ACIT5930

MASTER'S THESIS

in

Applied Computer and Information Technology (ACIT)

May 2021

Universal design of ICT

Universal Design and Child Online Safety

Joyce Ndalaye, s339955

Department of Computer Science

Faculty of Technology, Art, and Design

Contents

Introduction

Protecting children from all kind of harm should be the primary object of every member of any society. Children are very vulnerable to all kind of danger in their lives as children because they are not able to make decisions on their own due to their immaturity in both physical, mental and emotional state as mentioned by UNICEF (2009). According to the United nations convention on the rights of the child (Butrymowicz), A Child is defined as “a human being younger than 18 years of age, unless majority under the law applicable to the child is attained earlier” while the ITU Roberts, McFarlane, and Magpantay (2008) defined a child as “individuals of the age 5-14 or younger”. It is important to protect the children and safeguard their wellbeing.

What is Child Protection?

According to United nations children’s fund UNICEF (2006a), Child protection can be defined as “Preventing and responding to violence, exploitation and abuse against children”. In response to this, child wellbeing should be considered as the key point whenever the whole concept of child protection is accounted. Child well-being can be viewed in six different perspective such as Material well-being, health and safety, behaviors and risks, education, peer, and family relations, as well as children’s own subjective sense of well-being. Bryce (2010) pointed out the major threats to children and young people in online environment being sexual exploitation, cyberbullying, and exposure to violent online contents. Different forms of exploitation and abuse expressed can either be physical, emotional, or sexual which all end up destructing the children’s well-being (Child’s well-being can be defined as the quality of child’s life). It is important to protect children as their right to be safe from every harm because they are very vulnerable to all kind of risks because of their immaturity (both physically and mentally) and lack of experience which gives opportunities to cyber criminals to penetrate and attack young people who are the target (Pereira, Spitzberg, & Matos, 2016).

What is universal design in relation to child protection?

According to the United Nations(UN) Universal design can be defined as “the design of the product, environment, programs and services to be usable by all people without the need of adaptation or specialized design" mentioned by G. A. Giannoumis and Stein (2019). Also, according to UN (2006) acting as the human rights instrument intended to ensure people with all kinds of disabilities enjoys the human rights and freedom, including the freedom to access and use of ICT services and products. The concept of universal design and child online protection comes as the way forward in finding out solutions to the safe guide and protect the rights of children while they are using the ICT products and the internet for different purposes. In so saying, protective environment is necessary to be in place as of UNICEF (2006c) which explained the need of having protective environment for all the children. Why Universal design and child online safety? Savirimuthu (2011), explained by examining the role of EU in enhancing the child's safety in an online environment by the use of public awareness and education strategies, by the role of the medias to make sure that parents all the people in the community are aware of the harm available in some online contents, and educate them on how they can protect children from it. The fact that children are very vulnerable victims to different forms of abuse and exploitation from online environment some rules, regulations and polices should be enforced to make children safe when they are using ICT products and services, as well as ensuring that all the contents and the materials are accessible and well protected to ensure no harm as the result of their innocence. The role of the media in advocating child protection in online and offline environment is a good practice and should be adapted by all nations Livingstone and Haddon (2009). The universality in the design of ICT products and services seek to be inclusive leaving no one behind especially children with disabilities and special needs. So, by applying the principles of universal design we will be sure that no one is left behind.

Research Gap: There are little research on how children and young people use internet in Africa and the low level of parental awareness and engagement regarding to the risks associated with usage of the internet by young people.

Aim of Research:

The aim of this project is to examine how ICT can be applied to promote the safety of children by identifying to what extent are children affected by using ICT products and services for different purposes and what are the ways which has been used to protect children from the harm arising due to the usage of ICT products and services.

Research Question: How do we ensure that children and young people can use ICT products and online technologies safely and satisfyingly as anyone else?

Considering how children and young people use internet. It is very important to understand how children use internet, understand the risks, and how parents, guardians and stakeholders of child protection are aware of what are the risks associated with the use of internet, in order to have strategic plans on how they will be able to protect them.

Literature Review

Previous research works which has been done regarding the how children use the internet, universality to the internet access, and has revealed different indicators showing that children are not safe in the online environment, and how exclusive it is when it comes to children with disabilities. Also, how parents and other child protection stakeholders associate themselves with child online protection.

Online risks

According (FHI 360) it was reported that the well-being of million children's life, physical and mental health are threatened by maltreatment such as abuse, negligence, exploitation, and violence. And that children whose parent or care givers are absent due to illness, death or abandoned are more vulnerable to the abuse and all form of exploitation UNICEF (2006b). Online risks are the danger and harm that might face children when using the internet without guidance, some of these online risks can be in the form of Cyber harassment, hate speech, cyber bullying as well child trafficking and kidnaping. However, ITU (2019) in child online report categorized these risks into four groups 1. Contact risks 2. Content risks 3. Conduct risks and 4. Contact risks

Cyber Harassment:

In the public health journal by Fridh, Lindström, and Rosvall (2015) Subjective health complaints in adolescent victims of cyber harassment, examining the effect of cyber harassment to the group of young, since it is becoming the public mental health concern to the young people in Sweden. The conducted survey among the adolescence portrayed that the girls were much vulnerable to face cyber harassment compared to boys at the age of 15, due to the fact that girls use most of their online moments to chat and view things in the social networks as described by Findahl (2012) while exposing themselves to the cyber attacker, while at the same time boy use their time in online environment to play games which make them less vulnerable to the people with bad intention to them. Also, the survey shows different ways in which the victims of cyber harassment and cyber bullying heal and reported that the victims were at least able to talk to people they trusted, either their friends, parents, teachers and social support teams, and they got relive. The only question remains on how to stop these cyber attackers. Also, cyber harassment has be directly linked to the disability

(Emerson & Roulstone, 2014) The research shows that people with disabilities are likely to face harassment than people without disabilities (either face to face or cyber harassment) this has been well described in (Alhaboby, al-Khateeb, Barnes, & Short, 2016) The language is disgusting and they refer to my disability. In most cases the cyber harassment offender act as having the disability to be able to hide their identities and in this way, it is easy for them to attack the victims and complete their harassment plans or else, the offender could try to connect to the person with close contact with the victim in the social networks and directly offend the victim. Sometimes the perpetrators tend to interfere the support system and provide false information to the victims, lowering the victims' self-esteem. The effects of harassment are higher as it leads to psychological torcher to the victim and some reported facing physical torcher, and if not stopped can lead to more suicidal cases.

However, Quayle and Jones (2011) explored the concept of Sexualized images of children on the internet. The fact that child sex offenders use different ways to exploit the children, using children's images or showing some sexual activities done to children which are of explicit in nature, while Mirkin (2009) criticized the assumption of harm by the fact that the majority of the images depict children not engaged in the acts, being harmful by themselves, and thus raise the need to validate the images which is very difficult as it is very hard for children to disclose being photographed. These activities are very harmful to child's moral behaviors and can cause trauma to the child as mentioned by Freyd (2002) . Although different researches show that there is available large number of child's exploited images online, but it seems that it is not easy to directly identify the victimized child while the perpetrator's true identity is not easily found, making it difficult to identify the effect of sexualized image to the society as it has been stated to become people's routine especially in western cultures as mentioned by Döring (2009).

Hate speech.

With the emerging of the Social Networks Systems (SNS) whose primary purpose was to connect people through sharing their photos, interests, hobbies and exchanging information to make people more socially connected according to (Del Vigna12, Cimino23, Dell'Orletta, Petrocchi, & Tesconi, 2017). Unfortunately, SNSs has become an open space for harmful information such as hate speech, cyberbullying and sexual predation (Kontostathis, 2009). The use of Social network is characterized by four features as mentioned by (Boyd, 2008) which act in favor of the perpetrators as a hiding place of their evil deeds. These characteristics of a profile in social network systems:

Persistence – The communication in social network systems are recorded and this extend the lifetime of the shared information in the internet. This extends the effect of bullying for a long time.

Searchability – Since all the information are recorded there is a possibility of the shared information to be searched by anyone for the purpose of connecting as friends and this can lead to the exposure of the child to the predators who can harm them in one way or another.

Replicability – As the result of information being searchable and available for anyone in the internet it is easy for the information to be reused, for example images and information being copied, edited, and reproduced in any other page and platform.

invisible audience – Online audience are invisible to the real world, making it is hard to verify the identity of the audience whether is real friend or a predator. This increases the risks that might face children when engaging themselves in uncontrolled activities and access to the internet.

Livingstone, Winther, and Saeed (2019) pointed out that “children are using social media before the minimum age of thirteen”, and from the above features of social Network sites, it shows the internet is not a friendly place for children and young people to access without guidance and supervision from adult, which impose high risk to the children.

Burgstahler (2009) explained the importance of universal design in adding the value in diversity and inclusiveness, meaning universally designed social network sites should not be designed targeting people of a specified geographic location, ethnic values, ability and disability to perform and understand particular tasks, since there is great interaction of different people including children and young people. As far as child protection is concerned the social networks and other applications should be universally designed to be accessed globally. Different people use Social Networks Systems for good reasons, but for some personal reasons other people join the Social networks for their personal motives known as trolls (Hardaker, 2010) whose intention is to spread hate speech and bully other people (children) or group of young people. The hate speech and bullying activities was identified following the study done in speech detection (Del Vigna12 et al., 2017) by the use of code where two different classifiers were used to identify some italic words and comments used to spread the hate speech and bully other people especially disadvantaged groups especially minors in some Facebook public newspapers, accounts of some politicians, musicians and others. Del Vigna12 et al. (2017) The results of the classifiers identified the existence of words and statements which show elements of hateful nature. The detection of hate speech and bullying in the social networks can be improved by having a system which will be able to detects the words and statements as soon as they are posted and eradicate them from being shared and spread. It is now possible to identify face identities in the social network with the use of detection mechanism which compare the harasser's information in relation to the reality.

Taking into consideration universal design as a way forward in achieving inclusion and equal accessibility to all children, the same concept should be considered to ensure equal child safety while they are using the internet. G. Giannoumis and Paupini (2020) pointed out the importance of inclusion and safety of the child to the policy makers and law regulating authorities, content creators to establish technical, procedural, and legal measures to safeguard child experience while using the internet. Also, identified how hate speed and cyber bullying affect children especially children with disabilities and the most disadvantaged group, while giving a room for new researchers to work on identifying different solutions that will detect and trigger the hate speech against disadvantaged groups of children and hence measure the extent to how this is the problem that affect the children.

Cyber bullying:

Cyber bullying has been defined as “the use of electronic messages to harass, threaten or target another person” according to UNICEF. While D'Auria (2014) defined cyberbullying as the “deliberate and repeated use of information technology by an individual to harm or embarrass another person or group”. According to Cross, Piggin, Douglas, and Vonkaenel-Flatt (2012), the main target of cyberbullying (as well as traditional bullying) are children and young people who are vulnerable groups such as children with disabilities, members of minor ethnic groups, lesbians, gays and transgender. Popovac (2012) pointed out the nature of cyber bullying being more aggressive to tradition bullying due to the fact that the people in the internet (perpetrators) remain unknown to the victims making it possible for the bullying activities to occur repeatedly at any time and any place without being noticed by the parents and care givers, this is because "children and young people did not trust adults to understand cyber bullying and respond to it" said Li (2006). To what extent is cyber bullying affecting the children? According to Van Geel, Vedder, and Tanilon (2014) the effect of cyber bullying which is as much as traditional bullying was related to suicidal attempt, as children did not get immediate support to the recover from the effects of bullying. Other effects of cyber bullying has been described by Kowalski, Limber, and Agatston (2012) being depression and psychological problems, anxiety and fear of rejection, loneliness and isolation, offline victimization as well as poor parent-caregiver relation. Bullying has intensively been explained in the article of Risk and Safety on the internet, European kids' perspective (Lobe, Livingstone, Ólafsson, & Vodeb, 2011) . It is well illustrated by statistics how the children were bulled and the frequency in which the bullying happened while showing the comparison of the situation among the European countries where the research has been conducted. The extent of bullying activities is subjected to increase since children who had been bulled had high possibility to bull others either online or face to face. Although the face to face bullying is more common in most of the places the online bullying tends to have much effect as the image or text can spread to many peers especially in social networks and can be read repeatedly for long period of time due to the characteristics of social networks and internet (persistent and scalability) as describe by Boyd (2020).

Parental involvement and monitoring of children online activities is the best way to ensure children's safety (Ybarra & Mitchell, 2004). While, Dishion and McMahon (1998) pointed out that parental control and mediation enable parents to monitor their children's activities and people they are communicating with. But how are parents monitoring children online activities and what is the level of parental-caregivers engagement to help end bullying? Lobe et al. (2011) pictured out how bullying happens among kids, showing different level of parental engagement among the EU countries. Taking example of the countries such as Norway, Sweden and Finland where the level of parental/children engagement was pointed to be low, in some occasions parents were said to report that their children has been bulled while the children say they are not, and in the countries where the level of parental and children engagement is high, then it seems that children can report that they have been bulled while parents could say that it was not a bullying. The study portrays that most of the bullying activities takes place in the offline (19%) environment than it occurs in the online environment (12%), while the largest number of those who were bulled online had bulled others in an offline environment. Most of the bullying activities occurs among the children between 9- 16 years of age, rather than how it occurs in minors. Also, the study shows that most of the bullying activities occurs in the social medias than it occurs in other means of online communication such as email and instant messaging. Nonetheless, Bullying has been reported as less threat in developing countries following the report of Initiative (2016) case study conducted in Egypt reviled that the main risk is inappropriate contents, followed by virus and spyware as well as violent contents. At the same time the survey showed that children are not monitored by the parents or guardians when using the internet, this expose children to all types of dangers and attack from people with bad intentions. It is important that children are aware of

Child traffic and kidnaping:

According to the U.N Protocol to prevent, suppress and punish trafficking in persons, especially women and children Enck (2003) defined Child trafficking as "the recruitment, transportation, transfer, harboring or receipt of children for the purpose of exploitation" this violate children's rights and well-being causing denial to their opportunities and reaching their potential. In the digital era child trafficking is mostly facilitated by the internet as argued by Bhutia (2000) saying the internet is not only by people with good intentions, but also by the people with bad intention. Child trafficking and kidnaping come as the results of unsupervised children's access to the internet, where people with the wrong intentions can get access to children, and young people and cause harm including trafficking and kidnaping. It was also stated how important it is to protect children's information due to their vulnerability in the online environment as children share their information with trust, while having little or no knowledge about cyber space security which put them in more risk, as well as affecting their personal growth and wellbeing as stated by United Nations Children's fund UNICEF (2009).

Through the internet the trafficker can act as any anyone else and promise different things to the child, the trafficker take advantage of what the child is missing from parents or care giver (children showing signs of loneliness) which can either be love, attention, moral support as well as material things, while setting up the appointment to meet face to face and start to build trust with the child before fulfilling their bad intention to the victim as mentioned by Jordheim (2014).

There are different forms of child trafficking which are facilitated by the internet mainly targeting child labor and exploitation as it has been mentioned by OIM (1985), describing the work as hazardous which Bonded labor, commercial sexual exploitation and prostitution, drugs couriering and soldiering. Similarly, Santana, Kiss, and Andermann (2019), explained the factors which lead to child labor and exploitation being associated with societal problems like poverty, marginalization and lack of decent work to the parents, which cause more effects to the children including limited access to education, limited time to interact with family and other children losing their right to play, dream and being happy as a child. The above mentioned forms of child labor has been categorized by UNICEF (2009) as for girls are much engaged in commercial sexual exploitation and prostitution while boys are more engaged in forced labor and soldiering in which some of them can be involved in terrorism (Smahel & Wright, 2014). Different impacts child trafficking has been mentioned by (Kowalski et al., 2012) such as, psychological trauma and depression, loneliness and isolation, offline victimization as well as poor parent-caregiver relationship.

Information literacy, digital skills, access, and opportunities

According to Fourie (2021) children use the internet than any other medium to communicate and socialize, pointing out different technologies and platforms used such as e-mail, instant messaging, multiplayer for games and different social networks systems. Understanding the level of awareness of the parents, teachers, care givers and other child protection stakeholders in developing countries where parents/ guardians are faced with lack of enough digital knowledge and skills. According to UNCEF Innocent research center report UNCEF (2011) portrayed that there is lack of awareness or discomfort among parents and agencies with responsibilities for children protection concerning the nature of hazards and effective protection strategies as the awareness seems not yet to be integrated in the systems, where most of them might have been the victims of the cyber threat, regardless of the fact that parents, child protection services, service providers and other stakeholders show a significant concern on the safety of the child in online environment as it was described by Bryce (2010). However, children have shown high ability and expertise in their usage of ICT compared to most of the parents, while Li (2006) pointed out children lacking trust to their parents and care givers to understand and solve cyberbullying issues without aggravating their situation, and hence become very vulnerable to different risks due to available evidence of sexual exploitation committed to children.

Parental engagement in child online protection is one of the key solution that help to keep children safe in an online environment, as mentioned in child online safety and parental intervention by Tennakoon, Saridakis, and Mohammed (2018). since children are not aware of the danger associated with the internet usage and all the harm that the child can be exposed to such as sexual exploitation, cyber harassment, cyberbullying, and exposure to violent online contents. This study explored in detail and gave reflection of how different ways of parental intervention within parents of different demography, with different ICT experience and exposure, as well as cyber space harassed victims can bring the positive influence to their children's behavior by directly talking to them about the really impact and harms associated with the use of online platforms. Other ways described in the report (UNICEF) to keep the children safe was by parents blocking the harmful sites, filtering the sites as well as regular monitoring of the devices used by children such as mobile phones, tablets, and computers. The fact that boys and girls use the internet for different purpose , as it has been discussed by Notten and Nikken (2016) where boys tends to engage risk online activities than girls, and that boys are in great danger of facing cyber harassment than girls. However at the same time the studies shows that girls pay much attentions and act accordingly to whatever advise they are given with their parents regarding the harm and dangers associated with internet contents as they mediate than it is with boys, and this make boys more exposed to the cyber attackers mentioned by UNICEF (2011). Similarly different literatures explained the inclusion behavior and attitudes about children with developmental disabilities, as mentioned by Alkhateeb, Hadidi, and Alkhateeb (2016) in their reviews on the attitudes and perception of inclusion and the barriers to inclusion. Among the barriers to digital inclusion, parental guidance and collaboration towards child online protection is digital divide, Digital Divide in technology. According to different literatures it has been revealed that there is a huge gap between parents, teachers, care givers and children in the use and understanding of technology where children seems to know much than their parents, teachers and care givers on how to operate different technologies and this expose them to more dangers as they are out of control. Young and Tully (2019) expressed the need of parental awareness and participation in child online protection as the research showed that parents knew less on the risks that their children might face when access the internet unguided. Meanwhile most children and young people do not prefer to involve parents (Young & Tully, 2019) in whatever the situation and experience they are going through the internet (whether good or bad) as they do not trust adult to have understanding of situation (Li, 2006), with the fear of parents would have different reactions, where some of them could over react towards the problem to the extent of forbidding their children from accessing the internet, which make children to distant themselves from their parents.

Also, the digital divide is caused by the so called “Digital natives” and the “digital Immigrants” as it has been described by Prensky (2006), where most of the adults are termed as digital immigrants due to the fact that they started using the internet and technology while in their old age, while the children and young people were born and grew up with the internet and technology and hence termed as “digital natives”, this can also be termed as “digital generation gap” - which is the gap between generation when parents, teachers, care givers were born and grew up, with that of the children, the difference is always significant to the extent of leaving behind most of the parents, teachers and care givers in terms of their thinking and operating through the digital devices and technologies. This is caused by the low digital literate level in the old generations where many people in developing countries did not get the opportunities to go to school and acquire formal education and digital knowledge, and hence lack important skills and knowledge to guide their children in regards to the use of technology, including the risks and opportunities of using technology. In this situation most adults struggle to catchup with the digital changes, which cause the digital gap between most of the parents/ guardians and that of children to be very high. Other factors for digital divide are caused by gender inequality where women in developing countries are less digital technology users as compared to men and they are financially dependent, poverty, lack of awareness and absence appropriate education curriculum in schools on how children can be safe when using the internet and technology.

Creating Protective environment

(Guidelines and regulations, Universal design of ICT)

It is very necessary to think of how online environment can be protected and made safe for everyone especially children and the most disadvantaged groups such as children, young people including children with disabilities. To achieve this there should be great involvement to whoever is involved with child protection services such as teachers, parents, social workers, policy makers and other stakeholders, by raising awareness of child protection service. (Von Weiler, Haardt-Becker, & Schulte, 2010) pointed out the lack of knowledge and awareness among social workers on the risks associated with the internet abuse, educating them on the nature of risks and how to protect children in both online and offline environment, while encouraging children to be open to what they find as unusual experience or any harmful contents so that they can stay safer. Understanding the proper reporting channels to the crime will help the minors very much on their safety, also, by putting all the regulations and guideline to protect children from being hurt in both online and offline environment.

Guidelines and policies

These are the rules and declaration designed to guide parents, teachers, policy makers, service providers and care givers on the best practice to guide and monitor children's activities when using the internet and technology. The guidelines give directives on laws and legislations that can be used to ensure children's safety and wellbeing.

Legislation of law to protect children in developing countries

Despite availability of different laws and guidelines that guide different stakeholders (Parents, Policy makers and service providers) on how and what they can do to make sure that children's safety can be achieved, this is not the same situation in the developing countries where the guideline protocols has been signed but not implemented. (Brennan et al., 2019) mentioned lack of sufficient and robust mechanisms being the main contributor to failure to protect children from online risks, as it makes it hard for prosecution and case management. The lack of robust and mechanisms can be in form of laws and legislation as well as technological resources and capacity to perform cyber investigation. (Schia, 2018) argued that, changes in development of technology goes faster than the laws and legislation are updated, this cause failure in completion of investigation at the required time where, in some cases the laws may not been updated. There are different guidelines imposed by the ITU to act as the directives for all the stakeholders but it has been revealed that in most developing countries it is not implemented, including the countries that the data were collected in this research.

According to (ITU, 2016) There are different guidelines to be followed by parents, guardians and educators to make sure that children are safe when using the internet. Different guidelines have been explained as well as different ways in which parents, guardian and educators use to help children to be safe in the internet by blocking harmful sites, keeping records of visited sites, installing parental control software's from the mobile providers as well as installing antiviruses.

Universal Design of ICT:

From the above mentioned guidelines are consistent with the CRPD's definition of 'universal design', UN (2006) meaning that the design of products, environments, programs and services are to be usable by all people, to the greatest extent possible, without the need for adaptation or specialized design. Universal design does not exclude assistive devices for groups of people with disability where this is needed. Despite accessibility being the tool to enhance participation and inclusion, it is also one of the human rights as mentioned by UNCRPD which is to be enjoyed by everyone. However, Ekstrand (2017) portrayed that people with disability still face challenges form inaccessible web sites and mobile applications which make them less participatory. Parents with disabilities has the rights to protect their children as it is to other parents without disability. Foggetti (2012) pointed out the importance of accessible ICT products and services in promotion and protection of the rights of people with disability. To increase participation designers and developers should consider creating inclusive and accessible contents to people with different disabilities as mentioned by Harper and Chen (2012).

According to Ferri and Favalli (2018), The seven principles of universal design has been elaborated in a way that web contents and mobile applications can be inclusive to everyone including people with disability, where everyone can perceive, understand, navigate and interact with web contents and different applications as mentioned by Peters and Bradbard (2010).

Principle 1: Equitable use Design that is useful and marketable to persons with diverse abilities.

Principle 2: Flexibility in use Design that accommodates a wide range of individual preferences and abilities.

Principle 3: Simple and intuitive use Design that is easy to understand, regardless of the user's experience, knowledge, language skills, or concentration level. So, simplified technologies and applications will attract more parental engagement towards child online protection.

Principle 4: Perceptible information Design that communicates necessary information effectively to the user, regardless of ambient conditions or the user's sensory abilities. Creating contents that can be perceived in different format by people with different abilities.

Principle 5: Tolerance for error Design that minimizes hazards and the adverse consequences of accidental or unintended actions. The design that can give enough time for user to interact with the system.

Principle 6: Low physical effort Design that can be used efficiently and comfortably and with a minimum of fatigue. The design that can allow different users to navigate the contents and applications in their own preference, example screen contrast adjustment and portrait.

Principle 7: Size and space for approach and use Design that provides appropriate size and space—for approach, reach, manipulation, and use.

Considering universal design to break the barrier between parents, teachers, and care givers toward their engagement in child protection activities, parents regardless of their ability to operate in the mobile app, they should be able to access the parental control program.

Universal design of Parental control Program.

These are programs created to monitor and control child's activities when using internet. Universal design of parental control programs and applications can be used to accelerate more parents and care givers to participate in child online protection. Human diversity is the catalyst for universally designed applications and program implementation so that it can be usable and accessible to as many parents/ care givers as possible. However, Thierer (2009) argued that, technological control tools cannot be used as a substitute for education, mentoring and good parenting as they are not perfect, instead it works the best in combination with educational efforts and parental involvement.

Despite availability of several parental control tools such as Norton online family, K9 web protection, MacAfee family and others which at most did not provide complete solution said Srl and Chancen (2012), while Fuertes, Quimbiulco, Galárraga, and García-Dorado (2015) suggested for more advanced features with characteristics such as allowing centralized database, feature that allow remote access the application and verify children activities and measure the security level of their home while away. Also, suggested addition of functionality which will alert the parents and caregivers about different attempts done by the child in the internet which will increase the level of parental engagement on children activities. By removing the accessibility barriers in the applications parents will have no excuse in protecting their children in online environment, However, removing the accessibility barriers alone cannot make parents and care givers more engaged to protecting their children, regular training and raising awareness among different communities should be adapted as it was mentioned by O'Brien and Li (2020) "Parent trainings should be similarly targeted on Internet safety for children and emerging child grooming techniques via the Internet. Most participants suggested parental training on how to monitor their children's Internet use including a list of Internet based apps, usernames and relationships with others on the internet".

Despite the availability of a lot of different child control tools, it's usability is still low by most parents and guardians as described by Fuertes et al. (2015) in their parental control tools evaluation, by confirming that parents did not know how to block access to web contents and not all did the supervision. This is the same case in most developing countries parents and guardians face different challenges to access the tools, one of challenges being Language barrier, which cause them to participate less in child protection engagement, leaving children exposed to more harm in the internet.

Research Methodology

In this section, I explain how I have researched the topic and collect data. Following different research evidences, and reached a decision to which method I will use in order to gather the information I need, and which approach I will use to analyze the data I collected and get the results of my research.

Qualitative and Exploratory Research:

Why Qualitative research? The research aims to identify the human emotions and behaviors towards the use of internet and technology by children and young people, Qualitative method will be much advantageous to quantitative research. According to Madrigal and McClain (2012) they described the qualitative research as the type of study that aim to provide you with details about human behavior, emotions and personal characteristics which cannot be obtained using the quantitative research. And because we are intending to find a solution (design a product or service) that will help in protecting children while using the internet and online environment, it is important to get the information like user behavior, routine, desire, routines, use cases and other important information. Punch (2013) explained the qualitative research approach as a method used to obtain the quality data, unlike the quantitative research approach which aims to quantify and obtain the numerical data, due to this reason which suffice my needs to obtain the quality of data, it gives me more reasons to choose the qualitative research approach to investigate my topic of interest. However, Simons (2009) described “Case study as in-depth exploration from multiple perspective of complexity and uniqueness of particular project, policy, institution, program or system in real life”, as we are seeking to get the answers to complex reality and meaning of the actions happening in the online environment the qualitative approach gives more meaning as it was mentioned by Maxwell (2012) that the qualitative approach deals with the aspect of reality which cannot be quantified as qualitative research works with the universe meanings, motives, aspirations, beliefs, values and attitude of the phenomena under investigation.

Nevertheless, Astalin (2013) explained the conceptual framework of qualitative research designs, in this research am convinced that the best way to do it is by exercising the qualitative method since the research is curious in identifying the experience of Children when using the internet including their safety. Using Phenomenology qualitative approach, we will be able to collect the information concerning their experience, while finding out different policies exercised to protect the child. In this case when we refer to the Research Question which seek to understand how children are safe and how different policies are helps in protecting the well-being of children when online.

How will I use qualitative approach to research my topic?

Spriggs (2010) in his revision provided guidance to consent as ethical issues when it comes to researches that involves children and young people while presenting the model for best practice. The revision used different case studies to justify the consent issue as the ethical problem in Human research related cases. So, instead of using children as participants in this research Parents, Teachers, care givers and Social worker will be employed as our research participants, However informed consent is very necessary to the research participants as it was mentioned by Denzin and Lincoln (2011) that “participants should be well informed of the purpose of the research, what will be asked from them and the way the data will be used, as well as clarifying the confidentiality of the data and their identity, safety and security while giving them the flexibility to withdraw from participating in their research when they feel that it is no longer ok2.

Why qualitative methodology? Because we want to understand intensively how children are safe in the online environment, case study is the suitable method for us as it can be described by Travers (2001) we will use case study and phenomenology as qualitative approach to collect the information that will give the answer to my research question and generate the findings and observations which will leading to finding solutions which will save the best interest of the children. Yin (2011) explained in detail three different types of case studies being, Explanatory (the case study that seek to answer the questions which are sought to explain the expected cause of the problem in in real life circumstances), **Exploratory** (to explore the situations whose intervention or phenomena in which they are evaluated is not clear) and descriptive (used to describe intervention or phenomena in real life situations in which they occur). Due to nature of my topic of interest the exploratory case study will be appropriate to the answer of my research as I will be exploring different phenomenon on how the child is safe in online environment. G. Giannoumis and Paupini (2020) pointed out the need of exploring more in the field of universal design and child online safety since there is not much researches in child protection.

Research Ethics

Developing a good and trust relationship between the researcher and participants or the researcher and the research area is the key to successfulness of the research work. I am aware that I will be conducting my research in developing country which is characterized by population which is vulnerable due to low level of economy as well as education as it was mentioned by Punjwani (2015), in this case I am obliged to observe integrity of the vulnerable population to avoid any form of exploitation. According to the Norwegian National Committees for Research Ethics the concept of "research ethics" refers to a diverse set of values, standards and institutional arrangements that contribute to constituting and regulating scientific activities. The fundamental ethos of research is search for trust. As part of the international researchers I will have to adhere to social responsibility of the community in which I am aiming to conduct my research. Keeping the genuine consent of the research participants should be a key consideration throughout the research work, whereby I will be responsible to clarify the real purpose of my research and why I request for their consent, also to maintain the good relationship among the area of research and the community where the research is done, as well as the relation among researchers, and researchers and other people in the community.

However, scientific integrity, truthfulness and accountability are the required fundamental research ethics. I have an obligation to familiarise myself and observe research ethics guidelines that are relevant to my research type.

Scientific integrity: I am aware that, am responsible for respecting the research results of others and for exercising good scientific practice. I must not conceal, misrepresent, or falsify anything, whether in the planning, executing, or reporting of the research. I will avoid plagiarism and acknowledge the work of others and give balance and good representation in the way I represent their ideas in my work, and I will be accountable for my actions.

Protection of Research Subject: Also, it is my responsibility to keep openness as a fundamental standard in my research work. At the same time, I am aware that, there are areas where it is necessary to safeguard the privacy of the research subjects, particularly when sensitive information is collected. Information about the persons taking part in the research project, or about others with whom I will become acquainted during the research process must be handled with care. I must inform participants about how the information will be protected and stored. I will also provide confidentiality or anonymity for those who want it. By confidentiality means all information and data are de-identified, i.e. no unauthorised persons will be able to know who has provided which data to the research.

Declaration:

I Joyce Ndalaye, I acknowledge that I am a part of an international community of researchers. I will practise my activities in line with the recognised standards for good research practice. I shall conduct my research in an honest and truthful way and show respect for humans, animals, and nature. I shall use my knowledge and skills to the best of my judgement for the good of humanity and for sustainable development. I shall not allow interests based on ideology, religion, ethnicity, prejudice, or material advantages to overshadow my ethical responsibility as a researcher.

Participants and Data Collection:

Using the exploratory qualitative research to explore the answer to the question, how are children safe in online environment? Different methods of data collection can be used. However, Yin (2013) explained in detail how to use exploratory case study. We will use questionnaires and interview (which will be conducted with individuals who have been clearly explained the purpose of the research, why their answers to the interview questions are very important for the research while assuring their confidentiality and safety of their identity as the research is going to deal with human characteristics, behaviors and emotions on the real life case studies.) The interviews have been conducted in an online platform by sending the link containing all the necessary information together with information letter through email.

Participants and Sample size: The research has been done and data collected from 6 countries in the global south (Congo, Kenya, Mozambique, Tanzania, South Africa, and Zambia). 15 participants (5 female and 10 male) have been involved in answering the interview questions which was shared to them online through email containing the link to data collection tool. However, informed written consent was distributed to all the participants with all the necessary information about the research prior to their engagement in answering the interview questions. The participants sampling was done randomly among the groups of people who are directly involved in child protection (parents, teachers, and care givers). Participants were asked about their awareness about child online protection, including children's online activities, risks and opportunities, what parents/ guardians do to make sure that children are safe, and their opinion concerning child online safety. Three groups of participants with close experience in intervening with children, are good source of information. The data has been collected from teachers, parents and social workers or people who are working very close with the children and has good understanding of whatever kind of challenges children are facing when they are using internet and services.

Contents mapping: different sample of questions have been used to provide answers to different collected data which has been grouped to form different themes which provided answers to the research question. Example of questions which has been mapped in the research can be found in Appendix 1 attached in this thesis:

Data Analysis:

In this research, thematic content data analysis has been used (by fracturing the data obtained and arrange the compared data which fall under similar categories) as explained by Strauss (1987). Also, the data has been analyzed as they were collected, as it has been described by Coffey and Atkinson (1996) that “data analysis to be conducted simultaneously with data collection as the basic principle of qualitative research”.

Data analysis:

In this research three themes emerged from the collected data. **Online risk**, as it is for any other internet users, this theme identifies risks associated with the use of internet by children as they are more vulnerable to risks if their internet and technology usage will not be monitored. **Information literacy and Digital skill** is another theme which identifies how parents, social workers and teachers are informed about online child protection and the level of skills they have when it comes to how to keep their children safe when using the internet. Lastly, it is **Access and opportunities** theme which describe different activities children do when accessing the online environment using different devices.

Thematic and content analysis

Theme	**Contents**
Online risks	-Sharing of personal information and identity to the strangers -Child trafficking and kidnapping. -Bullying. -Psychological trauma. -Social addiction and self-isolation. -Behavior change
Information literacy and Safety skills	

Information Literacy	How parents get information about child protection -Exchange information from peer parents, friends, and churches -From internet -Information from TV documentaries -Nowhere (self-informed) What do parents do when a child gets new device -Discuss with the child on proper use of the device -Set up password protection. -Installing parental control program. -Linking the child’s device to that of the parent.
Digital safety skills	-Password protection -Limiting the internet access time to the device when used by a child. -Talking and educating the children on the risks associated with the use of internet without parental guidance. -Disconnecting the device from the internet when parents are away from children. -Linking the child’s device with parents’ email address as access control.

Access and opportunities	How are children accessing the internet? Children and young people use internet as the media of communication, learning and entertainment. - Online studies - Playing games and watching cartoons, movies - Social media such as YouTube kids, Instagram, twitter, WhatsApp - Downloading cartoons, games, and photos. **Access and use** Almost all the participants mentioned that their children had access to technology and internet through -Mobile phone, tablet, and computers (Laptops + desktop) **Opportunity** - Exploring new knowledge. - Connecting with friends and socialization - Learning platform, attending class and doing schoolwork

Results:

1. Online Risks

The use of internet by children comes with a lot of risks which must be taken into consideration for children to be safe while having great experience in using the internet, here are some of the risks that have been identified by participants in this theme which might put children's wellbeing in danger.

Several participants expressed their concern on how children can share their personal information and identity to the strangers which is very dangerous. This has mentioned by participant ID 08 "*can share their personal information unknowingly*" and participant ID 05 mentioned "*giving personal information to unknown people who can misuse their information and destroy their future*".
Participant ID 14 said "*share personal information with strangers*". Children are vulnerable to online environment due to their age and reasoning ability, for this reason it is very dangerous when children provide their personal information and identity to the strangers as it can expose them to more risks such as child traffic and kidnaping, sexual exploitation as well as cyber bullying .

However, Child trafficking and kidnaping is the risks associated with unsupervised access to the internet, where children trust and provide their identity to the stranger which may have many effects to the child. This has been identified by the participant ID 04 "*Child traffic and kidnapping*", and participant ID 09 "*It is easy for children to find the wrong friends online who are not good and kind to them because the process of finding them did not involve parents or guardians, this can lead to children being deceived and then scammed*".

Participant ID 04 said *"without proper monitoring they can fall into trafficking, kidnapping and other networks of destruction*". Participant ID 10 said" They *are likely to be exposed to child pornography, child and human trafficking*". this shows that, when children have unsupervised access to the internet it is very easy for the child to trust any friend they find online, give their personal information such as names, age, and address to the strangers whose intention is unknown to the children, there is a high risk that the stranger can easily get access to the child with the possibility to fulfill bad intentions such as child kidnapping, trafficking and sexual exploitation.

Similarly, several participants expressed their concern on children being bulled when online as the results of children sharing their identity to the strangers. According to participant ID 07 "*children being bulled*". Participant ID 14 saying "*online bullying and harassment*". Cyber bullying is another risk which can face a child when using the internet without supervision which will give chance for strangers to bully the child in cyber space after spreading of rumors, threats, pictures and sexual remarks which in turn will destroy child's self-esteem, imposes fear and psychological trauma which will eventually degrade their morals, behavior and social interaction.

The effect of bullying to children can results into psychological trauma as it has been mentioned by several participants. Participant ID 06 mentioned that "*Children may experience psychological trauma*". When a child has been bulled is likely to develop psychological trauma due to moral degradation and destructed self-esteem which will make a child to feel insecure, loose of social interaction with other children and parents as the trauma will make a child to have self-isolation as the way to feel safe which is not good for both mental and psychological health which when not acted in time can lead to damage in the physical health .

Several participants argued on the addiction effecting children when they have unsupervised and unlimited internet access. According to participant ID 03 the effect can be "*To be addicted and not to be able to socialize with their peer*" also, participant ID 04 mentioned children can be "*Addicted to the extent that they skip their meals and sometimes become lazy to accomplish their duties such as studies*", and participant ID 9 added that "*A waste of time by spending much of their time learning things that are not useful to them such as news of celebrities and gossips*". This show that unsupervised access to the internet for the children can cause more harm, this kind of addiction can also cause mental and psychological health problems to the child as they tend to isolate themselves from others which can cause more damage in their growth.

Health problem has been expressed as another potential risk that might affect children when having uncontrolled/ unsupervised access to the online environment. This has been mentioned by participant ID 12 "*Health problems such as vision problems, neck* *pain and overstain as well as reduced sleep quality*". The mentioned health problems are directly associated with the children using the internet and technology unlimitedly, when children spend much time on electronic devices and internet will encounter both eyes defect, neck pain as well reduced sleep quality, this very obvious and a thing to be considered by all the parents, teachers and guardians for the well-being of children.

And finally, the other risk discussed by most of the participants is behavior change to the children due to access to harmful and inappropriate contents. According to participant ID 05 "*Behavior change in negative way after accessing inappropriate contents*". Examples of inappropriate contents has been said by participant ID 07 "*Searching and accessing adultery contents e.g. Access to pornographic materials*". While participant ID 09 added "*Learning things that are not appropriate for their age, thus exposing them to the risk behaviors such as sex and drug abuse*". The harmful contents mentioned by participants can totally change a child behavior which might affect other children as well in long run, and the effect of accessing inappropriate contents can go as far as causing the impact in offline environment where the victim tends to practice what has been shown online and this lead to moral degradation.

2. Information literacy and digital safety skills:

This theme focuses on understanding how parents, teachers and social workers are informed on different issues regarding how to protect their children when using internet and the level digital skills on how they can support their children. In this way they will be able to keep children away from the above-mentioned risks.

2.1 Information literacy

This sub-theme seeks to understand where and how parents, teachers and social workers get information on how to protect their children and what do they do when their children get new devices or technologies. Where and how parents, care givers and teachers get information on how to protect their children? Several participants mentioned different ways in which they use to get information on how and where they get information about online child protection.

Several participants mentioned that they get information from family, friends, and care givers. According to participant ID 01 "*From peer parents and friend by exchanging their experience and apply it*". Participant ID 03 said "*from care givers and my wife*", while participant ID 04 said "*exchanging ideas with friends and try to implement it*" Showing that most of the important information about how to keep children safe while using the internet they get from other parents and friends; this implicate that the information can reliable or the other way around.

Whereas other participants expressed that they get information from the internet and social media. According to participant ID 01, 02, 05, 06, 09, 11 mentioned "*From Internet*", also, participant ID 07 said "*social media*" and participant ID 08 said "*From websites checking the parenting guideline, some websites always display the condition for guidelines and you can accept or denied*". Internet and social media has been a source of information to many people, parents and care givers can get the information about child protection as well as understanding the best practice used by other people and by this way they can use techniques to protect their children as well, there are a lot of useful information available in the internet.

Availability of different TV documentaries with child online protection contents has been used to inform parents/ guardians on the best way to keep children safe in online environment. According to participant ID 04 I get information from "*TV documentaries*", participant ID 04 said "*We get information about child online protection from TV documentaries*", by watching TV documentary they get some information which gives them information and knowledge to take more precaution from what has been shown by different characters concerning child online protection.

Churches and other community institutions play a great role in providing basic and important information to keep their community safe. Others participant mentioned that they get information about child online protection from church and fellow parents. According to participant ID 05 "*I get information from church seminars and from fellow parents*". Community services such as churches has been used to equip parents and their congregations with the necessary knowledge about the best practice to protect children from online risks.

As part of the societies there are other members who show their concern on lacking clear information on where they can get information and directives on child protection especially in online environment. According to participant ID 06, mentioned that "Nowhere". The participant lacks information on where to get the information and is not getting information from any source, he just does what he thinks will protect the child, this imposes high risk to children as they will have no guidance on safety use of the internet.

Also, parents have shown different responses regarding what they do when their children get new devices.

Several participants mentioned that they talk to their children on the proper use of the device. According to participant ID 01 he said that "*I discuss with the children regarding the appropriate use of the device*". And participant ID 15 said "*teach them what is not good and what is good for them*". Meaning that the parent explains and discuss with the child on what is a good practice on proper use of electronic devices and technology, this is one among the effective ways to quickly educate children on how to be safe from the cyber space and the cyber predators.

Similarly, several participants expressed their concern on restricting the device with password and creating different profiles. According to participant ID 03, said "*I restrict the device with password*". Also, participant ID 15 said "*Apply password protection for downloads or adult content access*". Also, "*Profile creation on tablets, profiling helps configure right contents for kids*" By restricting the device with password will help in controlling the child from directly accessing all the program installed in the device, the child will have access to the electronic device and internet after the parent/ guardian allowing them to have access to it, this will minimize the risks of children having direct access to the device and internet on their own.

Also, some participants talked about installing the parental control program and removal of unwanted program in the device. Participant ID 02 "*Installing parental control program and uninstall unwanted programs for the kids"*, while participant ID 15 said "*Remove all applications like games which are not suitable for their age*". By installing the parental control program and removing unwanted programs the child will be only allowed to access contents and applications which has been reviewed and approved by the parent or guardian, and this will ensure child's safety when using the device, the parental control program will have different functionalities which will help in protecting children from accessing unnecessary contents from the internet.

Regarding the use of different guidelines as a standard of information to guide parents, teachers and other child protection stakeholders to acquire enough information on how to keep the children safe, participant ID 08 said "*The parent guideline will help to protect the child as it will prevent him/her exposed into abusive actions*", guidelines are the directives/ rules to guide different stakeholders on how to act upon to make sure that children are safe in both online and offline environment.

By connecting the child's device to that of parent will also ensure parental follow up on children's activities. This has been mentioned by participant
ID 05 "*Connecting the child's device to that of the parent to monitor all the activities*". Participant ID 04 said "*Linking parents' email to the device so that they can agree on what programs a child can watch"* In this way parents/ guardians will be able to monitor their children even at a distant since the child will not have access to internet without parental/ guardian approval, and thus keep children safe from accessing harmful contents.

2.2 Safety skills:

This sub-theme aims at exploring the safety skills acquired by parents, teachers, and care givers on protecting children online. Things parents do to protect their children from the risks:

Several participants suggested that devices used by children should be password protected. According to participant ID 07 "*Setting access control like password to some of the application*".
Participant ID 01 "*Password protection*".
Participant ID 02 "*By putting password on the prohibited sites or applications*".
Protecting the device and some application using password is one way to restrict a child from having access to inappropriate contents, and this can also be done by creating separate user account to the devices so that children will only have access to their verified account which will keep them safe from accessing harmful contents.

Similarly, several participants said they limit the time for their children to access the internet. Participant ID 01 said "*I schedule time for internet use*". Participant ID 03 "*Sometimes I do limit their time on the internet*". ID 04 "*One of the techniques is to keep limits on what they can check and use in the* *internet*". ID 05 "*Make sure you monitor the time the time use when they are using internet*". Participant ID 05 "*Giving them limitation of access*". ID 14 "*I only give access to the App that the child would want to access on specific time to ensure that they focus and do only what they planned to do*". Scheduling the time to when, how long and what children can have access to the internet is one way of reducing the chances that a child will be addicted by spending more time to the internet, while giving the parents or guardians time to participate in monitoring every activity done by the child at the specified time.

Talking to children about their safety when using internet is the best way parents can do to raise awareness about the risks to their children. This was mentioned by several participants: Participant ID 04 "*Educating the children on the importance of safe usage of internet*", also participant ID 08 "*I motivate them before going to the device to share with me what exactly he/ she want to know*". Participant ID 12 "*Talk openly with your child about their online activities*". Participant ID 09 "*Teach the children on the importance of focusing on contents safe for them".* Participant ID 05 "*Teaching them the importance of using the internet, what to download and what not to, as well as the consequences of downloading materials that will not be helpful to them*". In this way children are aware of what are the risk they might face when they are not guided, this help children to be open and more friendly to their parents to the extent that they can share their experience and challenges they are facing in the internet, which will help parents/ care givers to be more attentive and protective.

However, participants have expressed different ways on which to control children activities while they are away. Here are some of these ways on how parents monitor their children's activities.

Several participants suggested that for children to be safe, they should not be allowed to access internet when parents are not around. Several participants mentioned this, according to participant ID 06 "*No direct access to online information is allowed in parent's absence, only access to downloaded content*". participant ID 10 said "*I try not to allow access to the internet in my absence, I make then use offline activities*".

Participant ID 12 said "*Allowing the access of internet on my presence out of that I* *download the materials and fun games and leave them without internet access*".

This can be one of the traditional way to ensure that the child is safe when parents are not available to monitor/ supervise their children's activities, but in the other hand it will not give children freedom to explore new ideas and information when they need in the absence of their parents and guardians.

Similarly, other participants expressed how hard they find it to control their children activities while they are away. According several to participants ID 01 "*it is difficulty to monitor while away*" and participant ID 04 added "*it isn't easy task, because nowadays children are more agile in using technology than their parents and also very clever*". It is difficult to monitor children activities because most of them are using Mobile devices such as mobile phones and tablets, so it is hard to monitor their activities, especially when the child is not at home or connect to different networks wireless network in particular since some of the rules applied to child protection are associated to the network connecting the device (some of the rules for child online protection can be set to the network devices such as routers and switches).

However, due to difficulty in monitoring children's activities as the impact of development of technology where devices are more potable and mobile, Participant ID 04 said "*Linking parents' email to the device so that they can agree on what programs a child can watch*". While participant ID 15 said "*I keep the device, they can only have access to them when am around*" and "*By tracking search attempts made on YouTube for kids*". connecting child's device to the parent's email, is to ensure that whenever a child access the internet through the connected device, then parent will receive an email notification on the activity that the child is doing, and the parent can approve that, and by keeping the devices away from the children when parents are not around helps to prevent children from accessing inappropriate contents.

3. Access and opportunities:

This theme highlights the opportunities children get through the use internet with different technologies. Participants shared their views on how children are using internet and the types of devices they use.

Online practices have been expressed in different thoughts from one participant to another, as children tend to have different activities when online. According to participant ID 06 "*children and young people use internet as the media for communication, learning and entertainment*". As children are having different activities which has been categorised as communication, learning and entertainment. This has been supported with different participant's view as follows:

As a media of communication, where children use the opportunity to communicate with friends and family as well as getting information from online sources. Several participants mentioned, according to participant ID 01 the child use the internet for socialization purpose "*Social media*", which was more elaborated by participant ID 07 as "*Through social media (YouTube kids, Instagram, twitter, WhatsApp and google)*". By using the mentioned apps children get the opportunity to communicate with others, socialize and uplift their self-esteem, and this is due to the fact that in today's world children are faced with a lot of risks and thus, cannot be allowed to walk or visit around their friends without parental/ guardian's supervision, in this case the use of social media act as a very common way for children to keep in touch with friends.

As a media for Learning and education opportunities, the emerging of internet and technologies made it possible for children and young people to acquire education through the internet. According to participant ID 01 "*Online studies*", participant ID 14 said "*searching school information and do assignments*" Several participants said their children use the internet for learning and studying purpose, and this has shown significant effect during the Covid-19 pandemic where children and young people could not go to school and hence had to adopt the online studying mechanisms, which helped all the children to keep track with their school curriculum.

As the media for entertainment children use internet for playing games, watching cartoons and movies. Participant ID 07, 06 mentioned "*playing games, watching cartoons and movies*", participant ID 13 said "*to access online games as well as kids platforms*" Children and young people as any other internet users need some time to refresh and entertain themselves through playing online games, cartoons as well as watching movies. All these activities help in entertaining and refreshing the children.

Children use different devices to access the internet, most of the participants said their children access the internet through mobile phones, tablets, laptop, and desktop computers. Due to advancement of technologies more portable devices are used.

Summarized results: According to this study, there are three emerged themes which relate to each other leading to content mapping which gives us the results of our study. The main theme in this study is Online risks which has direct connection with other two themes (Information literacy & digital skills and Access & Opportunities), It is possible to understand the online risk associated with the children's use of internet by having correct information about what are the important things to consider before allowing children to have access and opportunities to use ICT technologies and services including the internet.

as described in the figure below.

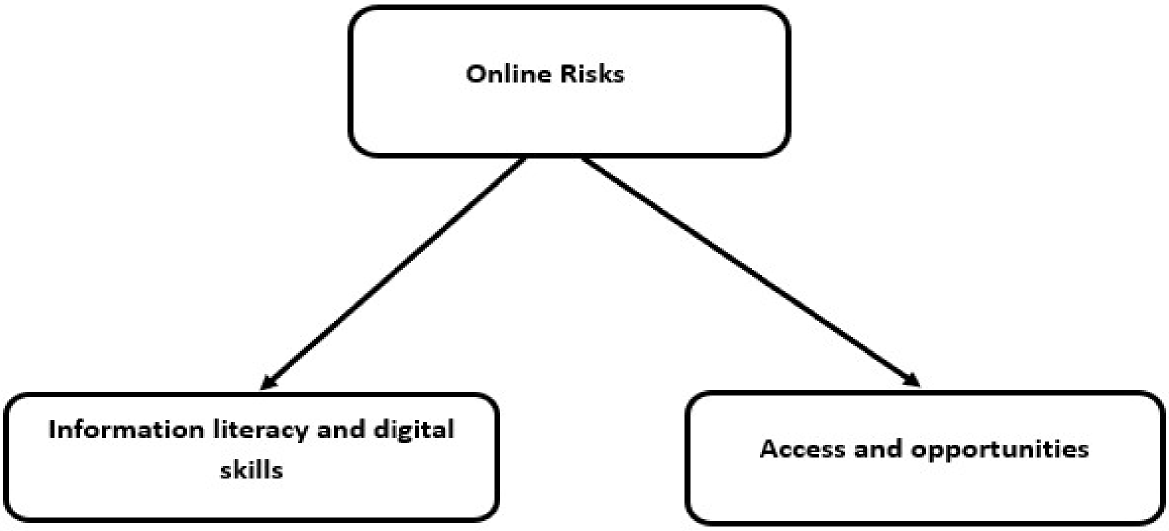


Figure 1. Describing the connection between the three themes emerged from the data analysis.

Discussion:

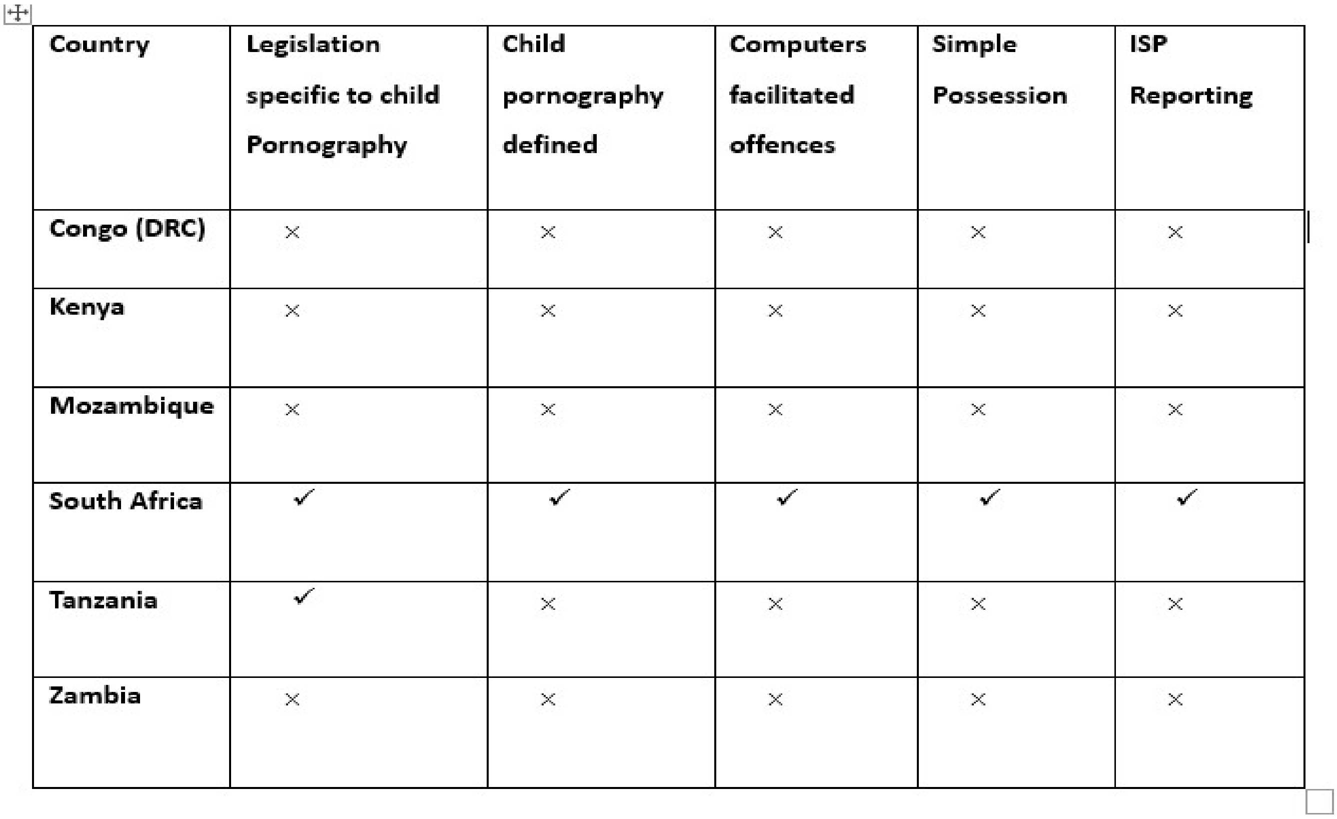
How do we ensure children can use ICT products, services, and online technologies safely, efficiently, and satisfyingly as anyone else? By understanding the online risks associated with children usage of internet can help to promote children's safety and efficiency experience in their growth as the parents, teachers and social workers are aware of what to do to keep their children safe from accessing and getting exposed to inappropriate and harmful contents, connecting with unknown friends who can have bad intention such as bullying, kidnapping and child trafficking. Also, by helping to control addictions which might lower their social esteem and cause psychological trauma as parents, teachers and care givers will be able to track everything the child is doing as it has been explained in the below paragraphs.

In previous research, Popovac (2012) pointed out importance of adults being aware of how to protect children online, urging that without adults awareness it not possible to protect children from online risks. In this research participants have shown different level of awareness on how they can protect their children. Having the right information and skills on what to do to promote children's safety and experience as they use online environment, different technics has been used by parents, teachers, and social workers to ensure children's safety, efficient and satisfaction. By controlling children's time to access the internet to avoid addictions, setting parental control programs which can restrict, filter the contents and applications. This has also been shown in previous research by (Fuertes et al., 2015) in their recommendation on the additional features to the parental control application, similarly in this research it has been suggested that parental to be installed on child's device and linked to parent's device, in this way parents/ care giver will be able to follow up what the child is doing even when at a distance. Also, by educating the children on the online risks can promote their safety and experience.

Understanding children's online practices, access and opportunities will help parents and care givers on proper management of what a child can access depending on the device and technology used. this way child safety and good experience will be promoted, this has also been pointed out by (Ybarra & Mitchell, 2004) saying "to ensure children's safety while using the internet, parental involvement and monitoring was very essential". For example, the use of social media without limit is harmful to children, but if parents and care givers regularly visit what a child is doing then the child will be protected and have good experience. This thesis has proven the same when some participants said “I motivate them before going to the use the device to share with me exactly what she/ he want to know” and others mentioned that they talk to their children concerning their safety when using the internet by explaining what do and what not to do especially on what to access and what to share in the social networks.

Similarly, ITU (2016) explained how different guidelines has been established to be followed and used by parents, policy makers and service providers (who are the main actors of child online protection) as a guide to create safer environment and children online protection instructor. This thesis has also shown that the use guidelines can help equip parents and other stakeholders with necessary information to keep their children safe. The use of guidelines will also provide all the necessary instructions on how parents can make follow up on what their children are doing online, such as how to restrict some sites, applications, and web contents, also how different stakeholders such as policy makers and service providers can make and amend different laws which will safe guard the best interest of the children. ITU (2014) provide different guidelines for the industry to follow to keep children safe. The need to advocate the use of available guidelines to equip parents, teachers, care givers, police makers, service providers, and other child protection stakeholders on safer ways to be adapted for their children to use internet safe and satisfactory is to be promoted. Despite availability of different laws and guidelines that guide different stakeholders on how and what they can do to make sure that children’s safety can be achieved, this is not the same case in the developing countries where the guideline protocols has been signed but not implemented. There are different guidelines imposed by the ITU to act as the directives for all the stakeholders but it has been revealed that in most developing countries it is not implemented, including the countries that the data were collected in this research. The below information has been retrieved from (ITU, 2009) which can act as an example to how different policies and guidelines are not implemented, this put more risks to the children because whenever the crime happens there is no laws in place which will be used to convict the perpetrator.

The diagram below is the evidence of lack of laws and regulations in most of the countries which makes it hard for service providers to be held accountable as it has been described by ITU (2019)



Country	Legislation specific to child Pornography	Child pornography defined	Computers facilitated offences	Simple Possession	ISP Reporting
Congo (DRC)	×	×	×	×	×
Kenya	×	×	×	×	×
Mozambique	×	×	×	×	×
South Africa	✓	✓	✓	✓	✓
Tanzania	✓	×	×	×	×
Zambia	×	×	×	×	×

(Von Weiler et al., 2010) pointed out lack of knowledge and awareness among social works associated with internet risk and abuse, the author mentioned that without awareness of the risks and abuse, it is very difficult to keep children safe from online risks. This thesis has shown the evidence that lack of information on how to keep children safe when using internet and online risk awareness is among the challenges facing different communities in developing countries, which has shown by most participants not knowing exactly where to get information concerning the online risks and what do to protect their children from online risks. 95 percent of all the participants in this thesis are not aware of where to get information regarding child online protection, For this reason, many children in developing countries are at the potential risks if the governments, parents and other stakeholders will not take immediate actions to solve this problem. ITU (2014) instruct industry to work with NGO's and government to raise awareness among the community, in this way all the relevant child protection stakeholders will be equipped with necessary information, especially the reporting channels.

Kontostathis (2009) pointed out how social networks is harmful by saying "Social Networks Services has become an open space for harmful information such as cyberbullying and sexual predation". This has also been identified in this thesis as some of the risks that children are facing online when using internet without adult's supervision. A lot of risks are associated with the use of social media networks by children without supervision, some of the risks identified in this thesis are cyberbullying, cyber harassment, child trafficking and exploitation. The effect of cyberbullying can lead to mental health and lowering the children's self-esteem as it has been shown in this thesis. And in the literature review the danger of social networks has been expressed as the results of all the information in the internet being recorded over a long period of time, ability of the information to be edited, duplicated and then be circulated all over the internet and put more children at risk of cyber bullying, child trafficking and other forms of exploitation.

However, Tennakoon et al. (2018) expressed how parental intervention plays a great role in child online protection. This has also been justified in this thesis, it shows how parents use communication to keep their children aware of the danger and risks that they might face when they use the internet unguided. Informing the children about the safe way to use technology will give children confidence to share with parents or guardians whatever they face in the online environment, and this will save on the best interest of children.

Following the above discussion, am convinced that there are different ways which can be done to promote children's safety in the internet. Universally designed parental control application can be one of the tools which will allow parents to monitor their children even when they are not with them and ensure their safety. In this research I designed KID Control application prototype with some universally designed features such as language option, automatic report generation from children's devices to that of parent/ guardian. This will promote child safety and will be an answer to some challenges that parents, and guardians are facing on how to monitor their children activities.

In this report I have designed the layout of the summary of the main operations of the proposed application. I attach the use case, sequential diagram, and example of application prototype in the appendix1 and appendix 2 attached in separate documents.

Limitation of the study:

Due to Covid-19 pandemic situation it was not possible to do the field work, which could provide diverse participation in data collection, and give more diverse results. In this case only participants with email address had a chance to participate, so only literate (participants with digital skills) participants were involved. This contributed to having a smaller number of participants.

It was not possible do the data collection through online video conferencing due to the expenses of the internet connectivity to the participants side, it is very expensive for them and they could not afford to participate.

It was not possible to reach out participants with special needs to know their experience on how they can protect their children.

Recommendations:

For the future research, to increase number of participants from all groups of child protection stake holders.

Conclusion

The three themes emerged in this thesis (online risk, Information literacy and digital skills, Access, and opportunity) together with other previous works gives a ground in finding the solution to children safety. Although Child online protection has been mentioned by UNICEF as global challenge, but the way to solve these challenges should be handled in consideration to different context such as level of development and literacy among different societies. ITU (2014) pointed out the need of the industry in national and international level to contribute in raising awareness among the community. The level of digital literacy in developing country is very low, so a different approach to child protection mechanism should be taken, and different strategies and guideline to educate the parents, care givers and child protection workers should be adapted depending on the socio-cultural and economic level of the society.

For the future research work, the mixed research method can be adopted, where quantitative research approach will help in providing large amount of data which will give the clear picture of the number of participants contributed and their performance towards child online protection. More qualitative work is required to include all the groups of stakeholders without exclusion, example collecting information from young and older parents, parents with different disabilities, parents/ guardians with and without digital skills, as well as participants with different social economic status. However, policy makers and industries available in these countries to be part of the research to have their contribution. Despite of availability of different parental control tools, their accessibility and usability is not convincing in developing countries, more accessible and customized tools are required as well as raising more awareness to the communities.

References

Alhaboby, Z. A., al-Khateeb, H. M., Barnes, J., & Short, E. (2016). 'The language is disgusting and they refer to my disability': the cyberharassment of disabled people. *Disability & Society, 31*(8), 1138-1143.

Alkhateeb, J. M., Hadidi, M. S., & Alkhateeb, A. J. (2016). Inclusion of children with developmental disabilities in Arab countries: A review of the research literature from 1990 to 2014. *Research in developmental disabilities, 49*, 60-75.

Astalin, P. K. (2013). Qualitative research designs: A conceptual framework. *International journal of social science & interdisciplinary research, 2*(1), 118-124.

Bhutia, J. W. (2000). INTERNET AND VULNERABILITY OF CHILDREN IN CONTEMPORARY SOCIETY. *IX*(VII).

Boyd, D. (2008). Why youth (heart) social network sites: The role of networked publics in teenage social life. *YOUTH, IDENTITY, AND DIGITAL MEDIA, David Buckingham, ed., The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning, The MIT Press, Cambridge, MA*, 2007-2016.

Boyd, D. (2020). *It's complicated: The social lives of networked teens*: Yale University Press.

Brennan, M., Perkins, D., Merdian, H., Tyrrell, E., Babchishin, K., McCartan, K., & Kelly, R. (2019). Best practice in the management of online sex offending.

Bryce, J. (2010). Online sexual exploitation of children and young people. *Handbook of internet crime*, 320-342.

Burgstahler, S. (2009). Universal Design in Education: Principles and Applications. *DO-IT*.

Butrymowicz, M. 1. The Convention on the Rights of the Child–an introduction.

Coffey, A., & Atkinson, P. (1996). *Making sense of qualitative data: Complementary research strategies*: Sage Publications, Inc.

Cross, E., Piggin, R., Douglas, T., & Vonkaenel-Flatt, J. (2012). Virtual violence II: Progress and challenges in the fight against cyberbullying. *London: Beatbullying*.

D'Auria, J. P. (2014). Cyberbullying resources for youth and their families. *Journal of Pediatric Health Care, 28*(2), e19-e22.

Del Vigna12, F., Cimino23, A., Dell'Orletta, F., Petrocchi, M., & Tesconi, M. (2017). *Hate me, hate me not: Hate speech detection on facebook.* Paper presented at the Proceedings of the First Italian Conference on Cybersecurity (ITASEC17).

Denzin, N. K., & Lincoln, Y. S. (2011). *The Sage handbook of qualitative research*: sage.

Dishion, T. J., & McMahon, R. J. (1998). Parental monitoring and the prevention of problem behavior: A conceptual and empirical reformulation. *Drug abuse prevention through family interventions, 177*, 229.

Döring, N. M. (2009). The Internet's impact on sexuality: A critical review of 15 years of research. *Computers in Human Behavior, 25*(5), 1089-1101.

Ekstrand, V. S. (2017). Democratic governance, self-fulfillment and disability: Web accessibility under the Americans with disabilities act and the first amendment. *Communication Law and Policy, 22*(4), 427-457.

Emerson, E., & Roulstone, A. (2014). Developing an evidence base for violent and disablist hate crime in Britain: Findings from the life opportunities survey. *Journal of interpersonal violence, 29*(17), 3086-3104.

Enck, J. L. (2003). The United Nations Convention against Transnational Organized Crime: Is It All That It Is Cracked up to Be-Problems Posed by the Russian Mafia in the Trafficking of Humans. *Syracuse J. Int'l L. & Com., 30*, 369.

Ferri, D., & Favalli, S. (2018). Web Accessibility for People with Disabilities in the European Union: Paving the Road to Social Inclusion. *Societies, 8*(2), 40.

Findahl, O. (2012). Swedes and the Internet 2013. *Stockholm:. se, internetstatistik*.

Foggetti, N. (2012). Special Briefing-e-Accessibility Standards Definition in the UN Convention on the Rights of Persons with Disabilities: Current Issues and Future Perspectives. *Computer and Telecommunications Law Review, 18*(2), 56.

Fourie, L. (2021). Protecting children in the digital society. *CHILDHOOD VULNERABILITIES IN SOUTH AFRICA*, 229.

Freyd, J. J. (2002). Memory and Dimensions of Trauma: Terror May be" All-Too-Well Remembered" and Betrayal Buried (From Critical Issues in Child Sexual Abuse: Historical, Legal, and Psychological Perspectives, P 139-173, 2002, Jon R. Conte, ed.--See NCJ-201288).

Fridh, M., Lindström, M., & Rosvall, M. (2015). Subjective health complaints in adolescent victims of cyber harassment: moderation through support from parents/friends-a Swedish population-based study. *BMC public health, 15*(1), 949.

Fuertes, W., Quimbiulco, K., Galárraga, F., & García-Dorado, J. L. (2015). *On the development of advanced parental control tools.* Paper presented at the 2015 1st International Conference on Software Security and Assurance (ICSSA).

Giannoumis, G., & Paupini, C. (2020). *Universal Design and Child Online Protection.* Paper presented at the Cambridge Workshop on Universal Access and Assistive Technology.

Giannoumis, G. A., & Stein, M. A. (2019). Conceptualizing universal design for the information society through a universal human rights lens. *International Human Rights Law Review, 8*(1), 38-66.

Hardaker, C. (2010). Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions.

Harper, S., & Chen, A. Q. (2012). Web accessibility guidelines. *World Wide Web, 15*(1), 61-88.

Initiative, J. (2016). *A Policy Brief on Child Online Protection in Ghana*. Retrieved from

ITU. (2009). Guidelines for policy makers on Child Online Protection. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP

ITU. (2014). Guideline for Industry on Child Online Protection.

ITU. (2016). Guideline for Parents, Guardians and Educators on child online protection. Retrieved from http://www.itu.int/COP

ITU. (2019). *Child online safety: Minimizing the risk of violence, abuse and exploitation online*. Retrieved from https://hivdev.gn.apc.org/library/documents/child-online-safety-minimizing-risk-violence-abuse-and-exploitation-online

Jordheim, A. (2014). *Made in the USA: The Sex Trafficking of Americaâ€ TMs Children*: HigherLife Publishing.

Kontostathis, A. (2009). *Chatcoder: Toward the tracking and categorization of internet predators.* Paper presented at the PROC. TEXT MINING WORKSHOP 2009 HELD IN CONJUNCTION WITH THE NINTH SIAM INTERNATIONAL CONFERENCE ON DATA MINING (SDM 2009). SPARKS, NV. MAY 2009.

Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). *Cyberbullying: Bullying in the digital age*: John Wiley & Sons.

Li, Q. (2006). Cyberbullying in schools: A research of gender differences. *School psychology international, 27*(2), 157-170.

Livingstone, S., & Haddon, L. (2009). *Kids online: Opportunities and risks for children*: Policy press.

Livingstone, S., Winther, D. K., & Saeed, M. (2019). *Global kids online comparative report*. Retrieved from

Lobe, B., Livingstone, S., Ólafsson, K., & Vodeb, H. (2011). Cross-national comparison of risks and safety on the internet: Initial analysis from the EU Kids Online survey of European children.

Madrigal, D., & McClain, B. (2012). Strengths and weaknesses of quantitative and qualitative research. In.

Maxwell, J. A. (2012). *Qualitative research design: An interactive approach* (Vol. 41): Sage publications.

Mirkin, H. (2009). The social, political, and legal construction of the concept of child pornography. *Journal of homosexuality, 56*(2), 233-267.

Notten, N., & Nikken, P. (2016). Boys and girls taking risks online: A gendered perspective on social context and adolescents' risky online behavior. *New Media & Society, 18*(6), 966-988.

O'Brien, J. E., & Li, W. (2020). The role of the internet in the grooming, exploitation, and exit of United States domestic minor sex trafficking victims. *Journal of Children and Media, 14*(2), 187-203.

OIM, I. (1985). Child Labour.

Pereira, F., Spitzberg, B. H., & Matos, M. (2016). Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents. *Computers in Human Behavior, 62*, 136-146.

Peters, C., & Bradbard, D. A. (2010). Web accessibility: an introduction and ethical implications. *Journal of Information, Communication and Ethics in Society*.

Popovac, M. L., lezanne. (2012). Cyber bullying inSouth Africa: Impact and responses. *Center for Justice and crime prevention*(No. 13).

Prensky, M. (2006). Digital natives, digital immigrants: Origins of terms. *Updated version of Marc Prensky's blog post of June, 12*, 2006.

Punch, K. F. (2013). *Introduction to social research: Quantitative and qualitative approaches*: sage.

Punjwani, S. (2015). Issues of research ethics in developing world. *J Clin Res Bioeth, 6*, 6.

Quayle, E., & Jones, T. (2011). Sexualized images of children on the Internet. *Sexual abuse, 23*(1), 7-21.

Roberts, S., McFarlane, J., & Magpantay, E. (2008). *Use of Information and Communication Technology by the World's Children and Youth: A Statistical Compilation*: International Telecommunication Union.

Santana, V. S., Kiss, L., & Andermann, A. (2019). The scientific knowledge on child labor in Latin America. In: SciELO Public Health.

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

Schia, N. N. (2018). The cyber frontier and digital pitfalls in the Global South. *Third World Quarterly, 39*(5), 821-837.

Simons, H. (2009). *Case study research in practice*: SAGE publications.

Smahel, D., & Wright, M. F. (2014). The meaning of online problematic situations for children: results of qualitative cross-cultural investigation in nine European countries.

Spriggs, M. (2010). Understanding consent in research involving children: The ethical issues. *A handbook for human research ethics committees and researchers. Melbourne: Children's Bioethics Centre*.

Srl, C., & Chancen, S. D. (2012). Benchmarking of Parental Control Tools for the Online Protection of Children SIP-Bench II. Assessment Results and Methodology 4th Cycle. In: Bruxelles: INNOVA Europe.

Strauss, A. L. (1987). *Qualitative analysis for social scientists*: Cambridge university press.

Tennakoon, H., Saridakis, G., & Mohammed, A.-M. (2018). Child online safety and parental intervention: a study of Sri Lankan internet users. *Information Technology & People*.

Thierer, A. D. (2009). Regarding Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video or Audio Programming, Filing by Adam Thierer of the Progress & Freedom Foundation to the Federal Communications Commission Mb. Docket No. 09-26. *Progress & Freedom Foundation Agency Filing, April 2009*.

Travers, M. (2001). *Qualitative research through case studies*: Sage.

UN. (2006). convention-on-the-rights-of-persons-with-disabilities. Retrieved from https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities/article-2-definitions.html

UNCEF. (2011). Retrieved from http://www.unicef-irc.org/publications

UNICEF. (2006a). Retrieved from https://www.unicef.org/protection/files/What_is_Child_Protection.pdf

UNICEF. (2006b). Child protection from Violence, Exploitaion and Abuse. Retrieved from http://www.unicef.org/protection

UNICEF. (2006c). What_is_Child_Protection.pdf. Retrieved from https://www.unicef.org/protection/files/What_is_Child_Protection.pdf

UNICEF. (2009). Child protection from violence, exploitation and abuse. In.

UNICEF. (2011). Child Safety Online Global challenges and strategies. Retrieved from https://www.unicef-irc.org/publications/pdf/ict_eng.pdf

Van Geel, M., Vedder, P., & Tanilon, J. (2014). Relationship between peer victimization, cyberbullying, and suicide in children and adolescents: a meta-analysis. *JAMA pediatrics, 168*(5), 435-442.

Von Weiler, J., Haardt-Becker, A., & Schulte, S. (2010). Care and treatment of child victims of child pornographic exploitation (CPE) in Germany. *Journal of Sexual Aggression, 16*(2), 211-222.

Ybarra, M. L., & Mitchell, K. J. (2004). Online aggressor/targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of child psychology and psychiatry, 45*(7), 1308-1316.

Yin, R. K. (2011). Case study research: Design and methods by Yin, Robert K. *The Modern Language Journal, 95*(3), 474-475.

Yin, R. K. (2013). Case Study Research Design and Methods, 5th Revise. In: Sage Publications Inc.

Young, R., & Tully, M. (2019). 'Nobody wants the parents involved': Social norms in parent and adolescent responses to cyberbullying. *Journal of Youth Studies, 22*(6), 856-872.

Appendix 1: INTERVIEW GUIDE FOR DATA COLLECTION.

Question 1: In what ways are children and young people using internet?

Question 2: Can you describe some of the typical activities that children do online?

Question 3: What are the potential consequences that a child might face when using internet without parental guidance?

Question 4: What are the things that you do to protect your child when using internet? Describe both technical and non-technical.

Question 5: What do you understand by the term parental control program? How do you use it to protect your child?

Question 6: When a child gets a new device/ technology what are the things that you do to keep them safe?

Question 7: Where do you get information about child online protection? How do use the information?

Question 8: How do you monitor what a child is doing on internet in your absence?

Question 9: What are the negative impacts/ risks associated with the use of internet and technology by the children?

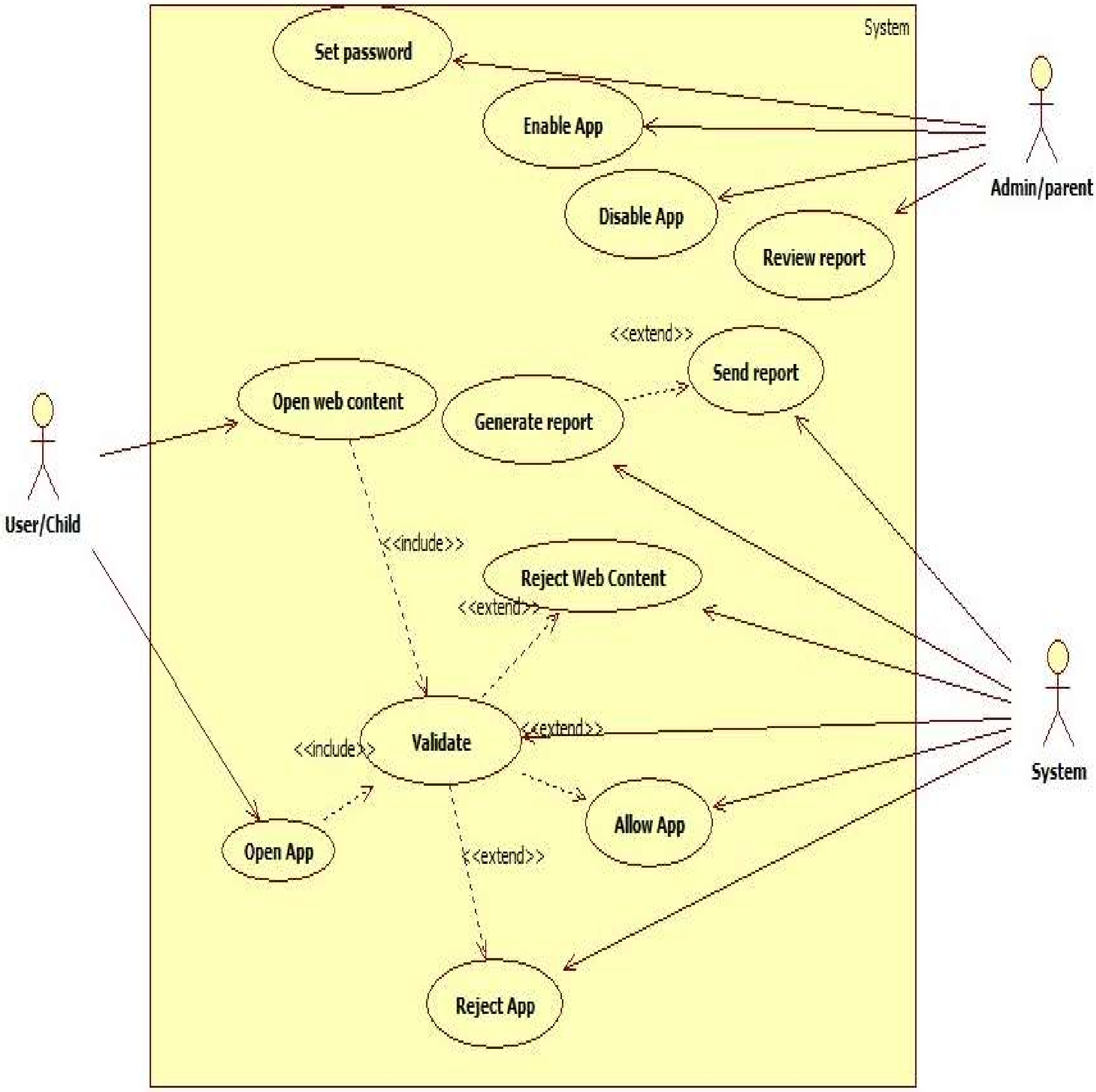
Question 10: What is your opinion on children’s experience in using ICT technologies and devices

Appendix 2: KID CONTROL APPLICATION DEVELOPMENT

Software engineering

Use Case Diagram

This diagram shows the different operations which can be performed by the primary actor (Child) and the secondary actors (Admin and system). The diagram shows the actor's operations.

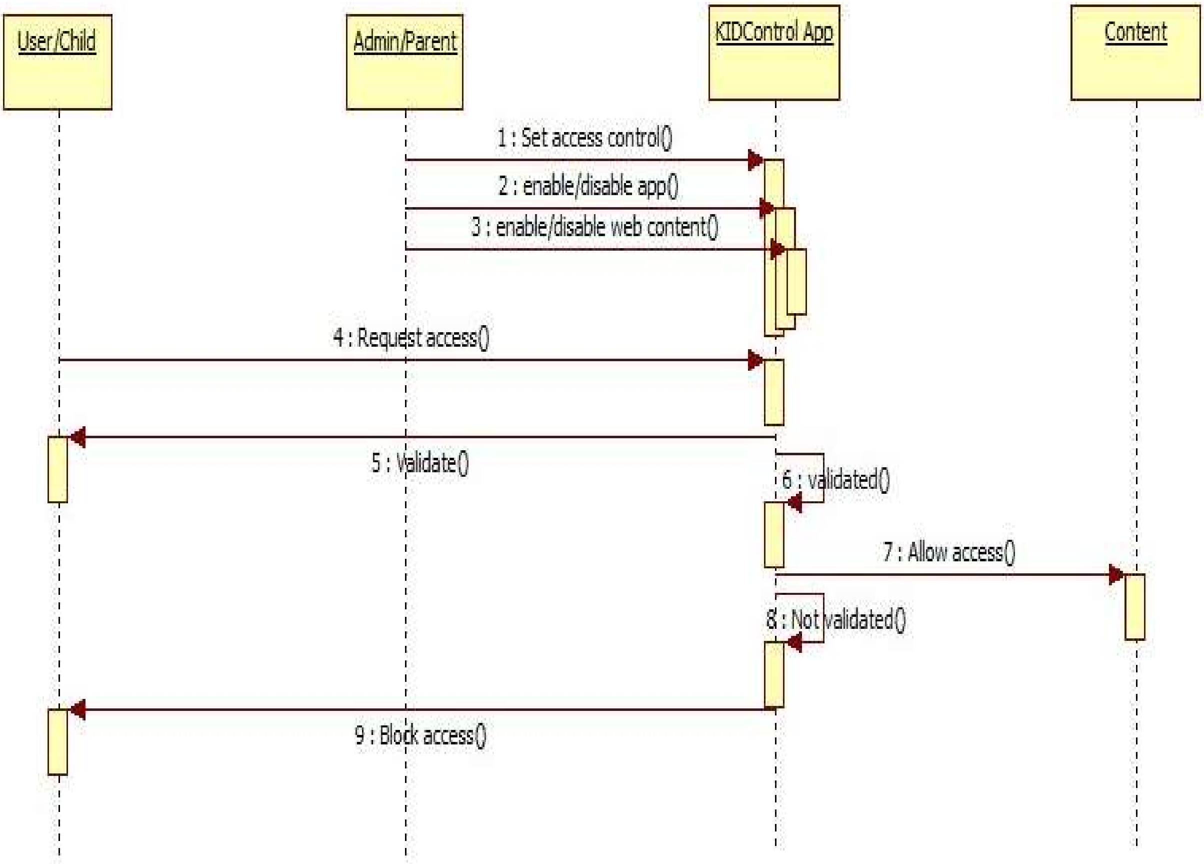


Sequence diagram

The sequence diagram shows the sequence of activities and operations that can be carried out by the children as they access the ICT services and products, as well as the sequence of operations that can be performed by the parent to control children's access.

The child as a primary actor of the application will be able to request the access to the web content and application, which will be able validated and verified by the system, after what a parent/ guardian has set as a control.

Parent/ Admin as a secondary actor who allow the access, able/ disable App as well as web contents which will be used by the system to control children's activities.

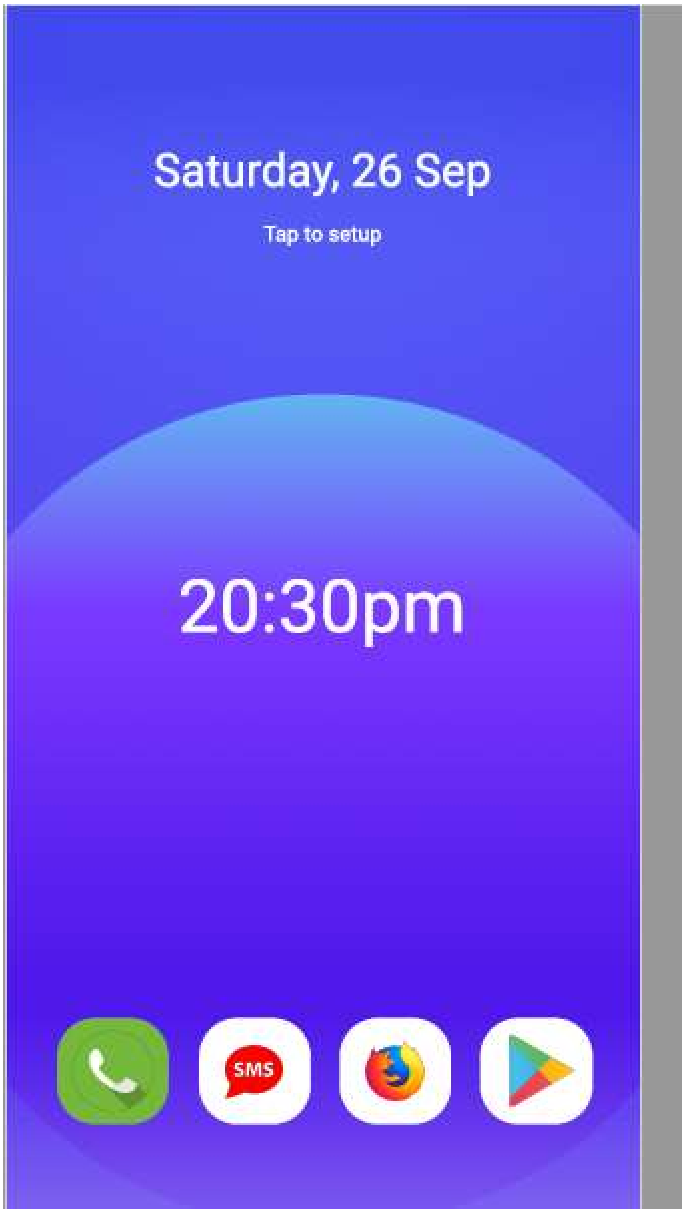


Appendix 3: END USER WORKFLOW PROTOTYPE

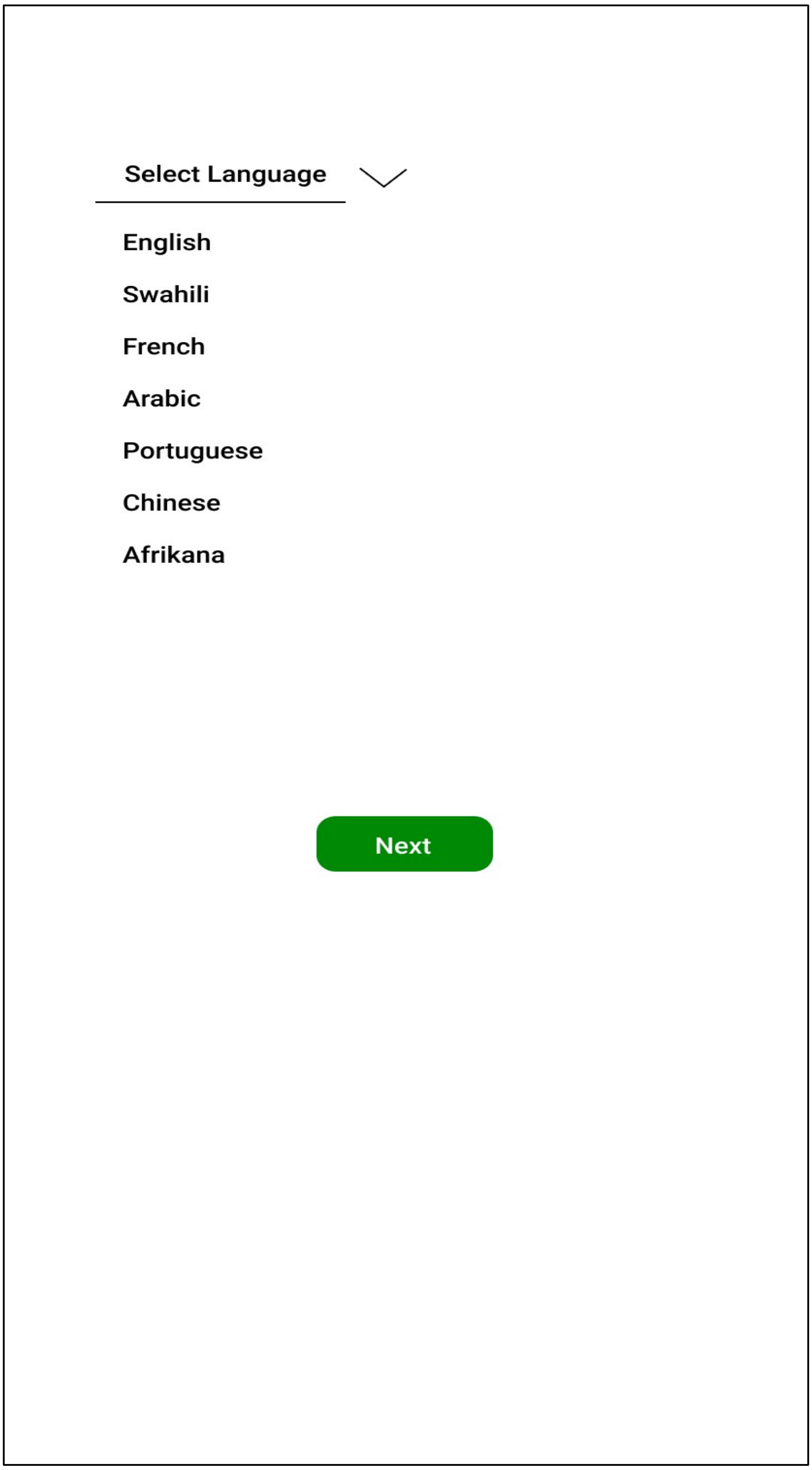
The end user workflow is the representation of the prototype showing how the application will operate in mobile devices.

The prototype below has been created from figma.com software for designing prototypes.

Home page

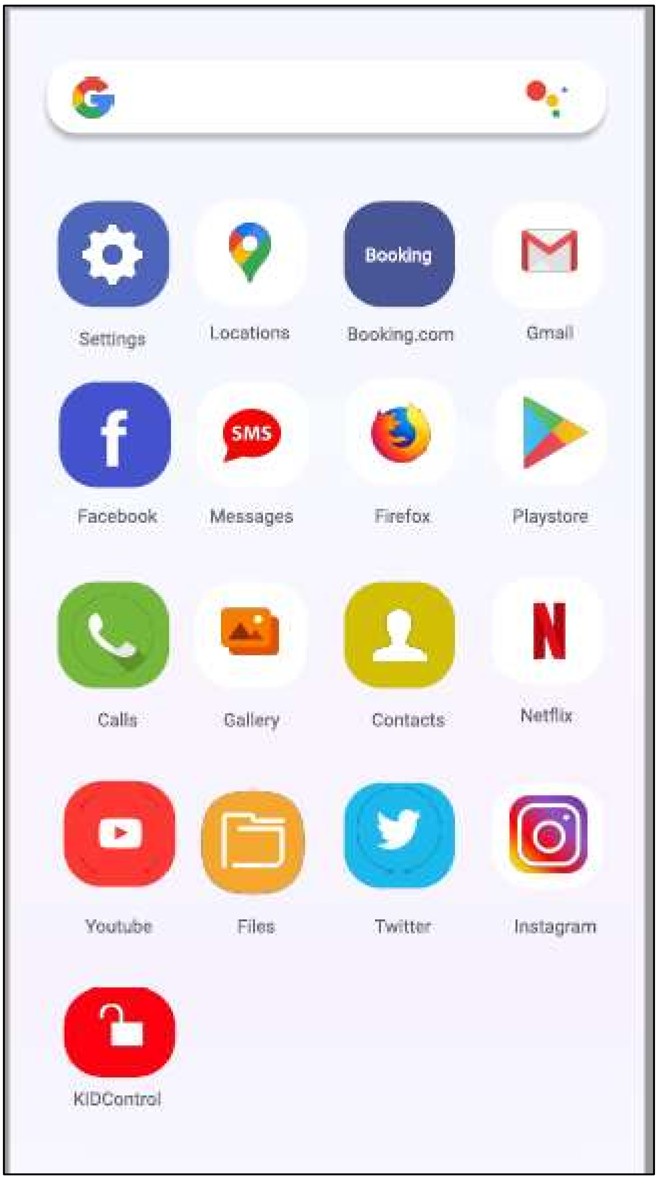


Language navigation page

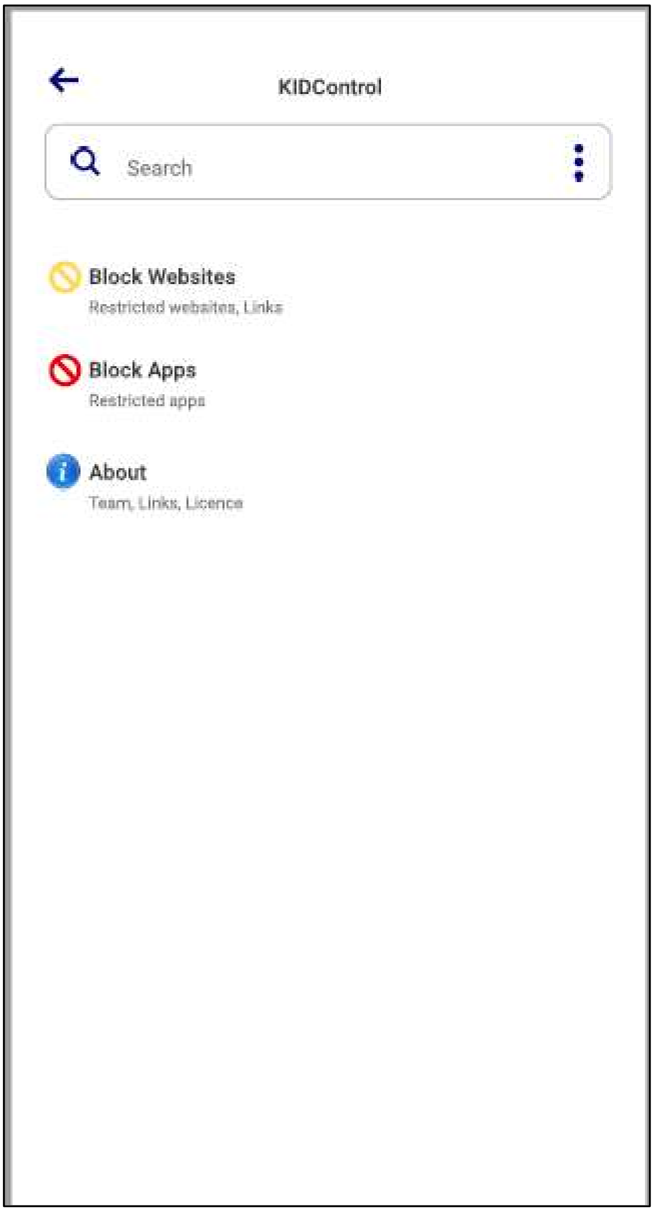


- After the application is created will be ready for the installation to different devices, and below is the illustration of how the KID control app will look.
  The figure showing the layout of the installed apps in the device.

Apps



KID Control setting



KIDControl

Search

Block Websites

Restricted websites, Links

Block Apps

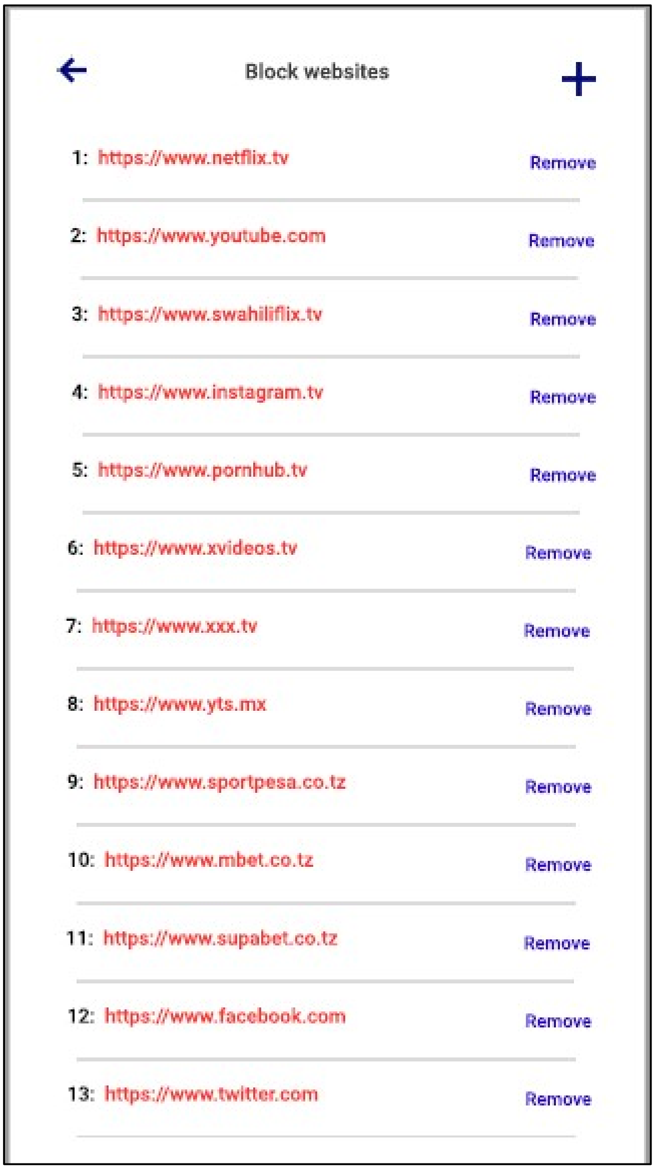
Restricted apps

About

Team, Links, Licence

The layout of the blocked web sites will be as:

Block websites



Block websites

1: https://www.netflix.tv Remove

2: https://www.youtube.com Remove

3: https://www.swahiliflix.tv Remove

4: https://www.instagram.tv Remove

5: https://www.pornhub.tv Remove

6: https://www.xvideos.tv Remove

7: https://www.xxx.tv Remove

8: https://www.yts.mx Remove

9: https://www.sportpesa.co.tz Remove

10: https://www.mbet.co.tz Remove

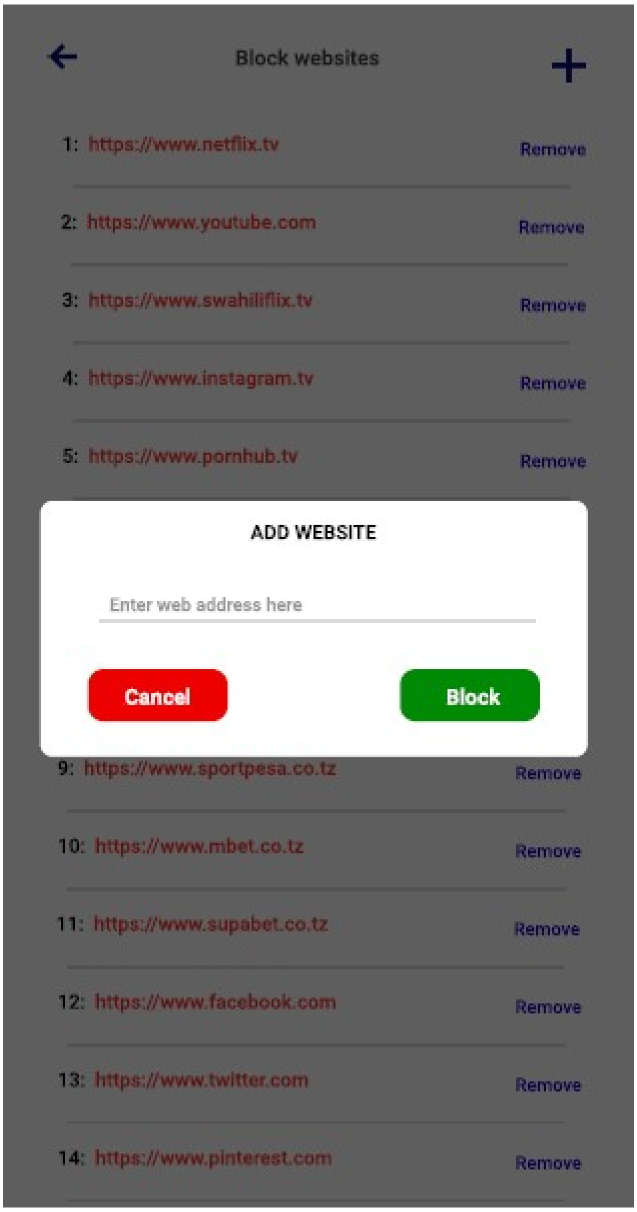
11: https://www.supabet.co.tz Remove

12: https://www.facebook.com Remove

13: https://www.twitter.com Remove

Parents and guardians will be able to block as many websites as they wish according to what they find as unsafe to their children. The below image illustrates how this will be done.

Add Website to block



Block websites

1: https://www.netflix.tv Remove

2: https://www.youtube.com Remove

3: https://www.swahiliflix.tv Remove

4: https://www.instagram.tv Remove

5: https://www.pornhub.tv Remove

ADD WEBSITE

Enter web address here

9: https://www.sportpesa.co.tz Remove

10: https://www.mbet.co.tz Remove

11: https://www.supabet.co.tz Remove

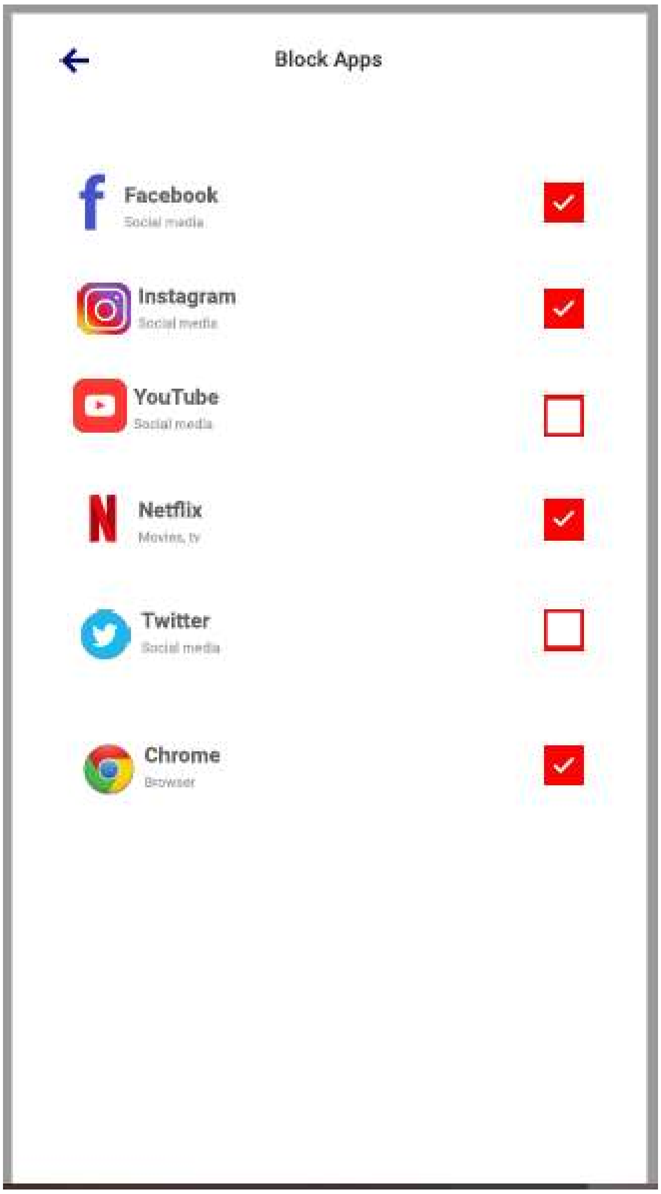
12: https://www.facebook.com Remove

13: https://www.twitter.com Remove

14: https://www.pinterest.com Remove

Also, the application will give parents or guardian the ability to control what applications a child can download and have access to.

Block Apps



Block Apps

Facebook
Social media ☑

Instagram
Social media ☑

YouTube
Social media □

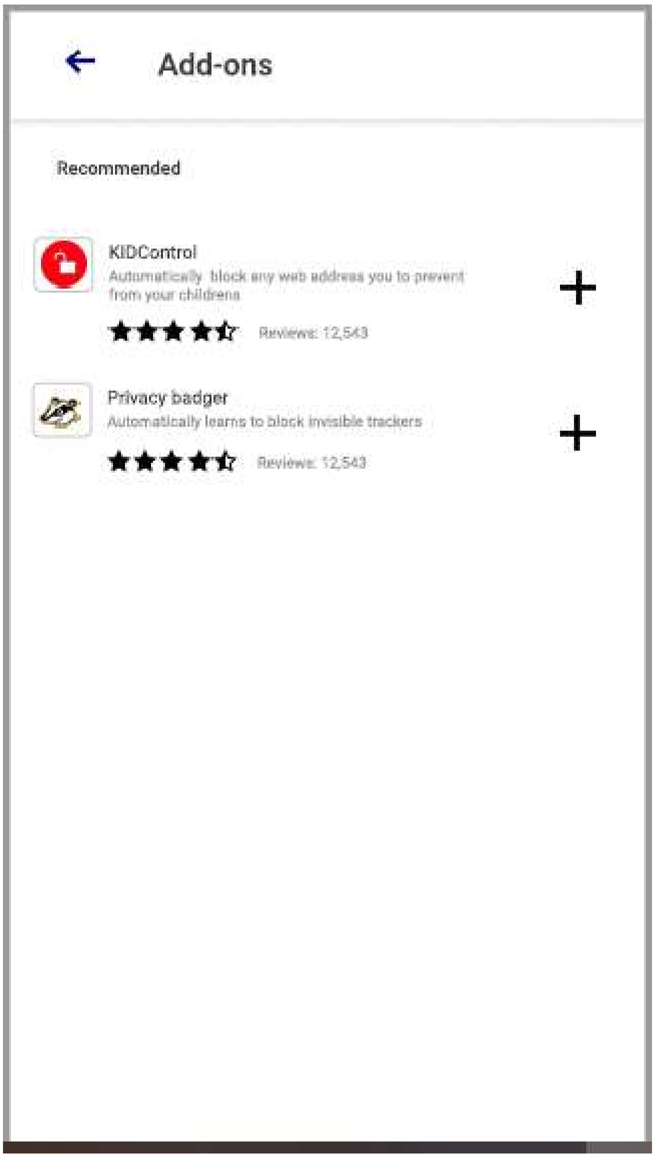
Netflix
Movies, tv ☑

Twitter
Social media □

Chrome
Browser ☑

The proposed application will also be able to block and allow different Ads according to its contents. By so doing the parents/ guardians will be able to prevent their children from downloading Ads with harmful contents.

Firefox Activity



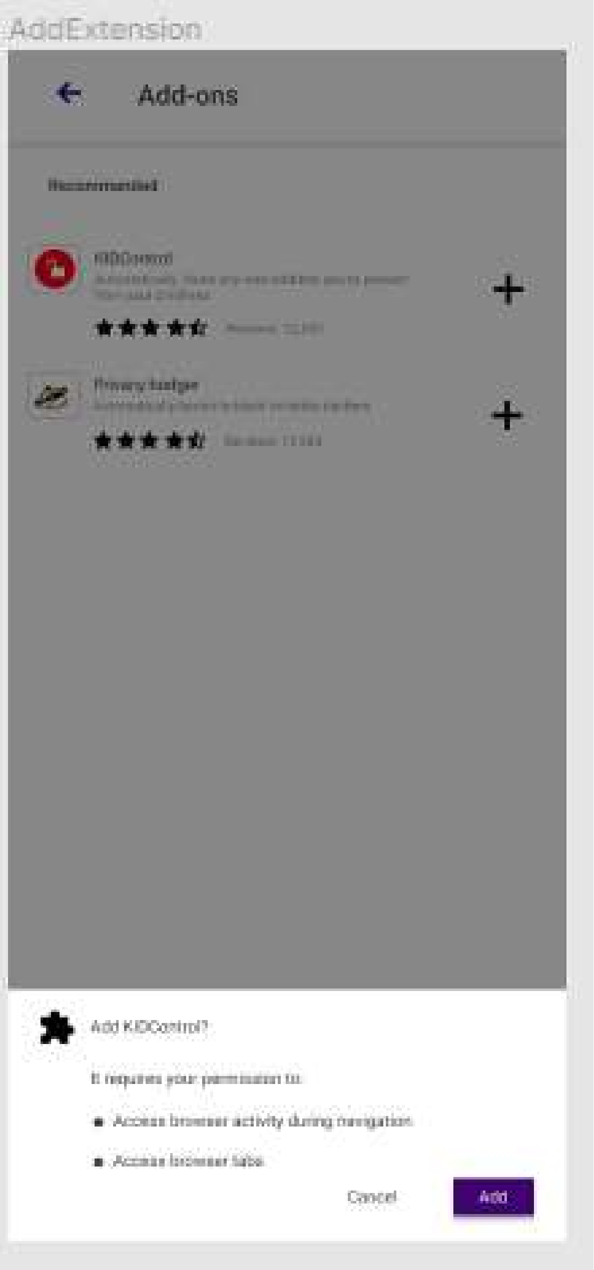
← Add-ons

Recommended

KIDControl
Automatically block any web address you to prevent from your childrens
★★★★☆ Reviews: 12,543
+

Privacy badger
Automatically learns to block invisible trackers
★★★★☆ Reviews: 12,543
+

Add Extension



AddExtension

Add-ons

Recommended

KIDControl

[illegible]

★★★★☆ Reviews: [illegible]

Privacy Badger

[illegible]

★★★★☆ Reviews: [illegible]

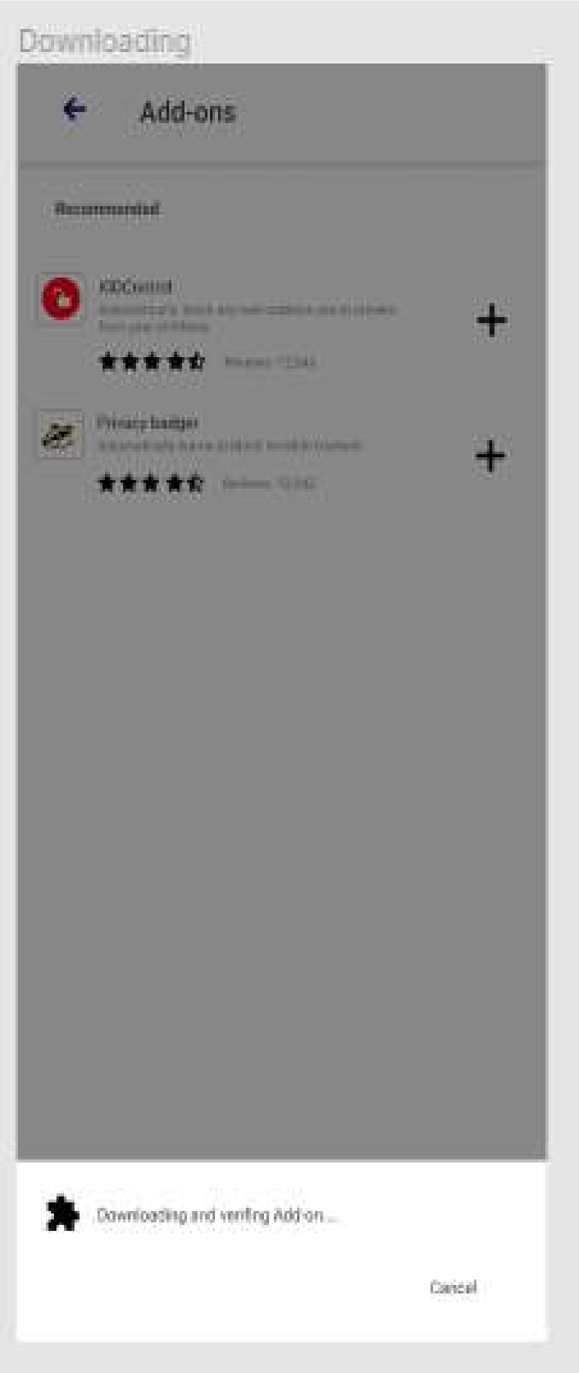
Add KIDControl?

It requires your permission to:

- Access browser activity during navigation
- Access browser tabs

Any Ad that will be downloaded will be verified whether its contents are age appropriate to the children.

Downloading



Downloading

Add-ons

Recommended

KIDControl

[illegible]

★★★★☆ [illegible]

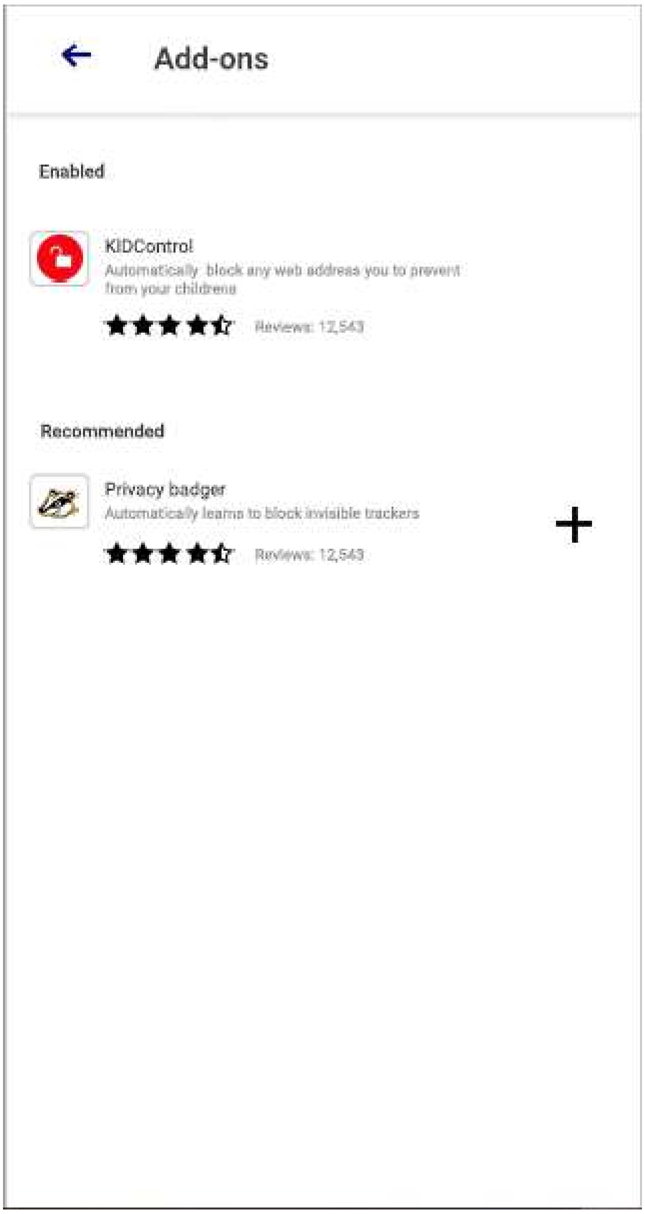
Privacy badger

[illegible]

★★★★☆ [illegible]

Downloading and verifing Add-on...

Extension Added



← Add-ons

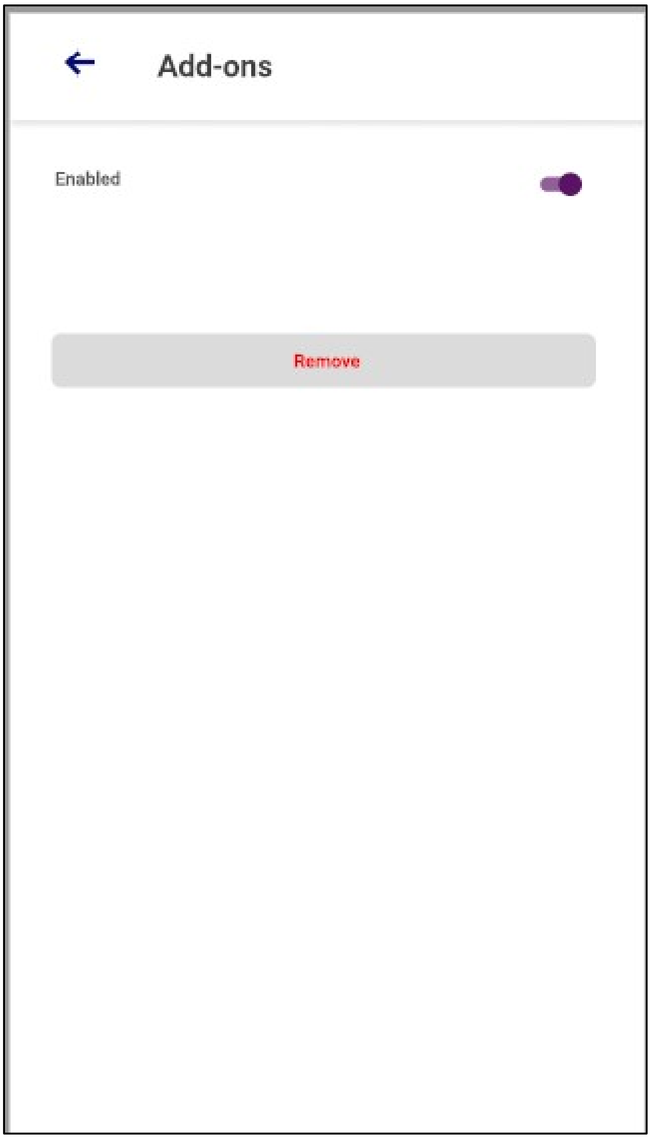
Enabled

KIDControl
Automatically block any web address you to prevent from your childrens
★★★★⯪ Reviews: 12,543

Recommended

Privacy badger
Automatically learns to block invisible trackers
★★★★⯪ Reviews: 12,543

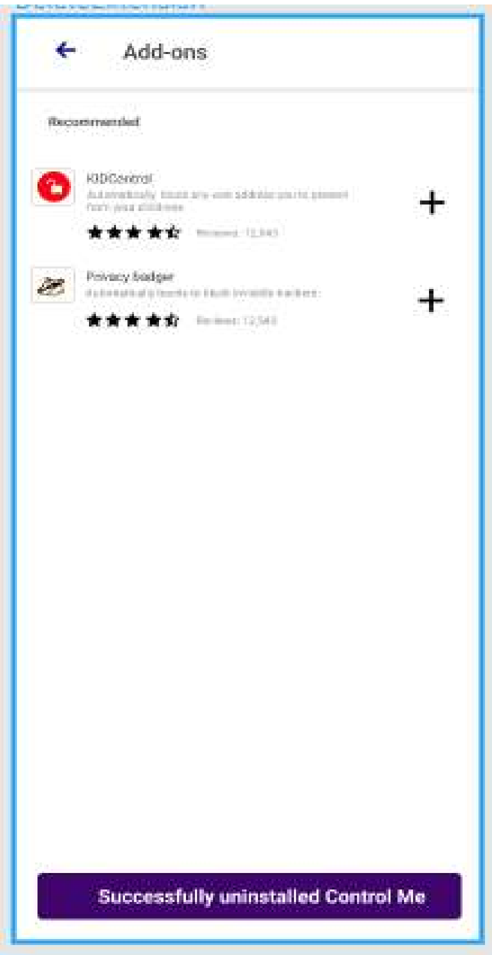
Extension Settings



Enabled ●

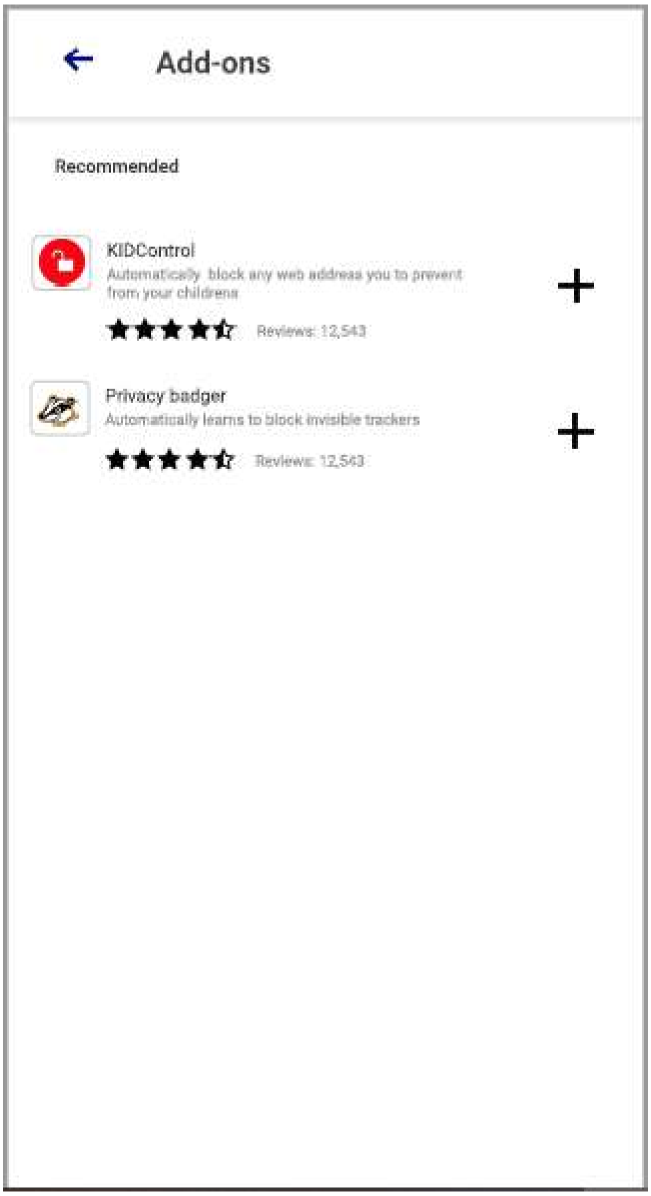
The added extension can be deleted by the parent/ guardian who is the administrator of the application.

Delete Extension



Successfully uninstalled Control Me

Extension deleted



Add-ons

Recommended

KIDControl
Automatically block any web address you to prevent from your childrens
★★★★⯪ Reviews: 12,543

Privacy badger
Automatically learns to block invisible trackers
★★★★⯪ Reviews: 12,543