing countries, lack cyber-safety knowledge, and skills (Dlamini, Taute, & Radebe, 2011). Fast-growing internet access makes African countries vulnerable to cyber attacks due to fast-growing internet access (Grobler & Dlamini, 2012). Some countries, such as Tunisia (Cole et al., 2008), Rwanda, and Mauritius (Dlamini et al., 2011), have begun the process of addressing cybersecurity between learners. However, African countries such as South Africa, Uganda, Sudan, Egypt, Morocco, and Kenya still do not have measures in place to ensure adequate cybersecurity among their school students (von Solms & von Solms, 2014). A study by Popovac, & Leoschut (2012) in South Africa showed that, even where supervision is available, the technical sophistication of young people also means they know how to sidestep content filters and erase histories that indicate the websites they have accessed.

A lack of awareness among adults means that children who are also largely unaware of the dangers of electronic media are unable to take precautions on behalf of themselves. This results in a lack of parental control due to inadequate online safety education and prevents children from taking responsibility for their safety. Therefore, awareness campaigns and safety programs are critical if children and adults are to be aware of the potential threats and how to mitigate them (Popovac, & Leoschut, 2012).

One realises that some parents are not aware of the full extent of what can happen online (African Social Programmes and Initiatives, 2015), as well as what should be done to educate their children (de Lange & von Solms, 2012). Parents, therefore, need information that will help them become aware of cyber safety so that parents can be effectual educators and leaders. Awareness and supervision are necessary components of any Internet safety initiative. The active involvement of caring adults is necessary to prepare youth and children for safe navigation online (Berson & Berson, 2013).

Literature shows that awareness-raising is a central focus of the EC's Safer Internet Action Plan (Weston & Mythen, 2020). It is implemented across Europe through the Safe network of national awareness-raising nodes. Thus a Safer Internet Day is organised by InSafe each year to promote safer use of online technology and mobile phones (Davidson, Grove-Hills, Bifulco, Gottschalk, Caretti, Pham, & Webster, 2011; Savirimuthu, J2011). Developed countries promote cybersecurity awareness by way of shared endeavour through government, business industries, and academic partnerships. A good example is the United States where cybersecurity is a large industry with a clear goal of keeping America safe (Department Homeland Security, 2017).

Studies found that there were several Internet safety initiatives like Thinkuknow [CEOP]; NetSmartz (National Center for Missing and Exploited Children, NCMEC, and Boys and Girls Clubs of America, BGCA; EU's Safer Internet Plus Programme) to educate parents and children on safe Internet use as well as the marketing of a variety of software programs that included but not limited to

Keylogger; Netscape Nanny. These initiatives facilitated parents to control or supervise their children's activities online. Thinkuknow for example is a UK based website that educated parents who were concerned about their children's sexual exploitation as a result of exposure to the internet. The website addressed matters regarding childhood sexual abuse, grooming, and nude images. The website also educated parents on child sex and relationships particularly on online relationships, unhealthy relationships, harmful and risky behaviour. Lastly, these initiatives advised on the matter about exposure to sexual content, online activity, and sharing information online (Dombrowski, LeMasney, Ahia & Dickson, 2004).

Awareness creation can happen in various settings including, school, home, and businesses (Erastus, 2020). In a school setup, senior management teams are encouraged to ensure the delivery of the e-safety message through the curriculum and to develop their acceptable-use policies (Becta, 2009). Teachers can find themselves responsible for the delivery of the e-safety message throughout the school with little support elsewhere. However, there could arise the challenge of keeping up to date with a rapidly changing landscape; not just in e-safety, but in general terms of trying to understand the technologies (Atkinson, Furnell & Phippen, 2009). According to the Government of Canada (2010), Canada set out a five-principle cybersecurity plan to optimize the advantages of Internet technology for Canadians. There's also another constructive, collaborative approach for a cyber-secure future by embedding cybersecurity in the education system to promote a security culture at the first Internet access.

Awareness about safe Internet is and has been the dominant focal point of international campaigns (Valcke, De Wever, Van Keer & Schellens, 2011). In Taiwan, a study by Chou and Peng (2011) focusing on promoting awareness of Internet safety in Taiwan in-service teacher education advised that teachers should be familiar with: Communication security and safety which refers to teaching students how to protect themselves from viruses, hackers, spam (junk mail), and illegitimate commercial transactions, and how to safeguard their confidential information, Information decency and appropriateness that concerns how to identify malicious rumours, pornography, sexual solicitation, misleading advertising, and other offensive content and also respect for copyright and ethical use of digital information, Online interpersonal safety which refers to all social interactions, including making friends online, meeting new friends in person, cyberbullying, and digital etiquette, especially in the Web age in which social networking is the main focus and Computer-/Internet use safety that is a miscellaneous category involving proper equipment, a good work environment, eyesight protection, and posture.

Internet safety awareness activities have been in Europe under the umbrella of the European Commission since 1999. Campaigns resulting from coordinated European action lines were set up in 2005 and 2008. The focus of the "Safer Internet Program" was to make the Internet a safer place (European Commission, 2009a & Chen, & Helal, 2011, September). Four key action lines were laid out as follows: fighting illegal or harmful content by setting national hotline networks; fighting harmful content by promoting filter software; the installation of the Safer Internet Forum, bringing together political and non-governmental organizations to promote safer internet use and the organization of large scale awareness campaigns.

Another campaign that ran from 2009 to 2013 focused on the following objectives (European Commission, 2009b):- Fostering awareness of children, parents, and teachers about safe Internet behaviour, Starting national contact points to report illegal or harmful online content; with a particular focus on child abuse and grooming, Promotion of self-regulation initiatives, Stimulating children to set up themselves a safer Internet environment and Developing knowledge acquisition of children and teenagers about safe Internet use, Internet risks and promoting related European collaborative research.

Scholarship observes that cyber-crime awareness is low among the law enforcement community and that regulatory institutions in developing economies are also insufficient and impractical for dealing with cyber-crimes (Kshetri, 2010). South Africa has made cybersecurity efforts to secure cyber infrastructure and cultivate a culture of cybersecurity knowledge among its citizens through the South African Cyber-Security Academic Alliance (SACSAA), which engages primary schools through contest awareness campaigns (Kortjan & Solms, 2014). The Philippines received a medium ranking in terms of the policy and regulations on cybercrime (International

Telecommunications Union, 2017). However, the Philippines is reported to be lagging in terms of tangible collaborative accomplishments to deal with cybersecurity awareness particularly on the training pillar (International Telecommunication Union, 2017). Nigeria and Malaysia are also showing effort in protecting their people through cyber ((Adelola, Dawson, & Batmaz, 2015 & Hasan et al., 2015), and Saudi Arabia is also keen on cybersecurity (Ramalingam, Shaik, & Mohammed, 2016).

African countries are poorly equipped to support school teachers and learners with cyber-safety awareness and education (Kortjan & von Solms, 2013 & Kortjan & Von Solms, 2014). This is exacerbated by the fact that schools do not have curricula or extramural for cyber safety education. According to Kritzinger (2011), teachers' knowledge regarding cyber safety is limited which is made worse by limited budgets and resources in various countries. This was noted to have made the education of children on cyber safety issues extremely challenging making children be at more risk. Research by Kortjan and

Von Solms (2012) found that South Africa has only recently begun developing a local culture of cyber-safety. A report on the status of CSEC in Kenya found that although Kenya had ratified relevant international instruments and adopted domestic laws and policies that acknowledge CSEC as a criminal offence, various challenges hinder their enforcement. Some of the problems included a lack of allocation of adequate resources to implement laws and policies, a lack of understanding of CSEC, and a reluctance by law enforcement agencies to deal with perpetrators of such crimes due, among other factors, to bribes from perpetrators. In some locations communities also adopt alternative coping strategies to address CSEC instead of using the law e.g. solving cases through elders using cultural laws (Otieno, 2015).

According to Ndaka (2017), a campaign called 'Be the Cop' by the Communications Authority of Kenya was launched to provide consumers, especially children and young people with information and skills to practice safe internet use, to minimise their exposure to risks, preventing them being victims of online crime and fraud. CA was appointed as the national ICT regulator to protect users of ICT services including children. In 2015, the Authority initiated the Be the CoP initiative to raise awareness among parents, guardians, and teachers about the various types of crimes children have been exposed to in an online environment (Kenya Communications Authority, 2015). It took much from international guidelines issued by the International Telecommunications Union and involved campaigns across all media platforms in its first process.

Moreover, he observes that Google Kenya also launched a children's online safety initiative to promote the responsible and positive use of the internet among young learners. Those were good steps in the right direction but much more needs to be done, especially among the 'critical mass' of children living in rural and marginalised communities in Africa, who are the majority, yet the least protected. The second phase would involve following up on the progress of the campaign in primary and secondary schools across the country, through outreach activities with schools, ICT clubs, and public lectures. Communication Authority was to launch this second phase in 2018. Further, the Authority established the National Computer Incident Response Team (CIRT), a national cybersecurity management framework, which was also referred to as the National Kenya Computer Incident Response Team Coordination Center (National KECIRT/CC). The Authority aimed at providing information and assistance in implementing proactive measures to reduce and respond to 'computer security incidents' (Sambuli, Maina & Kamau, 2016).

The Authority worked very closely with the Cyber Crime Unit (CCU), which was under the Criminal Investigations Department, to fulfill its mandate to respond to cybercrimes like OCSE. The CCU was Kenya's specialized law enforcement agency, which was tasked with investigating and collecting evidence to prosecute online child sexual exploitation perpetrators. The Cyber Crime Unit had 21 officers, and although the officers were well qualified in cybercrime matters, it was known that none of the officers were explicitly assigned to investigate cases of online child sexual exploitation (Goodman, 1996).

According to research, the private sector is an important stakeholder in online abuse matters. The private sector was a key player yet not always aware of its role in enabling, preventing, and responding to CSEC. This sector ignored its responsibility in protecting children. Literature also revealed that that certain industries, such as the private sector attracted vast numbers of migrant workers. Specific areas include mining, manufacturing, tourism, and travel industries known to cause demand for paid sex, like CSEC, which causes it to increase (ECPAT International, 2016). A study also revealed that several major construction projects in Kenya have been launched in recent years, such as the Sh1.2 trillion Standard Gauge Railway in Nairobi and the Sh130 billion 700 megawatts Liquefied Natural Gas factory on the coast, resulting in an influx of national and foreign migrant workers (Otieno, 2015), most of whom have a bearing on child abuse, particularly online.

It goes without saying that as children grow, the capacity of digitalization to shape their life experiences grows with them (Keeley, B., & Little, C. (2017). The internet offers children limitless opportunities to learn and to socialize, to be counted and to be heard. It is a global concern that digital technology and interactivity pose significant risks to the health, privacy, and well-being of children, magnifying threats and harms that many children are already facing offline and making children that are already vulnerable even more vulnerable. The internet-enabled the exchange of information and communication with other people away from us.

It has, however, facilitated the creation, dissemination, and sharing of sexually explicit material and other illegal content that exploits and abuses children. Furthermore, it has opened up new outlets for child trafficking and new ways to shield such transactions from law enforcement. It has also made it far easier for children to access inappropriate and potentially harmful content created by offenders and even content produced by children themselves. This section sheds light based on various themes the various forms of internet threats to children and presents research work on necessary interventions by various stakeholders to deal particularly with threats as a result of children using the internet. This review attempts to answer the questions: What can governments; societies, families, and children themselves do to help limit the harms of a more connected world while leveraging a digital world's opportunities to support each child? (Dombrowski, Gischlar & Durst, 2007).

There is a difference between children whose access is limited to a small range of local content services accessed through inferior devices with a slow connection, and the full range of content and opportunities that their better-connected peers enjoy. Such inequalities mirror and potentially worsen those offline which already affect marginalized kids. There are also gaps in our knowledge of online children's lives, including the effect of communication on a variety of areas, such as awareness, learning, and social-emotional development, making it harder to establish complex strategies that advance problems by mitigating risks and optimizing opportunities.

There are also limitations in our knowledge of how children feel about their communication experience–including their expectations of the dangers–further restricting us. There are also strong gaps in the online risk awareness of children, and given the rapidly increasing use among children and adolescents, many lack digital skills and the essential ability to assess the protection and integrity of the material and relationships they encounter online. This represents the need for much wider opportunities for digital literacy that can safeguard and empower children. Eventually, and crucially, all these gaps indicate lags in policy-making as well as produce Digital security regulatory frameworks, digital access, digital governance, and digital transparency do not keep pace with the rapidly changing digital world and ignore the significant effect that digital technologies have on children (Dushi, 2020). Such regulatory loopholes will be abused easily if left unclosed (Mohammed, Mohammed, Solanke, 2019).

3. Methodology

3.1 Design

This study adopted a concurrent mixed-methods approach (Teddlie & Tashakkori, 2009), utilising the descriptive cross-sectional design. Both quantitative and qualitative data were planned at the beginning of the research study to answer the question where data was collected, analysed, and interpreted together (Kaur & Kumar, 2020; Creswell & Creswell, 2017). This approach helped to have qualitative and quantitative approaches complement each other and allow for a more robust analysis (Ivankova et al. 2006; Tashakkori & Teddlie, 2008 cited in Kaur & Kumar, 2020). The use of the approaches was not to replace either a quantitative or a qualitative approach but draw from the strengths and minimize the weaknesses of both methods (Creswell 2003; Jick 1979; Johnson & Onwuegbuzie 2004; Venkatesh et al. 2013 cited in Kaur & Kumar, 2020). The other reason was for better researchers' comprehension of the study problem than using any method alone (Somekh & Lewin, 2011). The approach to qualitative research was used as it allowed the researchers to gain insight into the research question on stakeholders' awareness creation, by conducting one on one interview with the respondents (Hennink, Hutter & Bailey, 2020; Silverman, 2016).

3.2 Study site and target population

This study was carried out among primary school children in Lang'ata Sub-county in Nairobi county in Kenya. This study area was selected because of its internet connectivity and the availability of well equipped Information Communication Technology centres in the sampled schools and the diversity of the population that was reached. The diversity in the target population made it possible to collect data from children from low, middle, and upper socioeconomic statuses. Three out of the eight wards within the Sub-county were selected where the researchers researched 12 primary schools within Langata Sub-county. Two private schools and two public schools were selected per ward.

3.3 Target Population

The study population comprised of public and private primary school children, teachers, parents, and child protection experts in the Department of Children's Services and Directorate of Criminal investigation which has a child protection unit in one of the wards in Langata Sub-county, "South C". The study sampled 423 pupils aged 9 to 17 years to whom questionnaires were administered, with the help of two research assistants. The researchers and the research assistants administered research instruments following appointed time schedules. This was done in all the three selected wards in both public and private schools.

A sample of 423 children was determined employing Godden's (2004) formula to select respondents from the target population. Sample determination was as follows:

$$SS = \frac{Z^2 \times p\,(1-p)}{M^2}$$

Where:
SS= Sample Size for infinite population (more than 50,000)
Z = Z value (e.g. 1.96 for 95% confidence level)
P = population proportion (expressed as a decimal) (assumed to be 0.5 (50%) since this would provide the maximum sample size).
M = Margin of Error at 5% (0.05)

Multistage, simple random, stratified random sampling designs for the respondents and purposive sampling design for KII were adopted.

3.4 Research Instruments and data collection

Data were collected using questionnaires, interview guides, and focused group discussion schedules. Permission was sought from education authorities within the Sub-county to conduct the research after a permit from the National Commission of Science, Technology, and Innovation was obtained. The research permit and a letter from NACOSTI enabled researchers to get permission from the sub-county education office and the selected school headteachers. Appointments were sought to agree on specific research time for administering the questionnaires. With the help of research assistants, consent was sought from teachers to allow children to undertake research. Children were guided by the researchers on how to fill in the questionnaires. For Focused Group Discussion, data was collected at a later time after questionnaires were filled. Going through an ethical approval process helped researchers to think more deeply about the conduct of this research (Sikes & Piper, 2010; Velardo and Elliot, 2018) and as a matter of moral sensitivity towards our participants and our research topic (Henderson & Esposito, 2017; Baykara et al., 2015 &Tangen, 2014).

3.5 Data Analysis

Quantitative data were analysed using descriptive statistics with the help of Statistical Package for Social Sciences version 22, while content analysis was run with the aide of Nvivo version 12 to aided the researchers in coming out with themes and categories as advised by Bryman (2016).

4. Results and Discussion

Out of the 423 questionnaires that were administered, 370 (87%) were successfully filled and returned. Only 53 (13%) of the children either refused to or did not return their questionnaires. A significant number of 370 (87%) filled the questionnaires successfully and returned.

4.1 Findings on Awareness creation intervention

The researchers sought to answer the question: In which way does awareness creation by stakeholders as an intervention influence online child abuse in Langata Sub-county, Nairobi City County, Kenya? The results were as presented:

4.1.1 Help on internet use

To answer the question of help that children received on internet use, like being helped to navigate the internet or be protected, two choices were given, either yes or no. The results were as shown in table 1.

Table 1: Help on use of internet use (n=370)

	Frequency	Percent
Yes	146	39.5
No	224	60.5
Total	370	100.0

Source (Field data, 2019)

A good number of children, 60.5% (224) indicated that they were not taught at home how to use the internet because either parent thought it was risky to expose their children to the internet or they were not knowledgeable enough on matters internet. Slightly less than half of the pupils acknowledge that they were taught how to use the internet. They cited having been assisted with internet use by either their siblings or their neighbours who were able to use the internet well.

This was also true in earlier studies, for example, Kortjan and Von Solms (2013) who argued that many parents were not knowledgeable of the threats apparent online and that they were unable to teach their children about secure online behaviour. As a result, the safety of children was also compromised. Lack of knowledge was viewed as an important factor that contributed to insecure online behaviour by Internet users. People are seen as a severe threat to each other's security" (Mitnick & Simon, 2001). Lack of relevant knowledge has made the African population easy targets for hackers and botnet operators (Kritzinger & Von Solms, 2012). Because of the consequences of the lack of knowledge, cyber-security, and awareness, therefore, become issues of fundamental importance.

4.1.2 Children taught on online abuse

The research asked children whether they had been taught about online risk. They were given two choices: Yes or No. The descriptive statistics were run and findings were as shown in table 2.

Table 1: Children on having been taught on online risks at school (n=370)

	Frequency	Percent
Yes	146	39.5
No	224	60.6
Total	370	100.0

Source (Field data, 2019)

The findings showed that 60.6% (224) of respondents reported not having been taught at school about risks online. It is worth noting that some awareness had happened in some schools as the study showed that 39.5% (146) agreed that they had been taught at school about risks online. This shows more should be done to improve online exposure and presence to better equip pupils for internet use and their security while they are online. This finding concurs with studies that showed some countries in Africa are ill-equipped to assist school teachers and learners with awareness and education as far as cyber-safety is concerned (Kortjan & von Solms, 2013 & Kortjan & Von Solms, 2014).

Teachers intervened in pupils' internet use by ensuring filtering software installed on computers that had internet, introduction to safe Internet use by teaching some safety skills although not well structured, and school policy which was not very adequate. Pupils had this to say about their teachers' intervention on issues relating to the use of the internet and the dangers of the same.

> *"The teacher* **r***estricts files to be opened or sometimes the tablets and laptops in our school do not have any programmes or games. Computers in our school are only installed with safe materials for learning. Some teachers do not know a lot of things on the internet. We can even show them." (Respondent 11, 2019)*

This finding concurred with the research that revealed that a whole school approach, where teachers and support staff can recognise, respond and resolve online safety issues was found to be effective in protecting and supporting students in their use of technology (Ofsted, 2014). For such an approach, teachers and support staff engaging in training on online risks and their implications is essential. One teacher had the following to say concerning restricting and protecting children online:

> *"We do not have formal policies relating to cyber safety concerning the incidences that would arise in the event a child is abused online." (Respondent 13, 2019)*

The study revealed that no specific formal policy was in place regarding the handling of cyber-safety risks that could occur among learners. Teachers and headteachers suggested that they would like policies and regulations to be standardized before being administered to schools by the Ministry of Basic Education.

Inquiring on the benefits using the internet showed that pupils appreciated that despite the dangers associated with the internet, it is necessary to use it because they would learn a lot through the internet. One pupil observed this regarding the internet and its benefits:

> *"Inasaidia kujua kitu hujui (Respondent 5).*
> *"It helps in learning."*
> *"For example, we can use the internet to send photos like a teacher sending photos to another teacher." (Respondent 5)*

The pupils were also aware that there were dangers as a result of using the internet. One respondent stated:

> *"Internet can be dangerous when used for, downloading bad videos, chatting with strangers, posting bad photos (like a naked person) or a photo of a person in short clothes, sharing photos without permission, sending abusive texts to abuse me or abuse others" (Respondent 6)*

About the dangers of online presence another respondent remarked:

> *"itatuma waharibu masomo"*
> *((Respondent 7, 2019))*
> "It affects learning outcomes"

This means that the pupils were aware that interaction online or accessing online sites would affect learning outcomes because of the time spent communicating or gaming or just having fun. Children appreciated and also understood why parents and other significant others helped them keep safe on the internet. Some were surprised that there could be a lot of danger when they interacted with the internet. Responding on parental protection on the use of the internet one said:

> *"My parent keeps away my phone when she finds me connecting to the internet.*

> *She sometimes hides the phone or sits there to see if I am watching bad things or playing bad music or just doing something bad to make the phone dirty or have a virus" (Respondent 10, 2019)*

On educational support, most students in a study in the UK reported having received some lessons on how to use the internet 23% (N=1326), while some which are translated as nearly one-third of the respondents 30% had not received lessons at all using internet. In these two scenarios, it is evident that there was some educational support needed which was done to some extent in a school environment (Livingstone, Bober, & Helsper, 2005).

The findings also supported study findings in a study in the United Kingdom which showed that only 5% of schools did not have an online safety policy in place. Yet for those schools that did, students were not always well informed about this: only 74% of students were aware that they had an online safety policy at school. Besides, few students were involved in writing online safety policies (Ofsted, 2014).

Furthermore, this concurs with another study that found out that **i**ncluding online safety within the school's curriculum was important for children to become safe and responsible users of technologies (Hinduja & Patchin, 2018). A survey conducted in the United Kingdom showed that 25% of secondary students could not recall "if they had been taught about online safety over the last 12 months" (UK Safer Internet Centre, 2015). Moreover, most schools use assemblies and ICT lessons to provide online safety education, which focuses on teaching children functional digital skills and providing them with one-way online safety messages, as opposed to interactive and dynamic pedagogy (Harrison-Evans & Krasodomski-Jones, 2017)

The Department of children's services was instrumental in creating awareness and also protecting children online. However, one respondent acknowledged that the responsibility of protecting children online required a concerted effort from various stakeholders as the researcher noted.

> *"The responsibility of online child abuse like many other issues within child protection is for everyone including the children themselves. It is the responsibility of the Department of Children's services as well as other Departments in other ministries and sectors like the Ministry of Education, Health among others only that there is a need for proper coordination. There are other partners like UNICEF, NGOs, Churches, and the Civil Society at large. The technical Group that we mentioned is also responsible, not forgetting parents of the children as the family is where this spend some time. A good example of the role we have played before was an interview I participated in on this specific area of child protection to create awareness" (Respondent 1, 2019)*

These findings concur with earlier studies like one that observed that the fight against cybercrime requires a coordinated effort among all stakeholders such as government bodies, educational institutions, business organisations, and law enforcement authorities (Wada & Odulaja, 2012).

4.1.3 Methods used to create awareness among children

Many children had experienced awareness creation as an intervention strategy to protect them from online abuse. Teachers used instruction in the form of lectures, video watching to see the dangers associated with the internet, gaming, and simulation. These findings concurred with a more recent study by Mabitle and Kritzinger (2020) which revealed that awareness creation methods were those delivered to protect children online. The methods were categorised to include: traditional, game-based, instructor-led, online, simulation-led, and video-based.

5. Conclusion and Recommendations

5.1 Conclusion

The study concluded that a multi-level approach would be used to enhance awareness creation by having each stakeholder take the responsibility to address child online abuse. Many have argued that there are standards and guidance for digital policymaking but what is missing is strong communication and dedication to addressing common issues with the needs of children at the forefront. This study concludes that children still need awareness creation on internet risks as well as opportunities it affords.

5.2Recommendations

Since this study like other studies showed that the fight against cybercrime, particularly online child abuse, requires a coordinated effort among all stakeholders such as government departments concerned with children matters, NGOs, educational institutions, business organisations, and law enforcement authorities. The ministry of education should revitalise the efforts to create awareness on internet risks among children within schools through the curriculum. The ministry of education can also work closely with the Directorate of Criminal

Investigation and the Department of Children's Services on modalities of creating awareness on the internet risks among children. The Department of Children's services needs to train their staff particularly child protection officers on ways of creating awareness among guardians, parents, and teachers.

At the school level, there is a need to create awareness on relevant policies or strengthen policy implementation especially those policies aimed at protecting children online. Teachers need to create more awareness by coming up with more innovative ways since some children were not aware of the risks posed by the internet. Parents' awareness of Internet security is a significant topic that should be discussed to raise knowledge and awareness among parents about internet threats, information protection, security issues, and cyberattacks so that they can teach their children how to use internet security. These awareness initiatives should be recognised within schools during parents for a.

Social work training institutions should incorporate an aspect of online child protection in the curriculum as a means of creating awareness on the emerging areas of social work practice that have not attracted much attention earlier. Future research may concentrate on the awareness parents have about using internet filtering software on computers for their children in the Kenyan setting.

References

Asongu, S. A., & Odhiambo, N. M. (2019). Basic formal education quality, information technology, and inclusive human development in sub- Saharan Africa. *Sustainable Development*, *27*(3), 419-428.

Baykara ZG, Demir SG and Yaman S (2015) The effects of ethics training on students recognising ethical violations and developing moral sensitivity. *Nursing Ethics* 22(6): 661–675. doi:10.1177/0969733014542673.

Bakó, R. K., & Tőkés, G. E. (2018). Parental Mediation and Romanian Young Children's Digital Practices. Revista Romana de Sociologie, 29(1/2), 23-36.

Bryman, A. (2016). *Social research methods*. Oxford university press.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Dushi, D. (2020). Combating the Live-Streaming of Child Sexual Abuse and Sexual Exploitation: A Need for New Legislation. *Second International Handbook of Internet Research*, 201-223.

Elgharnah, K. G. E. (2020). The Awareness of Parents Towards The Safe Use of the Internet (Doctoral Dissertation, Near East University).

Esposito, J., Lee, T., Limes-Taylor Henderson, K., Mason, A., Outler, A., Rodriguez Jackson, J., ... & Whitaker-Lea, L. (2017). Doctoral students' experiences with pedagogies of the home, pedagogies of love, and mentoring in the academy. *Educational Studies*, *53*(2), 155-177.

Godden, B. (2004). Sample size formulas. *Journal of Statistics*, *3*(66).

Goodstein, A. (2007). *Totally wired: What teens and tweens are really doing online*. St. Martin's Griffin.

Harrison-Evans, P., & Krasodomski-Jones, A. (2017). The Moral Web: Youth Character, Ethics and Behaviour. *Demos, London, www. demos. co. uk/project/the-moral-web*.

Hennink, M., Hutter, I., & Bailey, A. (2020). *Qualitative research methods*. SAGE Publications.

Herrero, S. T., Nicholls, L., & Strengers, Y. (2018). Smart home technologies in everyday life: do they address key energy challenges in households?. *Current Opinion in Environmental Sustainability*, *31*, 65-70.

Hinduja, S., & Patchin, J. W. (2018). Cyberbullying research summary: Cyberbullying and suicide. *Online: http://www. cyberbullying. us/myspace_youth_research. pdf*.

Islam, A. A., Mok, M. M. C., Gu, X., Spector, J., & Hai-Leng, C. (2019). ICT in higher education: An exploration of practices in malaysian universities. *IEEE Access*, *7*, 16892-16908.

Kaur, M., & Kumar, R. (2020). Mixed Methods in Global Health Research. *Handbook of Global Health*, 1-22.

Kortjan, N., & von Solms, R. (2013). Cyber security education in developing countries: A South African perspective. In *e-Infrastructure and e-Services for Developing Countries* (pp. 289–297).

Kritzinger, E. (2016). Short-term initiatives for enhancing cyber-safety within South African schools. *South African Computer Journal*, *28*(1), 1-17.

Kritzinger, E., & Von Solms, S. H. (2012). A framework for cyber security in Africa. *Journal of*

Information Assurance & Cybersecurity, *2012*, 1.

Mashiane, T., Dlamini, Z., & Mahlangu, T. (2019, February). A Rollout Strategy for Cybersecurity Awareness Campaigns. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019* (p. 243). Academic Conferences and publishing limited.

McFarlane, A., & Sakellariou, S. (2002). The role of ICT in science education. *Cambridge Journal of Education*, *32*(2), 219-232.

Mitnick, K. and Simon, W.L. (2002), The Art of Deception: Controlling the Human Element of Security, Wiley, New York, NY.

Mohammed, K. H., Mohammed, Y. D., & Solanke, A. A. (2019). Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria.

Myers, J. J., McCaw, D. S., & Hemphill, L. S. (2011). *Responding to cyber bullying: An action tool for school leaders*. Corwin Press.

Nath, S. (2019). ICT integration in Fiji schools: A case of in-service teachers. *Education and Information Technologies*, *24*(2), 963-972.

Nikolovska, M. (2020). The Internet as a creator of a criminal mind and child vulnerabilities in the cyber grooming of children. *JYU dissertations*.

Ofsted (2014) Briefings and Information for Use during Inspections of Maintained Schools and Academies, [online] Available at: http://www.ofsted.gov.uk/resources/briefings-andinformation-for-use-during-inspections-of-maintained-schools-and-academies.

Ong'ong'a, O. (2020). Approaches to safeguard children online in Kenya. Case of Children aged 12-14 years. *Case of Children aged*, 12-14.Limited. https://dx.doi.org/10.2139/ssrn.3617517.

Rahman, N. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology*, *10*(5).

Romero-Ruiz, K., Echeverri-Sánchez, L., Peña-Plata, J., Vásquez-Giraldo, S., Aguilera-Cardona, M., Herazo-Avendaño, C., & Bran-Piedrahita, L. (2017). Information and communication technologies impact on family relationship. *Procedia–Social and Behavioral Sciences*, *237*, 30-37.

Savirimuthu, J. (2011). The EU, online child safety and media literacy. *The International Journal of Children's Rights, 19(3),* 547-569.

Scholtz, D., Kritzinger, E., & Botha, A. (2020, July). Cyber Safety Awareness Framework for South African Schools to Enhance Cyber Safety Awareness. In *Computer Science On-line Conference* (pp. 216-223). Springer, Cham.

Semerci, A., & Aydin, M. K. (2018). Examining High School Teachers' Attitudes towards ICT Use in Education. *International Journal of Progressive Education*, *14*(2), 93-105.

Somekh, B., & Lewin, C. (Eds.). (2011). *Theory and methods in social research*. Sage.

Tangen R (2014) Balancing ethics and quality in educational research: The ethical matrix method. *Scandinavian Journal of Educational Research 58*(6): 678–694. https://doi.org/10.1080/00313831.2013.821089.

Teddlie, C., & Tashakkori, A. (2009). *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences*. Thousand Oaks, CA: Sage.

Wada, F., & Odulaja, G. O. (2012). Assessing cyber crime and its impact on e-banking in Nigeria using social theories. *African Journal of Computing & ICT*, *5*(1), 69-82.

Wu, D., Li, C. C., Zhou, W. T., Tsai, C. C., & Lu, C. (2019). Relationship between ICT supporting conditions and ICT application in Chinese urban and rural basic education. *Asia Pacific education review*, *20*(1), 147-157.