

PROMOTING CHILDREN'S SAFETY ONLINE IN UGANDA

A study on children's safety online and guide to enhance their safety



ACKNOWLEDGEMENTS

This report was researched, written, and prepared for publication by the team at Encrypt Uganda under the leadership of Andrew Gole. We thank Adur Winnie, Akware Diana, Aguti Brenda Juliet and Abukui Mary who went out to the field to collect and analyze data as research consultants. Anthony Masake provided editorial support.

In a special way, Encrypt Uganda acknowledges the unwavering support and guidance from the Digital Human Rights Lab team that made the research and publication of this report possible. We also thank GIZ Uganda for the generous financial support towards publication of this report and the 'Children's Safety Online Project'.

Finally, Encrypt Uganda expressed its deepest appreciation to the individuals who shared their stories and experiences with us and to the schools for welcoming our researchers to interact with the pupils, students and teachers.

About Encrypt Uganda

Encrypt Uganda is a registered Non-Governmental Organisation (NGO) focused on securing information, data, and strengthening internet freedoms of human rights defenders, activists, and vulnerable populations in Uganda. The organisation offers preventive real-time solutions and seeks to strengthen the safety and security of individuals at risk by building their capacity with a view of equipping them with knowledge and skills to better protect themselves against digital security threats.



www.encryptuganda.net



info@encryptuganda.net

Correspondence and requests for permission to use or translate this publication should be addressed to Encrypt Uganda via email info@encryptuganda.net

Front cover image: ©Encrypt Uganda/Daniel Maina
Design and layout: Daniel Maina/Adamz Creations

©Encrypt Uganda - April 2021



CONTENTS

1. Introduction	3
2. Methodology	5
3. Key findings from the research	6
4. Recommended strategies	10
5. Recommended guidelines to enhance children's safety online	12
5.1. Recommended guidelines to share with children	
5.2. Recommended guidelines for teachers and schools	
5.3. Recommended guidelines for parents / guardians	
5.4. Recommendations for the Government of Uganda	

I. INTRODUCTION

As the Covid-19 pandemic ravaged many parts of the world, Uganda moved to close all primary and secondary schools, and other higher institutions of learning – including universities on March 20, 2020. In a national address, President Yoweri Museveni noted on March 18, 2020 that it was important to temporarily disperse the ‘concentration points to prevent the spread of coronavirus.’ As a result, almost 15 million children in Uganda were affected by school closures due to the pandemic.

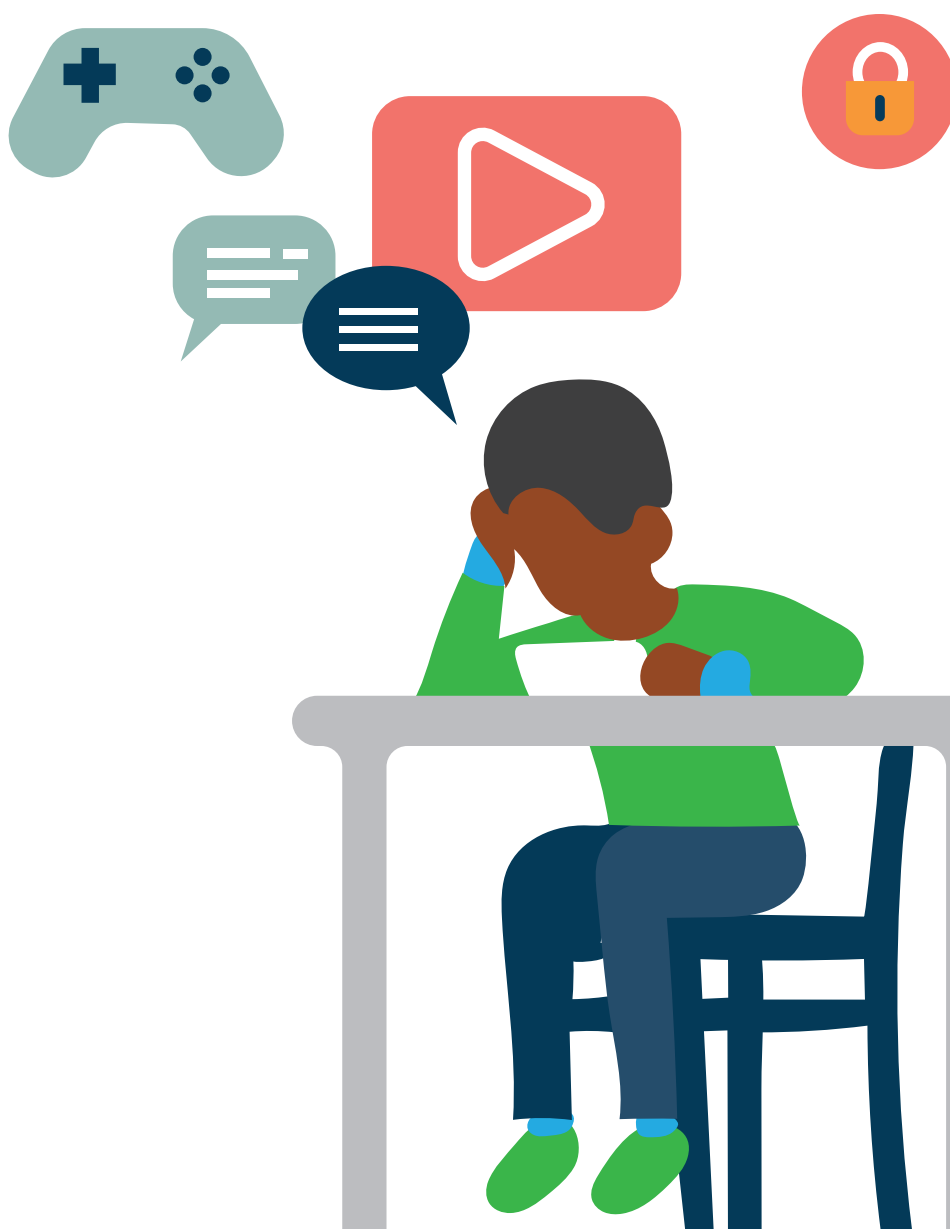
The indefinite closure of schools triggered the urgent need to find alternative ways to keep the pupils and students learning without being together in a physical class or lecture room. Some of the approaches adopted include distribution of home learning kits in hard copies and through emails and social media platforms, conducting lessons and lectures on Zoom and other conferencing applications, and class lessons on radio and television sets. Available literature review indicates that these changes have presented a number of challenges. For example, many pupils, students and schools are without reliable access to computers, smartphones, tablets, and stable electricity and internet access. As a result, there is a significant gap between those from privileged and disadvantaged backgrounds. Indeed, many are concerned that the pandemic will widen the digital divide.

Accordingly, as part of the organization’s ‘Children’s Online Safety Project’, Encrypt Uganda sought to understand the state of children’s safety online in Northern and Eastern Uganda as they navigate the dramatic change to online learning. The assessment will further guide Encrypt Uganda on the implementation of the children’s online safety project in the two regions to ensure that the project addresses the needs of the pupils and students.

With the support of the Digital Human Rights Lab under a funding agreement with the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), Encrypt Uganda conducted in-depth one-on-one interviews, key informant interviews, and focus group discussions to inform the assessment of the prevailing situation to assist in providing recommendations on addressing identified gaps.

The research study aimed to learn experiences of children, parents/guardians, teachers and schools during the rise of e-learning specifically in regard to children’s safety online. The researchers achieved this by examining the preparedness of stakeholders, how they are adapting to the technology, and assessing the various threats and harm faced by children as a result of the online learning.

This study report uses the findings from the research to provide strategic guidance to children, parents/guardians, teachers, schools, and the government of Uganda in promoting children's safety as they increasingly engage in online learning. It identifies the key issues of concern and sets out a recommended strategy for stakeholders aimed at enhancing children's safety online.



II. METHODOLOGY

This report is based on one-on-one interviews, key informant interviews, and focus group discussions. Desk research was also conducted to appraise relevant literature and identify links to helpful resources for the stakeholders for purposes of the recommendations section of this report.

A total of 162 children (46 pupils and 116 students) from 20 schools were interviewed for the one-on-one interviews. 52.4 percent of the respondents in the one-on-one interviews were male while 47.5 percent were female.

40 teachers in the identified schools were further engaged in key informant interviews and their feedback forms the basis for this report. In addition, the findings are further complemented by outcomes of 8 focus group discussions with 40 parents.

All the field data collection activities for this research were conducted in the month of March 2021.

Geographically, the research was conducted in Northern and Eastern regions of Uganda in the 8 districts of Gulu, Soroti, Jinja, Arua, Tororo, Lira, Mbale and Moroto.

The report also draws on available literature on online learning in Uganda and reporting on children's safety online. While almost 15 million Ugandan pupils and students were expected to be engaged in online and remote learning from March 2020, there is a significant gap in the available scientific information about experiences of the dramatic change in which education is being conducted.

All interviews and discussions were conducted in English language. Encrypt Uganda researchers presented introduction letters to all respondents, explained the purpose of the interviews to the interviewees and purpose of the discussions to the participants, and obtained their consent to use the information they provided in this report while observing privacy and confidentiality protections.

The 40 parents who participated in the 8 Focus Group Discussions (FGDs) were recruited into the survey through a head-hunting process with the help of local government leaders given the fact that they know the parents in their localities. The findings of the FGDs were obtained through discussing various research questions while note taking.

III. KEY FINDINGS FROM THE RESEARCH

1. **30 percent of the 162 children interviewed for this research reported suffering abuse and threats online.** The top online threats the children reported facing are as follows:



- a. **Exposure to inappropriate content:** Many children who suffered abuse online reported being sent nude pictures, pornographic and obscene messages with vulgar language.



- b. **Online predators:** Children also reported receiving Facebook friend requests from strangers (adults) who later started sending them nude photos, intimidating messages, and threatening phone calls with an intention of enticing them for sexual and other forms of abusive exploitation. Some of the friend requests were of accounts that appeared to be of the same gender with the child, especially female, only for it to be clear later that the account belongs to the opposite gender.



- c. **Cyberbullying:** The children who reported suffering from cyberbullying recounted receiving abusive comments on their photographs on Facebook and receiving threatening messages and calls for liking and commenting on photos on some Facebook. A boy reported being scolded by his peers for sharing a picture where he was standing with a girl.

2. **There is a high illiteracy level on children's safety online among the children, teachers and parents/guardians.** Whereas 100 children (62 percent) say they know something about children's safety online and only 62 children (38 percent) interviewed for this research say they do not know anything about children's online safety, most of them fail to identify the core aspects of children's safety online as elaborated in the notes in the appendices.



3. **The majority 115 children (71 percent) believe online studies are helpful in bridging the gap.** However, 47 children (29 percent) interviewed for this research do not believe that online studies can be a better approach to bridge the learning gap.



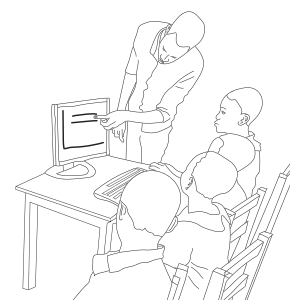
4. **Many children did not receive tips on how to use the internet safely.** While 88 children (54 percent) interviewed for this research note that teachers or parents provided them with some safety and security measures on using the internet during online studies, a significant percentage of 46 percent (74 children) said they were not guided or advised on how to safely use the internet when they started using the internet during the online studies. These findings were almost similar when asked whether they received any 'capacity building' on attending online studies from either their parents or teachers. 83 children (52 percent) said yes while 79 (49 percent) said no.



5. **The majority of the children note that their parents were supportive towards online studies.** 122 children (75 percent) felt their parents provided the necessary support that was within their means while 40 children (25 percent) felt they did not receive the support they expected from their parents in their quest to attend studies online.



6. **The majority of the children interviewed for this research (123 representing 76 percent) noted that they have never participated or heard of any awareness campaign on children's safety online.** Only 39 children (24 percent) have heard or participated in some form of awareness sessions on how to safely use the internet during online studies.



7. **Children do not feel safe online while attending to online studies.** During the research, 88 children (54 percent) observed that they do not think their safety is guaranteed online while 74 children (46 percent) said they generally feel safe. Out of the 40 teachers interviewed for this research, 31 noted that they do not think children's safety online is guaranteed during online studies. The research further indicates that the majority of children are in favour of controls and restrictions for their safety online.



8. **Despite the challenges and gaps identified above, the majority of the children interviewed (73 children representing 45 percent) recommend continuous teaching online studies given the circumstances.** 26 children 'strongly recommend' the online studies while 11 children noted that they were 'not sure' whether online studies should continue. Despite the generally positive feedback, it is concerning that a significant number of the respondents (52 children representing 32 percent) 'don't recommend' online studies.



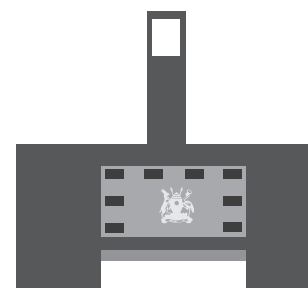
9. **Despite the high vulnerability levels, few children suffered online abuse while attending online classes.** 113 children (70 percent) noted that they did not suffer any form of online threats or abuse while 49 children (30 percent) reported suffering from various forms of threats and abuse online. When teachers were asked about cases of online abuse reported by the children, the number was lower. Only 7 teachers (17 percent) are aware of reports of abuse online while 33 teachers (82 percent) are not aware of any reports of abuse online suffered by pupils/students. Most teachers (27 out of 40) do not know the referral pathways in case of cybercrimes.



10. **A significant number of schools do not have any rules in place on children's safety online.** Whereas 88 children (54 percent) confirmed that their schools have some form of rules to guide and protect them online, 75 children (46 percent) observed that they were not aware of any of such rules. Out of the 40 teachers interviewed for this research, 18 noted that there were no 'precautionary measures' put in place to protect children from online threats and abuse during online studies.



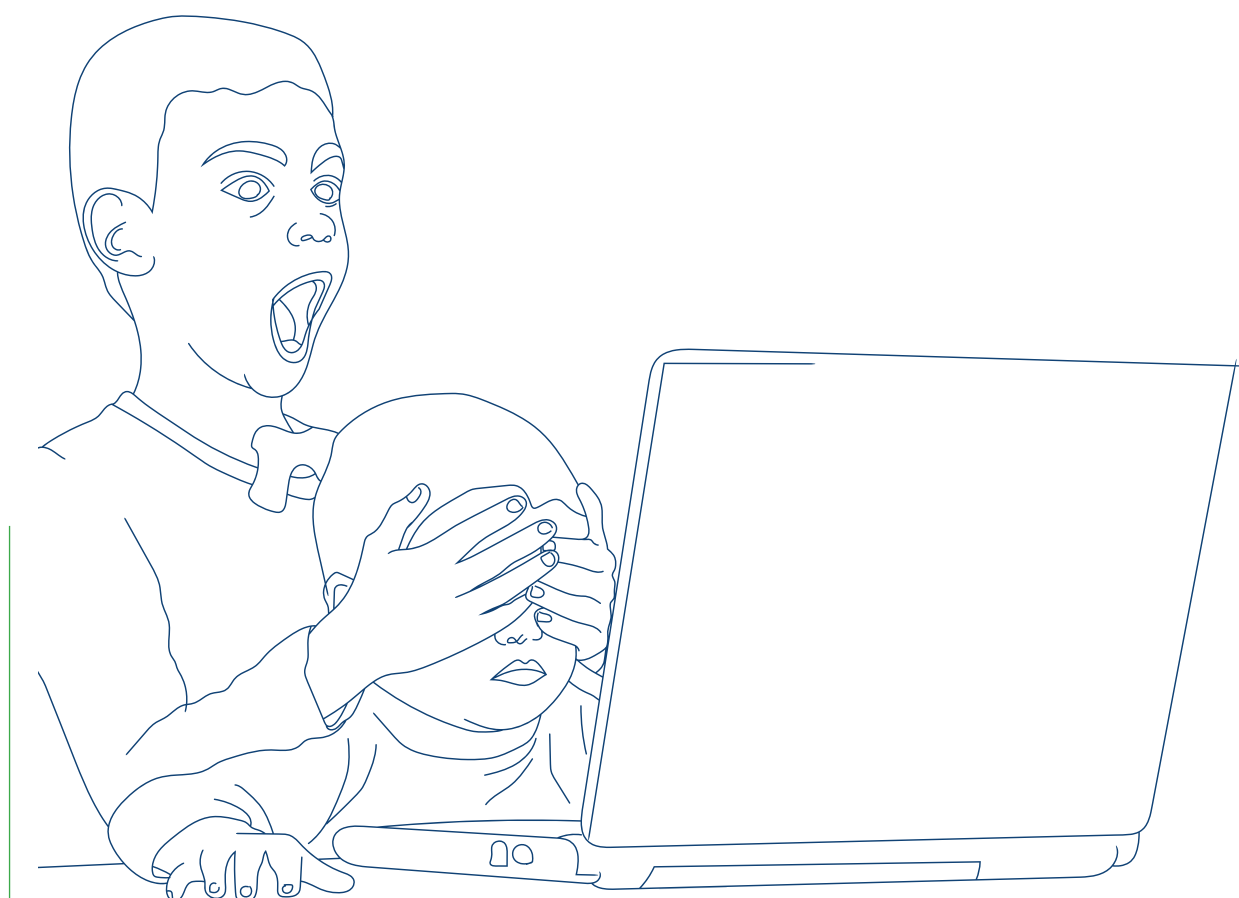
11. **The government has not put in place necessary measures to protect children during online studies.** Out of 40 teachers interviewed for this research, 36 noted that the government has not taken necessary steps to protect children online. 'There is no measure or effort that I can think of,' noted one of the respondents.



12. **Several schools are moving to integrate cyber security module in their curriculums.** Out of the 40 teachers interviewed for this research, 25 noted that there are plans in their schools to introduce cyber security classes to educate the pupils and students on how to secure their activities online and protect themselves from attacks. 'We have plans but don't have the means. We need to have enough computers and internet,' noted a respondent during key informant interviews.



13. **Most of the schools did not conduct refresher trainings for teachers on safety of children online even as they looked to scale up education activities on the digital platforms.** Out of 40 teachers interviewed, only 9 confirmed that their schools conducted refresher trainings for teachers to prepare them to safely interact with the pupils/students and guide them accordingly. 31 teachers noted that they were never trained. 'Only computer teachers are called for trainings organized by the government at the National Curriculum Development Center annually,' noted a respondent.



IV. RECOMMENDED STRATEGIES

The research findings indicate that children, teachers, schools, parents/guardians, and the government are engaged in a number of activities that are not strategic and adequate in terms of ensuring the enhancement of children's safety online. For instance, whereas some computer teachers are trained by the government on online learning, most of the sessions are focused on how to use the computer and other tools of digital learning and little or no focus is placed on how to ensure children's safety online. Digital security awareness is also shallow and does not address crucial needs. In this section of the research, Encrypt Uganda proposes five strategies that are designed to guide stakeholders to ensuring safety of children online.

1. **Invest in digital equipment for all children:** Research shows that children who have regular and easy access to digital tools and platforms are bound to be more tech-savvy and therefore more likely to navigate online spaces safely. In addition to bridging the digital divide between privileged and disadvantaged children, the investment will also provide equipment for hands-on digital security sessions.
2. **Ensure all devices are set up safely:** It is recommended that all devices of children are set up using the child's accounts. For example, sign up a Google account/Email for your child and use it to set the device up. Be sure to use the age of the child to give Google a better chance to identify age-appropriate apps and content for your child.
3. **Use parental control software, privacy settings:** It is recommended that all parents and guardians who have purchased for their children broadband access, smart-phones and tablets download and install parental control software. During the research it was observed that few parents/guardians are aware about the various applications that can help them to monitor and control how their children utilize the internet. The recommended guidelines in this report provide a detail of the benefits of this software. Parents and guardians should also update privacy settings.
4. **Talk about staying safe:** It is recommended that more efforts are taken by parents/guardians and teachers to talk to children about e-safety issues in an interactive way. It is encouraged that you educate yourself as a teacher, parent or guardian about the latest e-safety tips so that you are able to respond to the issues raised by children appropriately. Keep the communication lines open so that the children can inform you if anything online makes them uncomfortable.
5. **Increase awareness of teachers and children on the important tips for children's safety online** through awareness campaigns, encouragement to read and keep up to date with the latest safety tips, and trainings.

This study report uses the findings from the research to provide strategic guidance to children, parents/guardians, teachers, schools, and the government of Uganda in promoting children's safety as they increasingly engage in online learning. It identifies the key issues of concern and sets out a recommended strategy for stakeholders aimed at enhancing children's safety online.



V. RECOMMENDED GUIDELINES TO ENHANCE CHILDREN'S SAFETY ONLINE

4.1. Recommended guidelines to share with children

- a) Encourage children to pay attention and follow online safety guidelines issued by your parents, older siblings, teachers and schools. Help the children to understand that the controls and restrictions are for their good by showing the pitfalls of not regulating their activities online.
- b) Encourage children not to reveal personal information such as phone number and home address during their activities online. Inform the children that such information can be used by strangers to target and harm them.
- c) Do not write your passwords down or share them with anyone. If you do, another person can use it to access your accounts and do harmful things in your name. Children are further encouraged to use strong passwords and change them every after six months.
- d) Encourage children never to agree to meet a stranger they met online without the approval and possible supervision of a parent/guardian or any other trusted adult. It does not matter how friendly the child thinks the person is.
- e) Always tell a parent/guardian, teacher or other trusted adult about any threatening messages or bullying for appropriate advice and/or action. If you feel a conversation was scary, strange or hurtful, please report too. It is important to seek help before a situation worsens.
- f) Children are encouraged to learn more about privacy settings on the various apps to know how to block accounts that make them uncomfortable and take other protective measures.
- g) Encourage children to search safely by using safe search engines such as Kids-Search Engine and Swiggle . These safe search settings can also be activated on Google and YouTube.

4.2. Recommended guidelines for teachers and schools

- a) Create and enforce rules safeguarding pupils and student's safety online. Talk to the children to help them understand that the rules are for their own good to minimize resistance and attempts to bypass the controls.
- b) Build the capacity of all teachers on online learning and stay up-to-date with latest technology to
- c) Raise awareness about user privacy online for pupils and students. Teach them about digital footprints and how information is stored online and why they need to stop authorized persons from gaining access to their information.
- d) Use SafeShare.tv to safely share YouTube and Vimeo videos without adverts, links to other potentially inappropriate content, and other distractions. To create a 'SafeView' link, you simply copy and paste the URL of a YouTube or Vimeo video on the site. This website further enables a teacher to enable privacy controls, share video directly to Google Classroom, and allows a teacher to trim videos to show only the part you care about.
- e) Create safe spaces by setting up a support system in the school against cyberbullying. The group should encourage pupils and students to speak up and report bullying online to receive support and accountability.
- f) Accounts for pupils and students to study online should not require names, photos, and other personally identifiable information (PII) during log-in sessions. It is advisable that the children only be required to log-in using a unique registration number to protect their identity in case of a safety breach.

4.3. Recommended guidelines for parents/guardians

- a) Take an active role in your child's internet activities and keep abreast of what you need to know about the social media apps. This will make it possible for you to teach children the appropriate online behaviour for their safety.
- b) While setting up your child on a smartphone or tablet, ensure that you use their Google Account/Email address which was set up using their actual age. If the child does not have a Google Account, sign up one for them. Never sign in using your account because that will grant them general access to adult content.
- c) Put yourself in control. Install 'Google Family Link for Parents' mobile app or other parental control apps on your phone and pair it with the devices used by your children. The app, which is free, will enable you to:
 - See the location of your child's device.
 - Receive email notifications of all apps installed on the child's device and remotely exercise powers to block an app that you consider inappropriate.
 - Monitor activity and time spent on each app on the child's device on daily, weekly and monthly rates.
 - Set limits on access to the apps.
 - Set daily limits or bedtime hours for the child's device.
 - Review privacy practices.
 - Activate filters on Google Chrome and Google Search Engine by turning on 'SafeSearch' button to help filter sexually explicit and violent results.
 - Activate controls on Google Play.
 - Control settings on YouTube. It is advisable to activate only 'YouTube Kids' for young children and if your child is a pre-teen and older, you can allow 'YouTube (Parent supervised)'
 - Control Google photo sharing on the child's device.

Set up parental controls for your child's Apple devices (iPhone, iPad or iPod touch) , for Google Play , for YouTube Kids , for Facebook , for Twitter , and for Netflix .

- d) Videos that are not age appropriate can still make their way into your child's feed on YouTube Kids app even if you have turned on the 'Safety Mode' on YouTube. If you have a YouTube video which you want a child to watch online, copy the URL and paste it on SafeShare.tv to create a 'SafeView' link to increase safety of the children.
- e) Keep the communication line open and make sure the child feels comfortable to turn to you when they have any challenges online. When he or she reports to you about an uncomfortable experience online, take them seriously and make sure to check it out and take necessary appropriate action. In all situations, it is recommended to pay attention and follow the following four steps: -
 - Remain calm and find out more about the issue;
 - Talk to your child in a calm and open conversation;
 - Take action by discussing with someone you trust and knows more about the subject, and finally;
 - Seek support for yourself, if necessary, from a friend or relative who understands the situation.
- f) Watch out for the following warning signs of a child being targeted online and take steps to talk to find out:
 - Unusual withdrawal from family life.
 - A child suddenly turns off the computer or phone when you walk into the room or go near them.
 - When a child spends long hours online.

4.4. Recommendations for the Government of Uganda

- a) The Parliament of Uganda should enact a law on children's online safety/protection to help provide a legal framework for the protection of children when they are online and create offences for the abuse of children's privacy and safety online.
- b) Develop a national protection strategy for children's safety online for Uganda. This strategy should recognize all actors and stakeholders, assess the existing responses and pathways, analyse the state of safety of children online in the whole country, make a case for the cost-benefit analysis for the protection of children online, and provide a national framework for implementation of the identified recommendations in line with the broader government strategic plans.

- c) Take action to ensure that Internet safety for children is included in the curriculum for all primary and secondary schools. Safety of children online should not only be a subject of ICT.
- d) Train all teachers (not only ICT teachers) on Internet safety for children because they are all now involved in online studies one way or another.
- e) Ensure that the law enforcement agencies are trained to investigate cases of abuse of children online, the prosecutors are trained to successfully prosecute the cases, and judicial officers are sensitized on the delivery of justice in such cases without causing more harm.

