



UNDERSTANDING AFRICAN CHILDREN'S USE OF

INFORMATION AND COMMUNICATION TECHNOLOGIES (ICTs)

a youth-led survey to prevent sexual exploitation online

















This report was written and edited by Anjan Bose and Renata Coccaro. Proof reading support by Laura Healy. Legal section was written and edited by Francois-Xavier Souchet with support from Jessica Klinke. Special thanks to Melanie Gnandi and Jonathan Ssembajwe for coordination in the region throughout the process and also inputs on youth friendly approach.

Support and advice from Junita Upadhyay, Erwin Mom and Mark Capaldi was an invaluable resource throughout the planning and publication process.

Acknowledgement of EU Kids Online Project that inspired much of the questionnaire design.

Designed by Manida Naebklang

January 2013

Copyright © 2013, ECPAT International

ECPAT International wishes to thank SIDA, Oak Foundation, European Commission, The Body Shop, Irish Aid and Ladies Circle International for the financial support to implement this youth-led study.

We also would like to express our appreciation to participating ECPAT member organizations and partner agencies that mobilized the youth in conducting this research such as; WAO Afrique -Togo, CPA (Child Protection Alliance) -The Gambia , ASSEJA (Association, Enfants, Jeunes et Avenir)- Cameroon, ECPAT Uganda and End Child Prostitution in Kenya (ECPIK).

The views expressed herein are solely those of the authors. The support received from the above-mentioned donors does not constitute endorsement of the opinions expressed.



ECPAT International

328/1 Phayathai Road Ratchathewi Bangkok 10400 THAILAND Tel: +662 215 3388, +662 611 0972 Fax: +662 215 8272 Email: info@ecpat.net Website: www.ecpat.net

TABLE OF CONTENTS

1.	Executive summary	3
2.	Introduction	6
3.	The sharp penetration of technology in Africa: major implications for child protection	7
4.	Cybercafés: a unique feature of the digital landscape in Africa	9
5.	Engaging schools in child protection online	10
6.	Approach and methodology	11
7.	Key research findings	13
	7.1 Children's behaviour and vulnerabilities online	13
	7.2 Access from cybercafés	22
	7.3 Family settings and parental guidance	31
	7.4 School setting and guidance from teachers	34
8.	Recommendations for action	43
9.	Legal framework	45
	9.1 National legal frameworks	46
	9.2 Regulations for private sector stakeholders	52
	9.3 The legal position of the child victim of sexual exploitation	54
	9.4 Legal recommendations	55
Ar	nnexes	56
	Children's questionnaire	56
	Cybercafés' questionnaire	67
	Teachers' questionnaire	73

ACKNOWLEDGEMENTS

First and foremost, ECPAT International would like to thank the young researchers who showed tremendous commitment and enthusiasm while conducting the interviews in their respective countries. We also thank the adults who trained them and coordinated the research process. In particular, the local knowledge and support from the Coordinators of the Youth Partnership Project against Commercial Sexual Exploitation of Children — YPP and the following ECPAT members in Africa was essential to the success of this project: ASSEJA in Cameroon; CPA in The Gambia; ECPIK in Kenya; WAO-Afrique in Togo; and Rights of Young Foundation in Uganda. The names of all these contributors are listed below.

Moreover, we are grateful to the 1.073 teenagers, teachers and Internet café representatives who took time to fill in the questionnaires, as well as to the school principals and teachers who allowed us to implement the questionnaires in their institutions and to interview their students. Several representatives of local government and public institutions also played an important role by facilitating access to schools and Internet cafés.

Finally, we would like to express our appreciation for the funding received from our partners and donors, who trusted us in carrying out this project.

ECPAT International is confident that the dissemination of this research study will be invaluable to raise awareness of the need to prevent the sexual exploitation of children through Information and Communications Technologies (ICTs) in Africa, while contributing to the design of policies and programmes to make the Internet a safe place for African children, especially in the five participating countries.

Cameroon Team

Young researchers: Pascal Tang, Pascal Ondao, Paulette Monga, Brice Afia, Carine Ndzina, Julienne Ngah Ndongo, Rachina Moussa, Tatiana Zock, Christian Kila and Mohamed Toukourou.

Adult support: Solange Tsala Nga (Coodinator)

The Gambia Team

Young researchers: Amie Jobe, Yasin Nyan, Almami

Barrow and Abdoulie Badjie.

Adult support: Junkung Jobarteh (Coordinator)

Kenya Team

Young researchers: David Oketch, Aggrey Otieno,

Sarah Owendi and Phillip Peris.

Adult support: Diana Mwai (Coordinator)

Togo Team

Young researchers: Baham Emefa Agalatossi, Afito

Carole Ahontor and Essenam Fumey.

Adult support: Mélanie K. Gnandi (Coordinator) and

Vaida Abra Dotse (Coordinator)

Uganda Team (Areas covered: Kampala, Wakiso, Luweero, Masaka, Mbarara, Jinja and Gulu)

Young researchers: Jonathan Ssembajwe, Wilson Nsereko, May Ruth Nankya, Joseph Isiko, Catherine Tibenkana, Viola Nakiggwe, Brian Kityo, Scalet Kyomuhangi, Majorine Nanteza, Jesca Nalwoga Adult support: Nakkazi Naomi, Aaron Waguma, Yawe Godfery, Paul Tumusiime

ECPAT International Secretariat

Research coordination: Anjan Bose and

Junita Upadhyay

Report written by: Anjan Bose and Renata Coccaro

Design and layout: Manida Naebklang

1. EXECUTIVE SUMMARY

Children in Africa are increasingly using the Internet and ICT tools at home, schools and public spaces, but receive poor guidance to ensure their safety online. The understanding of parents, teachers and cybercafé operators regarding the risks and harms that can be caused, particularly in relation to sexual exploitation, is rather basic and insufficient to effectively protect children. While countries such as Kenya have invested heavenly in ICT implementation, child protection measures have not scaled up accordingly.

Engagement in risky behaviours

- Online practices that have the potential to cause harm do not seem to be quite widespread among the interviewed children, but some figures do raise concern and demand proper prevention strategies.
- A large number of children (49%) have accessed adult pornography online. This is highest in Kenya (55%) followed by Uganda (49%) and about 30% in the other countries. In most of the countries surveyed, it goes up with age and is more prominent among boys than girls. However, the 11-13 year olds in Uganda (both boys and girls) show a high percentage of such viewing. Moreover, all the girls from the 17-18 age group in Cameroon said yes to having viewed such content. Many shared such experience with their friends, especially the males of the higher age groups.
- It is quite disturbing that a very large number (54%) have seen someone of their age represented in pornographic materials in particular 80% of the 11-13 year old boys and 75% of the 14-16 year boys.
- About 10% have been approached by online contacts asking them to share sexualised images of themselves.
- A very low percentage of children (3%) said that they actually shared such images with someone, however mostly were among the younger ages categories (11-13 year-old boys from Kenya and the girls from Uganda of the same age group). No children from Cameroon and The Gambia said that they had done it.
- 21% use webcams with their friends. Fortunately the use of webcams with people they do not know is much lower (6%), with the highest percentage in Togo (8%). The younger age groups (11-13 and 14-16) engaged in this behaviour more frequently.
- While using the social networks and other online platforms, 22% of the children surveyed post personal information online, including home, school address and their mobile phone numbers. In general this trend is stronger among higher age brackets (17-18).
- There is a trend among children to acquire friends online. About 14% of the total sample have met someone offline whom they had first met online (with a high percentage of 33% among 17-18 year-old boys in Cameroon). This was more common among boys.
- A significant number of the interviewed children (47%) already use smart phones instead of the simpler versions. The understanding from parents regarding potentially harmful uses of mobile phones e.g. exchanging sexualised images of oneself or receiving money for this is extremely poor (and, on average, only 50% of them set some rule regarding the use of mobile phones by their children except for The Gambia).
- Almost 45% read guidelines on safety posted online, but a still large number (32%) do not and 14% showed
 ignorance of such materials. Such awareness materials need to be much more attractive and meaningful to the
 child segment.

- Children do want to enjoy safe online experiences and would welcome most of the key measures that can be
 implemented by cybercafés in order to guarantee their protection. In fact, most children in all countries except
 Uganda mentioned safety as the main aspect that needs to be enhanced by ICT companies. The majority also
 mentioned the provision of a clean Internet service, with no access to age inappropriate content such as adult
 pornography and other content deemed illegal to access in the county, as the main measure that cybercafés
 should adopt for their safety.
- There is indication that children and young people in Africa are undertaking online activities (either at home, school or public spaces) that have inherent risks, but most have not yet experienced significant harm.

Impact of their online ventures

- A total of 15% of the children surveyed said that they were hurt when they received sexual images or videos from online contacts. This phenomenon was least observed in Togo. Generally, girls were more affected than boys. In almost all cases (except for Cameroon girls) younger children within the age group 11-13 were more affected than their older counterparts when receiving such images/videos.
- Other uncomfortable situations included: being asked to pose in a compromising state in front of a webcam (10%), being asked to accept indecent materials sent to them (7%), being forced to add certain people to their friends list (14%) and seeing bad things said about them online (9%).
- Among the incidences causing discomfort to children, the highest percentage occurred through emails (23%) followed by those in social network platforms (22%) and messenger programs (17%), and considerably less in chat rooms. This suggests a lower relevance of chat rooms in the context of Africa, compared to other regions such as Asia, and that they may pose less threats to children compared to other emerging interactive platforms.
- Among the children who experienced uncomfortable encounters online, 37% said that they were very upset by the incident, while 40% were just about upset and 22% were not upset at all. The 11-13 boys from Kenya were the most distressed among all surveyed groups.
- Overall, the surveyed children were able to cope up with uncomfortable situations arising from online interactions.
- A large percentage of the children surveyed (62%) did talk to someone when they were upset or felt uncomfortable, an overwhelming 44% of them choosing their friends for that, followed by their siblings (19%) and parents (18%).
 They hardly chose to approach their teachers for guidance and support (only 11%). A very low percentage (3%) went to the police for help, which nevertheless indicates the seriousness of the incident.
- Children are engaging in behaviour that they think is 'fun' but which might cause stress and discomfort to their friends or others, such as posting images without their consent, saying things about others that are untrue, or sending links and pornographic material to make them uncomfortable. While the primary reason for doing such things is 'fun', they also mentioned that they did not think this could cause harm to people because it was just done through the Internet, and that they see others doing it all the time so it should be ok. Children also said they did such things because somebody had done the same to them at some point.

Cybercafés policies

- Cybercafés are, by far, the location where children most access the Internet. About 40% of the cybercafés owners and managers consider themselves knowledgeable about the risks posed to children when going online, which may indicate a lack of preparedness to make these environments safe for children.
- Children reported having seen pornography at the cybercafé at late hours, particularly in Kenya (30%) and Uganda (29%).

- A large number of Kenyan (82%) as well as Togolese (70%) cybercafés said that they do not allow pornographic
 content to be downloaded or viewed, but it is not clear how this is enforced. Uganda, Cameroon and The Gambia
 cafés show greater acceptance of accessing pornography Uganda presenting a particularly worrying rate,
 nearly 60%, followed by 46% in Cameroon.
- Cybercafés do not appear to take concrete measures to prevent customers from accessing pornography, which is of concern since such premises are visited heavily by children.
- Cybercafés owners and managers have hardly come across incidences whereby children were upset while using their services, with the exception of Uganda with nearly 60% acknowledging it, and Togo with around 35%.
- Hardly any of the cybercafés surveyed demands a valid ID from their customers.
- In terms of what is permissible and what is not within the cafés premises, there is a high degree of laxity in the surveyed countries: cybercafés owners usually create their own policies and guidelines, mainly to ensure that their business assets are not damaged, services are not disrupted etc.
- There is an absence of national policy frameworks on cybercafés operations and not much supervision from the ISPs about how their services are being used in these premises. It is evident that anyone who has money to invest can set up a cybercafé without going through a vetting process or inspection or to ensure conformity with protection standards.
- Across all countries the cybercafés demonstrated openness to implementing child safety measures.

Schools engagement

- On average, only 30% of the children surveyed said that they received any kind of guidance on safe Internet use at school. Most schools appear not to have filtering systems installed.
- In spite of the increasing use of ICTs among children and the many implications that this has, educational authorities do not seem to prioritise the capacity building of teachers to ensure child safety online, and there are no child protection frameworks to this end.
- Teachers would welcome such support but also seem to prioritise other types of learning in relation to ICTs. On
 the other hand, these duty bearers demonstrate a growing awareness of the risks involved and that this is a
 complex issue that requires greater preparedness.

Parental guidance

- The penetration of the Internet in the home is pretty low, except for Kenya. Usually the computer with Internet connection is placed in the living room (more than 50%), which can help to prevent misuse and unsafe practices by children.
- Nevertheless, children hardly receive any guidance from their parents regarding ICTs'safe use. Most of them fail to engage with children to share their experiences, properly assess what they are doing and advise accordingly.

2. INTRODUCTION

An ECPAT research conducted in Eastern Europe in 2008¹ revealed the quite extensive use of the Internet to sexually exploit children, not to mention the numerous cases of harassment by their peers, with tragic sometimes consequences. Similar research has been conducted by ECPAT in other regions,² but not in Africa, in spite of a number of reports that African children are being harassed and groomed online as well as being solicited for sexual services through webcams.³

Studies to assess children's vulnerabilities and the risks arising from their online presence - specially their increasing familiarity with social networking sites (Facebook, Mxit etc.), file sharing and downloads - are rare. The fact that ICTs are coming up with more advanced iterations poses further challenges, particularly in the African context, where there is no historical built up of knowledge and mechanisms to understand emerging risks and develop counteractions. A significant gap is the lack of indication about the numbers and the specific groups of children who may have been victimised by or are at risk of receiving sexual solicitations, luring by traffickers for sexual purposes, being exposed to depictions of sexual violence and child pornography, not to mention the extent to which African children are represented in the global child abuse image transactions.

This research project thus seeks to address some knowledge gaps, with a view to designing suitable interventions and alerting policy makers and relevant private sectors to the need to commit resources and develop plans to ensure the protection of children in ICTs. Although it is not designed to provide accurate numbers pertaining to the above, it sheds some light on the trends and patterns of ICT use by children and gives insight into their vulnerabilities in the countries where the research was conducted, namely Cameroon, The Gambia, Kenya, Togo and Uganda.

^{1.} ECPAT International. Regional Overview of Child Sexual Abuse Images through the Use of Information and Communications Technologies in Belarus, Moldova, Russia and Ukraine. 2008.

² ECPAT International. Child Abuse Images and Sexual Exploitation of Children Online. 2008.

According to a presentation made by the Communications Commission of Kenya (CCK) at the thematic workshop titled 'Child online protection in Africa', at the World Summit on Information Society - WSIS forum held in Geneva in May 2011; as well as to a presentation made by a South African hotline (The Films Publication Board) at the same meeting. http://groups.itu.int/wsis-forum2011/Agenda/ThematicWorkshops.aspx

3. THE SHARP PENETRATION OF TECHNOLOGY IN AFRICA: Major implications for child protection

The Internet plays a fundamental role in children's educational and learning experiences, being the largest easily-accessible, single source of information, reference material and resources. With the current growth of ICTs in Africa, in particular the increased use of mobile phones and wireless Internet and the popularity of cybercafés, more and more children are in contact with the online world. The ongoing deployment of the optical broadband link (under the project EASSY- East African Submarine Cable System)⁴ means that many more countries in Eastern and Central Africa are being connected to the global Internet through faster links, which has far-reaching implications in terms of child protection.

The uptake of technology in Africa is increasing rapidly. According to a report published by the United Nations Conference on Trade and Development - UNCTAD in 2011, there has been a significant increase in the uptake of mobile phones in Africa, comparing to the situation described in a previous study done in 2005. In The Gambia, for instance, this rise in mobile phones users was in the order of 85% compared to 16% in 2005; in Ghana, the number of users increased from 13.28% in 2005 to 71.49% in 2010. Kenya shows similar growth from 12.95% in 2005 to 61.63% in 2010.

The fast pace of mobile phones penetration shows remarkable resemblance with the increasing number of Internet users. In Ghana, for example, it has grown from 3.80% to 9.20% of the country's population, a rise of 242.11%. In the case of Kenya, it is a staggering 676% rise in Internet use compared to 2005. This increase tallies with the current government of Kenya's policy on ICT deployment, according to which ICTs will play a strategic role in fostering the country's economy in the next years. Much of the communications infrastructure is being developed based on wireless technologies such as mobile networks, enabling the provision of various services to the public as well as e-commerce and e-governance.

In countries like Kenya, mobile commerce is a very popular use of ICTs. Money transfers are commonly made through mobile phones, whereby the sender simply tops up the money at a kiosk and the recipient presents his details at another kiosk to collect the cash. This system, known as M-Pesa provided by Safaricom, has revolutionised the way people carry out financial transactions in Kenya. Although this technology has great potential and benefits, it can also be misused, for instance by luring a minor to send a sexualised image of him/herself through the phone and then receive money through this system, without even meeting the offender. It is important that the companies providing such services understand the risks and develop policies to prevent malpractices and alert users about possible risks to them and their children.

^{4.} http://www.eassy.org/about.html

In most of the countries assessed, the growth of mobile broadband in the business sector is also remarkably high compared to the fixed broadband. This is very significant as it means that businesses like cybercafés can start operating in rural and remote locations, providing access to the Internet to communities where education and awareness regarding the risks related to its use may be minimal or simply non-existent.

African children are therefore becoming common users of online applications, just like children in other parts of the world. The impacts of online experiences manifest themselves differently according to a child's age, gender and particular characteristics, and also in view of challenging conditions he/she might already be subjected to, such as social exclusion, domestic violence, sexual abuse etc. These factors can compound the risks and aggravate the harms they may suffer in their online practices. It is well known that a child can be more susceptible to grooming by a sex offender online, or by traffickers, if he or she is already in a vulnerable situation within the family or society, feeling lonely and desperately looking for some psychological support. The capacity of a child to deal with uncomfortable situations also depends on what projected as right or acceptable within their immediate environment and culture. For example, if a child is witnessing their parents access to pornographic content, or seeing adults in public places viewing pornographic materials, they may, in time, start to present unsafe behaviours, such as engaging in sexual activities at an early age and without the required guidance and precautions; producing sexualised images of him/herself and sending them to offenders upon receipt of cash; sending sexualised images to friends only to be harassed and blackmailed later on; developing a higher acceptance of providing sexual services in exchange for financial or other gains and thus becoming more vulnerable to sexual exploitation etc. On the other hand, a child who suddenly comes across sexual or violent images, or child pornography, may feel bewildered and react strongly to them, especially if there is no adult who is thought to be trustworthy to talk about such subjects and who can provide appropriate guidance. Even though it is hard to assess the full impact of such materials on a particular child, previous studies⁶ indicate that such exposures can result in changed behavior, confusing feelings around sexuality, and psychological trauma, besides having the potential to normalize certain behaviours that could be highly damaging, as mentioned above.

In this scenario, it is essential to reduce the risks and prevent harm to children, and there are various duty bearers who should be involved in the development of preventative strategies adapted to the African context. It is also important to observe and understand children's experiences online in order to teach them adequate self-protection strategies, build their resilience and ensure that proper mechanisms (such as helplines, counselling, peer support) are in place to assist them if disturbing or harmful incidents occur. This survey research study hence looks at distinct settings such as the home, schools and public places like cybercafés to get a better understanding of how these measures stand and how to effectively ensure safe use of ICTs by children in Africa.

Report published by the United Nations Conference on Trade and Development - UNCTAD in 2011.

⁶ B. Paul & D.G. Linz. The Effects of Exposure to Virtual Child Pornography on Viewer Cognitions and Attitudes toward Deviant Sexual Behavior, 2007.

4. CYBERCAFÉS: A unique feature of the digital landscape in Africa

Internet use in Africa presents a very unique characteristic compared to other regions: access to the online world is predominantly provided by the cybercafés as most people cannot afford to buy a computer. A large number of cafés have thus sprouted, almost as a cottage industry, rather than in a structured manner and regulated by the relevant authorities. Hence it is important to clearly highlight the role that cybercafés play in ensuring child safety online. Developing preventive strategies with them - such as promoting the adoption of a code of conduct - may involve working directly with the individual owners, given the loose association that exists between the cafés. Such codes of conduct may relate, for instance, to the practice of requiring customers to present an ID before using the café, since all sorts of criminal activities, and not only CSEC, are being facilitated by the anonymous online access afforded in public places. Another important measure is having filters installed to block age-inappropriate content. Moreover, ISPs must be involved with a view, for instance, to providing guidance on reporting illegal content and developing policies regarding acceptable use of their services. By all means, partnerships with law enforcement should be forged so that abusive images are reported by such stakeholders and cooperation in relevant investigations is strengthened.

There are indeed several factors that may affect how a child is impacted during his/her interactions in a cybercafé. This includes operating hours (as the child may be away from home unsupervised for longer hours), the type of activities they engage in at such spaces (type of content watched, using webcams, communicating with people that they do not know in real life) as well as the lack of understanding by cybercafé owners and managers about the various risks that they might be exposed to. Children who are allowed to use the same computers as adults might be accidentally exposed to age-inappropriate content (from the browser history, chat logs, downloaded files etc.), unless there is a mechanism within the café to prevent that. Moreover, the adult can be privy to the interactions of the child and gain information that is personal to them, potentially using it for ill-intentioned purposes. In search of higher profits, some café owners may facilitate the inappropriate usage of their facilities by children, allowing them to download adult material or to use webcams for sexualised communications. However, many simply ignore the harms that might be caused to children during the time spent at their cafés. This research thus sought to explore how such situations are manifesting themselves in the African context, in the countries where the study was carried out.

Some practices were found to be of particular concern:

- Lack of standards and mechanisms to ensure that adult / age-inappropriate content is not accessed by children.
- Lack of strict operational hours for children's admission.
- Lack of monitoring and guidance anyone can do whatever they want during their online sessions, as long as they pay for the services.

Whereas the research aimed to find out to what extent such practices are taking place, it is worth noting that the research process in itself was useful to generate awareness among the cybercafés, teachers and the children themselves about misuse of online interactions, paving the way for future interventions targeting key stakeholders and hopefully creating a better sense of accountability among them.

5. Engaging schools in child protection online

From providing education to building up core ethics and morals, schools have a huge impact in the life of a child, which lasts for their lifetime. Increasingly, schools are making use of ICTs for education and learning, and with the support of national policies (for example in Kenya) it is not surprising that schools are providing access to the Internet as a means to step up the education system. It is quite important to evaluate whether such deployments are accompanied by adequate child protection mechanisms, and if not, what are the missing links. The involvement of schools in child protection is of primary importance especially in Africa, where previous research has demonstrated that girls are highly susceptible to sexual violence within the school environment⁷ in this continent. Having more access to online technology means that their interactions with potential abusers and exploiters are no longer limited to their locality. It also offers new ways for their peers and others to reach them with a view to harassing or abusing them, soliciting sexual services and sexualised images etc. Moreover, their sudden exposure to new lifestyles, values and cultural perceptions might incite them to adopt risky behaviours if proper guidance is not at hand.

It is important to underscore the importance of providing all sorts of new opportunities for children through the evolving ICT tools and technologies, instead of presuming that all risks will lead to harm. Nevertheless it is also essential to bring the right set of knowledge and education to them in order to prevent certain actions that carry greater possibility of harm. This research study sought to assess the fundamental principles governing schools' practices in terms of ICT and child protection in the researched countries. The questions posed to teachers and students thus covered, among other themes: a) school curriculums on Internet safety; b) policies related to Internet use; c) awareness, among teachers, of the risks posed by online interactions; d) knowledge and skills of ICT usage amongst teachers; e) incidence of child sexual exploitation through ICTs in the school environment, among other aspects that have a bearing on child protection online within the school environment.

^{7.} ECPAT International. Linkages between HIV/AIDS and the Commercial Sexual Exploitation of Children in Africa. 2007. Accessible from: www.ecpat.net. This information was also gathered during missions undertaken by ECPAT officers to some African countries.

6. Approach and methodology

Research purpose

The research aimed to shed light on the situation in Africa with regard to current risks and harms caused to children by their use of ICTs.

As such, it explored when and how children access ICTs, what are their patterns of interaction according to gender and age, what forms of protection they use, what is their notion of exposure to risks, in which cases they recognise risky situations, and their ability to report and request help.

Additionally, it assessed the level of prevention of abuse and exploitation online in each of the three key locations of ICTs use by children - the home, the school and the cybercafés - with a view to identifying gaps and defining strategic interventions for online safety in these key locations.

Participating countries

Cameroon, The Gambia, Kenya, Togo and Uganda, mostly in the capitals but also in some smaller towns were the Youth Partnership Project had a presence.

Target groups

A total of 1.073 respondents were reached, from the following groups:

- 1. Children aged 11-18, disaggregated by age and gender (875 in total)
- 2. School teachers involved in ICT education (105 in total)
- 3. Cybercafés owners and managers (93 in total)

Data collection methods

Individual assessments through three types of survey sheets (see annexes), distributed respectively to children, cybercafé owners/managers as well as teachers, in schools and cybercafés selected randomly.

All respondents received explanations regarding the purpose of the study and why they were invited to take part in it. They were then asked to fill up the questions within a given timeframe while the researchers waited. This eliminated the possibility that their responses would be influenced by others. Previously, a pilot process was carried out in Togo to assess the feasibility of the survey and to incorporate the feedbacks in the design of the questionnaire.

Although the drafters of the questionnaires and the researchers undertook every effort to make the questions clear and easy to understand, it is important to note that some of the respondents may not have been able to fully grasp their meaning or may not have provided a honest opinion due to a variety of reasons.

Youth-led approach

Over the past years, ECPAT International has developed considerable expertise in carrying out youth-led research studies, given the many benefits of engaging youth in research with children:

- 1. Children and young people open up and share information more easily and comfortably with their peers, particularly when discussing issues such as sexual exploitation. This helps gather better quality data in comparison to employing adult researchers (provided that the young researchers are properly trained).
- 2. It is easier for them to access and mingle with their peers.
- 3. Young people can provide valuable inputs on research methodologies and strategies, and design questionnaires that are child-friendly and relevant to the target stakeholders, being in the same age group as the child respondents and knowing well the local communities characteristics.
- 4. The involvement of local youth as researchers lends credibility, builds trust and facilitates access to community members.
- 5. Engaging young people in this type of activity is also tremendously empowering: it builds their self-esteem; develops interpersonal skills; enhances their knowledge on the issue, allowing them to better protect themselves and their peers; gathers the respect of fellow community members; and can give new directions to their lives, as many become activists or get further involved in some kind of advocacy or community work.
- 6. The capacity building they receive on research processes, interview techniques, ethical considerations, data collection, tabulation and analysis can be valuable professional skills.
- 7. Young people bring fresh energy and spirit to the whole process.

In this context, the research was undertaken in coordination with ECPAT International's Youth Participation Project YPP, which is implemented in various countries around the world. The YPP seeks to prevent the commercial sexual exploitation of children (CSEC) through peer education and support, a truly effective strategy to reach at-risk children. Peer supporters - many of them at-risk or survivors of CSEC - are thus trained and mentored to implement a wide range of activities in shelters and schools mainly, to empower and better protect children from CSEC. They are also involved in campaigns and advocacy targeting decision makers, local authorities, law enforcers, cybercafés and other important stakeholders. Except for Kenya, the participating countries benefited from the presence and expertise of local YPP teams to carry out the research, composed of peer supporters, youth motivators and youth advocates. Their contribution was crucial in several ways: they provided feedback on the questionnaire after sharing it with local peers for their inputs, introduced the research project to local educational authorities, and reached out all three categories of respondents to have the survey answered, having explained its purposes to all.

Before the research project started, the young YPP researchers received training focusing on:

- The goal of the research and how the information gathered will be used;
- · Child sexual exploitation online and its different manifestations;
- Protection of children in ICTs;

Methods of approaching children and adults.

- Possible challenges and difficult situations during the research process;
- How to access support from designated adults whenever necessary;
- How to handle sensitive questions and queries from the respondents;
- Ethical issues in doing research with children, such as confidentiality, non-judgmental attitude, safeguarding the privacy and the personal details of the respondents;
- The responsibility to set off protection measures when needed etc.;
- Data collection, tabulation and the analysis process.

7. KEY RESEARCH FINDINGS

The following selection of key findings provides an overview of the current risks and harms to children when using ICTs in the selected African countries. The findings are divided in sub-sections related to:

7.1 Children's behaviour and vulnerabilities online 7.

7.2 Access from cybercafés

7.3 Family settings and parental guidance

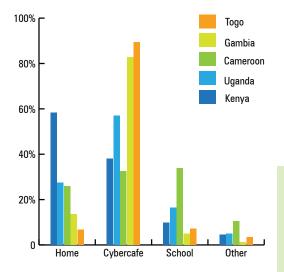
7.4 School setting

In each sub-section, the questions made to the three types of respondents - children, cybercafé owners/managers and teachers - are followed by graphs and tables accounting for the responses given, which sometimes show the variations from one country to another. A brief analysis then follows.

7.1 CHILDREN'S BEHAVIOUR AND VULNERABILITIES ONLINE

QUESTIONS TO CHILDREN

Where do you usually access the Internet?

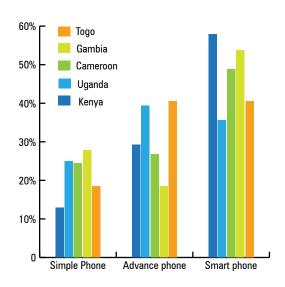


With the exception of Kenya, cybercafés are, by far, the location where children in the researched African countries access the Internet most, mainly because they have no computer at home (about 70% have no computer). Hence preventative initiatives to ensure child safety online must thoroughly involve cybercafés' staff, managers and owners. In Uganda, Cameroon and The Gambia the research indicated that children contribute to a significant percentage of the cybercafés' income.

African children in the researched countries are already using the Internet between one and two hours per day. A significant amount of their online time is spent playing games and on social networks such as Facebook. Most of them discover websites of interest either by surfing the net themselves or through friends.

What kind of mobile phone do you have?

The majority of interviewed children — except in Uganda — already use smart phones instead of the simpler versions, although some of them affirmed that they do not use them to go online because it is expensive (especially in Togo). Around 84% are exchanging files by Bluetooth and MMS, which can be done through a simple phone model.



Question 26 100 80 40 40 Kenya Uganda Cameroon Gambia Togo

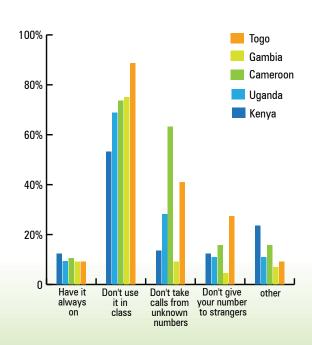
Did your parents set rules on how you can use your mobile phone?

There seems to be little guidance from parents regarding the use of mobile phones by their children, and on average only 50% of them set some kind of rule for the varying age groups.

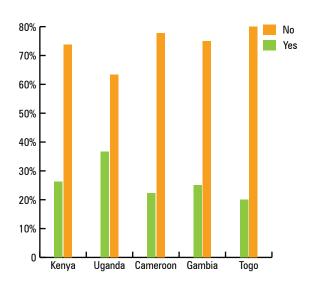
Compared to the other countries, parents in The Gambia showed higher concern, especially in relation to younger girls (11-13 years old), taking measures to prevent misuse. On the other hand, none of the Gambian boys aged 11 to 13 received any type of guidance from their parents.

What are the rules (on mobile phones use) about?

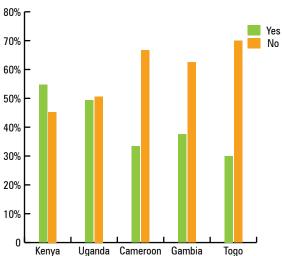
The biggest concern for parents around the use of mobile phones by their children is that they might waste time during school hours. Less than about 30% alert their children that it can be dangerous to give their number to or accept calls from strangers. The understanding from parents regarding potentially harmful uses of mobile phones — e.g. exchanging sexualized images of oneself or receiving money for this — is extremely poor. Also, there is a marked difference in the advice given to boys and girls towards giving numbers to strangers, which may indicate that parents see their daughters as more vulnerable than their sons.



Have you ever felt the compulsion to see adult content such as pornography, using the Internet connection at home?



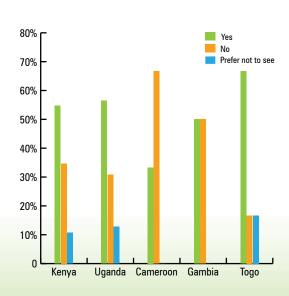
⇒ Have you ever seen adult content on the Internet (pornography such as photos or videos of people having sex) at home or other places – such as at cybercafés with your friends?



Exposure to age inappropriate content such as pornography can take place through intentional searching (in public websites, photo sharing sites, media download sites, video sharing sites such as Youtube, social networking websites) and also through accidental access (via automatic pop-ups, email links, web redirects or typos that are cleverly redirected by creators of such sites).

Did you ever see anyone of your age or younger in such images or videos?

This set of questions is quite revealing. It shows that only between 20% and 36% of the researched children felt interested in seeking adult content /pornography online. However, around half of them have actually seen such content, which suggests that they may come across it inadvertently. In addition, 58% of the researched children know about friends who had seen such content online (72% in Cameroon), and among these 56% shared it with them (again, a particularly high incidence of 69% in Cameroon). It is highly disturbing that more than half also came across child pornography (less so in Cameroon, with 33%).



Some examples of the impact of ICTs penetration without the required child protection measures can be drawn from the Philippines, where a number of perpetrators have been arrested in connection with cases where children were forced to pose in front of a webcam in various states of undress and also while enduring physical sexual abuse, for the trade of such images online through money transfer services. Families have also resorted to such criminal activities as a way of making quick money, using their own children and sometimes their neighbours', wrongly assuming that such acts are harmless in comparison with actual child prostitution. The perceived anonymity afforded by the Internet and the absence of physical contact help parents delude themselves into thinking that the children are not being victimised or affected. Since this is usually done at home, they often mistakenly believe that the police cannot track them. Also failing to understand the impacts of such activities, young girls in the Philippines are using online video streaming channels to perform to paying audiences from all over the world. They provide their personal details and the time when they will be available online, and have some sense of control as they are not within the physical reach of offenders. However, they are unaware of the mental agony that is often experienced later on in their lives, when they realise that such images will be forever available on the Internet. The psychological and other impacts of such actions must be more broadly discussed in society, especially in emerging economies where ICTs are becoming increasingly prevalent and children, young people or their parents might utilise these online platforms to make quick money without being aware of the implications.

⇒ In your school, have you ever attended any event that talked about risks arising out of using the Internet?

It is of serious concern that, on average, only 30% of the children surveyed actually received any kind of guidance on safe Internet use at school. Such a low rate indicates that it is indeed essential to educate schools about their important role in this regard and to build their capacity to properly guide children on safe online practices.

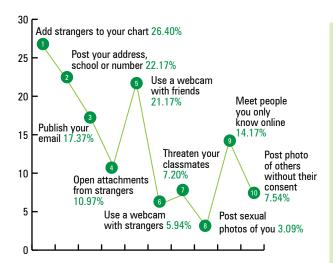
No Our school has not organized such event organize

Yes

Do you do any of these actions when using the Internet or a mobile phone?

Online practices that have the potential to cause harm do not seem to be particularly widespread among the

interviewed children. Nevertheless, about 22% post personal details such as their address, school and number, and 14% meet people they only know online, which are some of the most dangerous practices. While some of the above mentioned activities are common for ICT users — such as chatting with strangers and using webcams - it is essential that they are carried out with full knowledge of how to do it safely as well as awareness of the risks. Children must be taught how to stop actions that may lead to uncomfortable and dangerous situations — such as "grooming" i.e. having a stranger ask questions of a sexual nature, sharing child and adult pornography images etc. so as to slowly break their resistance and finally obtain sexualised images, solicit sexual services or abuse them in an arranged offline meeting.



In 2009, a 61 year-old Norwegian national was arrested in Gambia for taking pictures of naked women and girls, and charged with the offences of child pornography and defilement. He was sentenced to one-year imprisonment based on article 8 (1) of the Tourism Offences Act 2003 for child pornography, but was acquitted of the charge of defilement. The Judge stated that it was "an affront to our customs and traditions as a nation. It is therefore tantamount to an abominable act that is intolerable and unforgivable". Gambia is a well-know sex tourism destination.

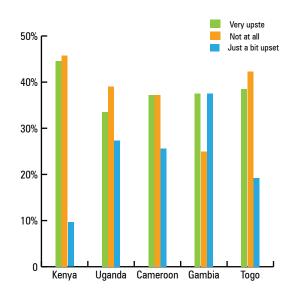
Has anyone ever tried to hurt you on the Internet through the following?

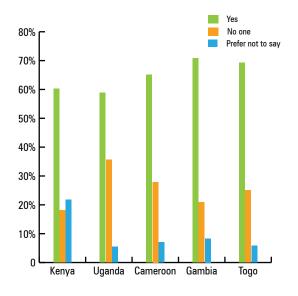
i) Sending you inappropiate images or videos of adult pornography								
	Total	Kenya	Uganda	Cameroon	Gambia	Togo		
i) Yes	15.09%	18.18%	19.10%	11.69%	17.28%	6.73%		
ii) No	77.14%	76.86%	78.28%	49.35%	71.60%	88.46%		
iii) Don't know	1.37%	2.07%	0.37%	0.00%	4.94%	0.96%		
iv) Prefer not to answer	6.40%	2.89%	2.25%	38.96%	6.17%	3.85%		
ii) Asking you to pose in front of the ca	mera wihout	clothes on						
i) Yes	10.51%	12.81%	12.73%	3.90%	16.05%	5.29%		
ii) No	82.06%	83.88%	84.64%	57.14%	71.60%	89.90%		
iii) Don't know	0.91%	0.41%	0.37%	0.00%	4.94%	0.96%		
iv) Prefer not to answer	6.51%	2.89%	2.25%	38.96%	7.41%	3.85%		
iii) Demand that you receive the photo	s/videos they	send to you	which you	did not feel cor	nfortable wi	th		
i) Yes	7.20%	7.85%	7.49%	0.00%	16.05%	5.29%		
ii) No	85.49%	89.67%	89.51%	61.04%	71.60%	89.90%		
iii) Don't know	1.03%	0.83%	0.37%	0.00%	4.94%	0.96%		
iv) Prefer not to answer	6.29%	1.65%	2.62%	38.96%	7.41%	3.85%		
iv) Asked you to add them to your frier	nds list even t	though you c	lid not want	to				
i) Yes	14.51%	12.40%	22.47%	1.30%	16.05%	11.06%		
ii) No	78.17%	85.12%	74.53%	59.74%	71.60%	84.13%		
iii) Don't know	1.03%	0.83%	0.37%	0.00%	4.94%	0.96%		
iv) Prefer not to answer	6.29%	1.65%	2.62%	38.96%	7.41%	3.85%		
v) Posted bad things about you in text	format or upl	loaded your p	personal pho	tos/videos wit	hout your kn	owledge		
i) Yes	9.03%	8.68%	11.61%	0.00%	17.28%	6.25%		
ii) No	81.26%	87.19%	81.65%	61.04%	70.37%	85.58%		
iii) Don't know	2.63%	1.65%	3.37%	0.00%	4.94%	2.88%		
iv) Prefer not to answer	7.09%	2.48%	3.37%	38.96%	7.41%	5.29%		

[&]amp; Gambian News, Norwegian National Gets 1 Year Jail Term, 22 May 2009, accessed on the 12th April 2012 from: http://www.gambianow.com/news/News/Norwegian-National-Gets-1-Year-Jail-Term.html

⇒ If that has happened, how upset were you about the incident?

The vast majority of children did not report the occurrence of some incidences that can be harmful to them. An exception is Cameroon, where, 38% of the surveyed children did not want to provide an answer to this question. On the other hand, between 30% and 25% of those who did experience such incidences felt very upset about it, especially girls aged 14 to 16, followed by girls aged 16 to 18. Between 35% and 47% felt just a bit upset, which may indicate that either they are not unfamiliar with such incidences and thus do not feel so shocked, or else are better prepared to deal with them.





Did you talk to anyone about what had happened? If you had said yes, who would you approach for this?

Most of the children surveyed rely on friends to discuss upsetting incidences online, or else do not talk about them with anyone.

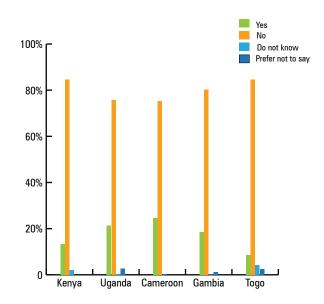
⇒ If you are still thinking of the incident that took place, did you do any of the things below in response to what happened to you?

	MALE			FEMALE			
Age between	11-13	14-16	17-18	11-13	14-16	17-18	
i) I Stopped using the Internet for a while	15.79%	16.05%	14.75%	19.44%	22.35%	17.02%	
ii) I deleted all messages from the person	18.42%	22.22%	16.39%	25.00%	12.94%	8.51%	
iii) I changed my privacy/contact settings	15.79%	14.81%	21.31%	11.11%	11.76%	23.40%	
iv) I blocked the person	36.84%	22.22%	34.43%	22.22%	22.35%	29.79%	
v) I reported the problem	2.63%	4.94%	4.92%	2.78%	4.71%	4.26%	
vi) None of these	21.05%	34.57%	24.59%	38.89%	30.59%	29.79%	

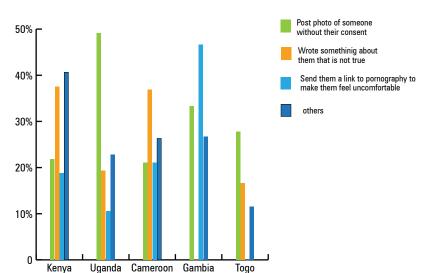
There are many possible reasons to explain why children are not reporting the problems they face: there may be no reporting system in place, or they may not be aware of it; they are not aware of the gravity and risks associated with the event; they do not trust others to discuss it; they might blame themselves; or may chose not to be in conflict with the person who provoked the incident. Such explanations were given by children who took part in previous research in other regions of the world. Lack of reporting is a serious concern, and there should be channels in place for children to do so, anonymously if preferred, and to obtain the necessary support, not to mention the need to involve law enforcement when serious offences are committed or else to provide information that may help current investigations on pedophiles, child pornography and trafficking rings etc.

In the last months have you acted in similar ways as above?

While most children do not appear to act in these distressing ways, the percentage of those who do are not particularly low in Cameroon (nearly 25%), Uganda (21%) and The Gambia (nearly 19%), which suggests there is a need to educate them about the potentially harmful effects of such actions.

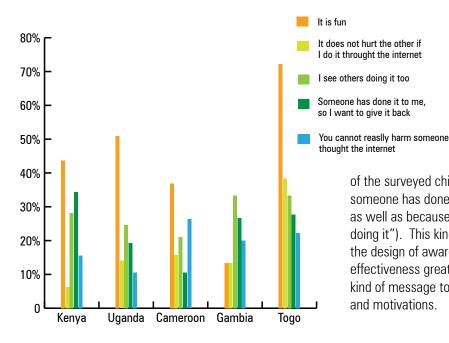


If your answer was yes, what exactly did you do?



The Gambia presents a higher incidence of the sharing of pornography links among children (46% - although this is only among the 18% of the surveyed children who revealed that they acted in these ways).

What would be the main reason for you to behave like that?

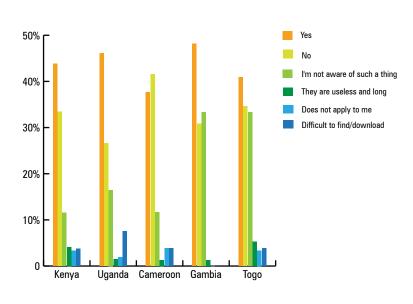


The vast majority perform such acts because they think it is "fun", which again suggests the need to generate greater awareness among children regarding the damage that certain online practices can actually cause. Moreover, about a quarter

of the surveyed children act in such ways because someone has done the same to them (34% in Kenya), as well as because of peer influence ("I see others doing it"). This kind of information is important for the design of awareness raising campaigns, as their effectiveness greatly depends on sending the right kind of message to children, in tune with their realities and motivations.

Do you read any safety guidelines for using the Internet that is posted online?

Even though almost 45% said that they do read such materials, a large number (32%) said that they do not, while about 14% showed ignorance of such materials - which means that most children do not really consult safety guidelines. Clearly, a big area for improvement is targeting such awareness raising materials to the appropriate demographic of users, making them more attractive and meaningful to their experiences online. Interestingly, only a very small percentage of all age groups from both genders expressed that they did not need such guidelines or instructions. This suggests that children do not always

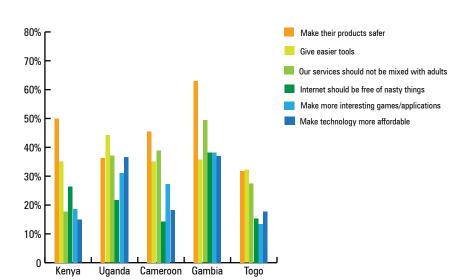


believe that they know everything and do not need help, in contrast to what people tend to think.

Even though many cases have been documented worldwide, children continue to fall victim to sexual abuse by an offender whom they meet offline. To children, communicating with strangers online can be seen as opportunity to make friends and have fun, which in most cases is true, whereas from the view point of parents and adults this is perceived as a real risk. Whether it is a risk or an opportunity, many children who go online to look for friends to share their feelings and experiences will end up meeting them in real life. The understanding of the risks, the preparations for the process (such as telling parents about such encounters or involving them

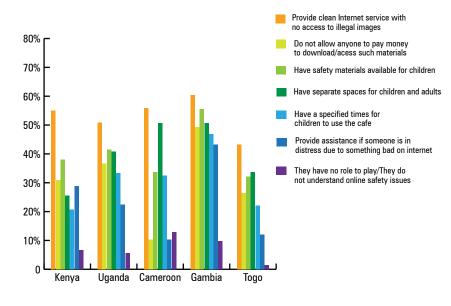
in the meeting) is important and needs to be part of the learning for both parents and children. Moreover, such learning must be facilitated for children in ways that acknowledge and respect their motives - e.g. wanting to find a boy/girlfriend, trying to escape loneliness, seeking to exchange knowledge about specific subjects etc. - with appropriate language and media.

What do you think the big companies should do to help your online experience?



Somewhat surprisingly, most children in all countries except Uganda – between 31% and 62% - mentioned safety as the main aspect that needs to be enhanced by ICT companies. This is followed by the desire to be provided with easier tools, and by the need to have services that are not mixed with those provided to adults. Not many showed concern, however, about having the Internet free from "nasty" things (with exception of The Gambia).

What do you think the cybercafés should do to make Internet access from their cafés safer for children?

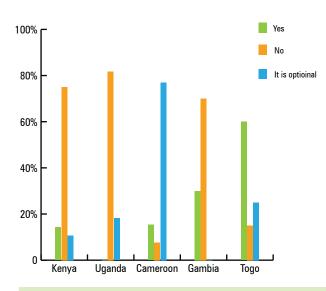


In line with the answers to previous questions, children want to enjoy safe online experiences and would welcome most of the key measures that can be implemented by cybercafés in order to guarantee their protection.

7.2 ACCESS FROM CYBERCAFÉS

QUESTIONS TO CYBERCAFÉS OWNERS / MANAGER

Do customers need to register or sign up before they can use your café? If yes to the question above, was it mandated by the regulatory authorities?



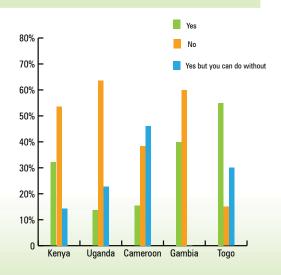
Except in The Gambia and Togo, there are no regulations obliging customers to register or sign up before they can use a cybercafé. Although some respondents in those two countries mentioned that this is mandated by the authorities, therefore perhaps the other cybercafés are simply unaware of such regulations. Very few cafés - in The Gambia, Togo and Cameroon only - require customers to do so by their own initiative, Togo being the country where such rates are higher (40%).

The anonymity afforded by cybercafés that do not request a valid ID from their customers means that law enforcement officers will track down the cafés' computers and not the offenders' whereabouts when investigating sharing of child pornography and other child abuse materials, money transfers, dialogues

between child sex offenders in chat rooms and between groomers and children etc. Many countries in Asia (for example in India) and Europe already make it mandatory for users to provide their credentials before using cybercafés facilities, to ensure that they can be traced in case they commit any illicit activity while on the Internet, and also to deter the misuse of their online presence.

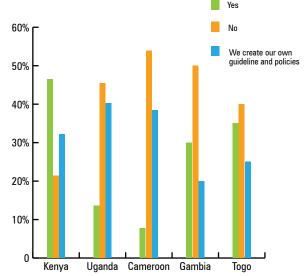
Do you have to sign a contract or an agreement before you can start up your café?

The sector is highly unregulated, as in most countries it is not even necessary to sign a contract (i.e. apply for a permit/ license that is granted once certain criteria are fulfilled) to start up a cybercafé. Similarly, the control by authorities is inadequate when contracting is mandatory. Again, Togo exhibits the higher percentage of cybercafés indicating a presence of such regulation, though it is possible to operate without it. The contradictory responses within the same country may indicate that the cybercafés are unaware of existing regulations or there is no monitoring by the relevant authorities.



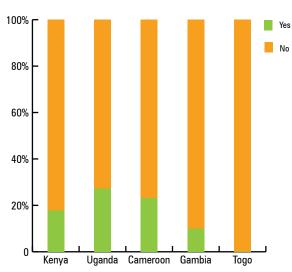
Is there any kind of guidelines that are made available to you that say what you can or cannot do in your café environment?

Similarly, the absence of guidelines about what is allowed in Internet cafés is reported — or perhaps most cybercafés are unaware of the existing ones, which would suggest lack of proper dissemination. The research suggests that most cafés either have no policies at all or develop their own.



Do you have separate spaces for children and adults?

Very few cybercafés provide a separate space for children (none of them in the researched Togo and the Gambia cafés). A separate space for children normally refers to a place within the cybercafé that is equipped with computers meant only for children's use, where adults cannot enter. It could be an area isolated by glass walls or other partitions which prevent access to those children by adults. Sometimes the computers in such areas have restrictions regarding the type of content that can be accessed, but this element is also missing in the cafés in the countries examined.

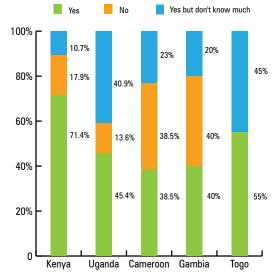


Why did you create a separate space for children?

The cafes in Togo and Gambia do not have separate spaces for children and adults hence they did not respond to the

ahava quastiannaira					
	Kenya	Uganda	Cameroon	Gambia	Togo
a) So children don't see adult content or mix with adults	3.57%	13.64%	15.38%	0.00%	0.00%
b) Adults are disturbed when children are around	10.71%	13.64%	7.69%	0.00%	0.00%
c) Adults specifically asked	0.00%	9.09%	7.69%	0.00%	0.00%
d) Children specifically asked	7.14%	13.64%	0.00%	0.00%	0.00%
e) So that children use specific computers with filters	10.71%	13.64%	7.69%	0.00%	0.00%
f) So that I can monitor them through the server	7.14%	4.55%	7.69%	0.00%	0.00%

Are you aware of any risks that children might face while using the Internet?



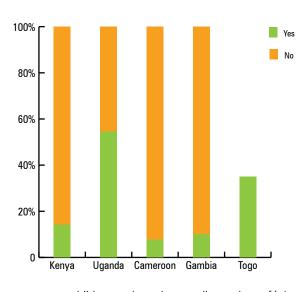
Generally, under 40% of cybercafé owners and employees consider themselves lacking knowledge about the risks to children when going online (Kenya and Uganda presenting much lower rates).

⇒ If you answered yes to the previous question, can you list what type of risks they might face while using the Internet?

Almost all mentioned pornography, fewer mentioned access to violent content and very few mentioned abuse, deception, trafficking or in contacting with dangerous individuals. This demonstrates very little actual knowledge of the range of vulnerabilities that may affect children online.

⇒ Have you ever had a case in your cybercafé where a child/children were upset with something they saw or did on the Internet?

In the countries surveyed, cybercafé owners and employees have rarely come across such incidences, with the exception of Uganda, where nearly 60% of those surveyed reported it, and Togo with around 35%. These are significantly high rates. However, while a significant percentage of the children who were upset asked for help in Uganda, they did not do so in Togo. There could be numerous different reasons for such behavior, for example they were better able to deal with the situation themselves (ECPAT has run the

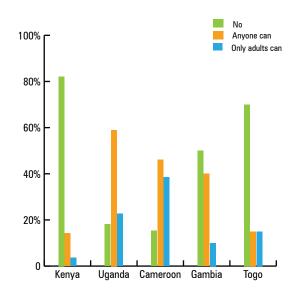


Make IT Safe campaign in Togo, to build capacity and awareness amongst children and youth as well as cybercafés), or they did not think the café managers would be able to help them. Regardless, there is indication that such upsetting incidences do take place in cybercafés and could be risky for children.

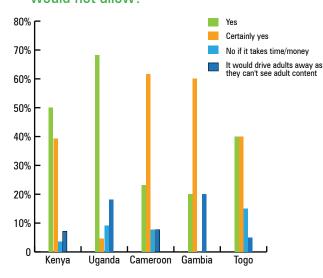
Incidences that may upset a child range from being approached by strangers online; coming across offensive content such as pornography, illegal materials, depictions of violence and being harassed, among others. They also include "physical" incidents within the café premises, such as being approached by an adult with a sexual solicitation, watching others engaging in sexual activities or posing in front of the webcam nude etc. It is important that the communication established between the businesses and the clients promote the reporting of such events.

Can someone download or view pornography in your café?

A large number of Kenyan cybercafés (82%) said that they do not allow pornographic content to be downloaded or viewed. It is not clear how this is enforced (e.g. clear rules that users have to sign up for, or by filtering such content). In Togo, this is not permitted in 70% of the cafés. Whereas in Uganda, Cameroon and The Gambia, there is much greater acceptance of the fact that pornography can be viewed or downloaded by anyone who uses the cybercafé — Uganda presented a particularly worrying rate, nearly 60%, followed by 46% in Cameroon. If anyone can access pornography at the cafés, this means that children are allowed to do so as well. It can also mean that adults may view, download and/or distribute child abuse materials.



Would you mind if your customers go to other cafés that allow certain activities that you would not allow?



Most cybercafés would not design their policies based on the fear of losing customers. There is indication that Kenya would be particularly open to adopt policies that encourage ethical use of the Internet, whereas in countries such as Cameroon it could be more challenging to promote them.

→ Have you ever seen anyone in the café (including a child) appear in front of the webcam in revealing poses or trying to take off their clothes (particularly when they are using a computer alone and not visible to others)?

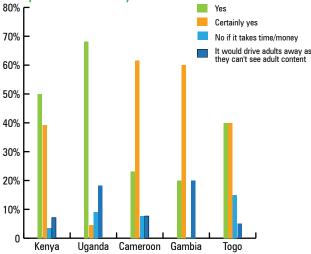
Such incidences are basically non-existent. Although a very small number is represented, in Uganda and Cameroon such accurrences were was actually reported.

With growing access to, and increased affordability of accessories such as webcams and the relatively cheap cost of broadband Internet, cybercafés in most countries are equipping their computers with services that allow broadcasts to be generated. As social networks and online platforms such as YouTube facilitate the creation and immediate uploading of media content, particularly videos, it is important to bear in mind the implications of such systems. For example, children may upload their own compromising videos but come to deeply regret it later, often because of associated harassment. Even though this kind of activity is seldom performed in public places such as cafés, the availability of isolated chambers, off-hour access etc. facilitate such interactions. Around 80% of the cybercafés in the countries examined have webcams and microphones that can be used by anyone including children. Togo is an exception - just half of the cybercafés examined have these devices, and among them only 50% allow them to be used by children.

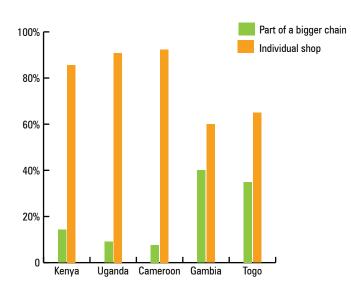
Would you like to know more about how to help children use your café in a more secure

and comfortable manner?

It is extremely positive that across all countries there is a general openness to implementing child safety measures.



Is your cybercafé part of a larger association or network of cybercafés?

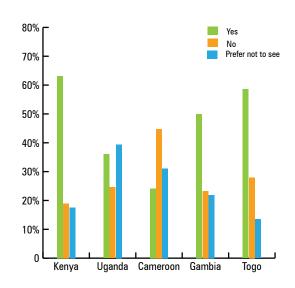


Most cybercafés are owned by an individual and not linked to a larger chain, which suggests that it could be more laborious and time consuming to reach them through projects to raise awareness and implement the adoption of policies to ensure child safety online. Special strategies would have to be designed to adequately educate and involve all stakeholders in the development of a code of conduct – such as involving children and young people as campaigners for that purpose, using local contacts in the field and balancing revenues to diminish the fear of losing revenue etc. Such initiatives are all the more necessary in view of the absence of governmental regulations and policies.

QUESTIONS TO CHILDREN ABOUT CYBERCAFÉ USE

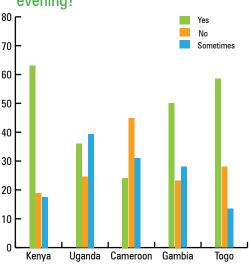
Does the cybercafé manager allow you to use the facilities in the cybercafé at any time of the day? (percentage of those who said YES)

In the countries examined, not all cybercafés have policies to impede children's use of their facilities at certain hours that may be particularly risky (e.g. late hours), when such policies exist, the duration and timing varies widely from one cybercafé to another within and across countries. For example, in Kenya children are not allowed to use the café after 6 pm, though one of the respondents said that they extend it to 7 pm. Some cafés would not allow children between 9 am and 4 pm, which are usually school hours. In The Gambia some cafés allow



children to enter until 11 pm, while in Cameroon there are no such time restrictions, even though some respondents said that children are not allowed to stay "too late".

Does the cybercafé owner charge you extra money to stay during late hours in the evening?



It is disturbing that a high number of cybercafés not only seem to allow children to use their facilities at late hours but also charge them extra money for doing so.

Why do you choose to come to the cybercafés?

Most children use cybercafés because they do not have a computer at home. They do not seem concerned about their parents' supervision, which may indicate that they have little interest in accessing pornography or doing other practices that may be frowned upon by their parents.

	MALE			FEMALE			
Age between	11-13	14-16	17-18	11-13	14-16	17-18	
i) No parents watching	13.92%	6.93%	1.63%	21.74%	6.71%	8.14%	
ii) Stay as long as you want	22.78%	11.39%	13.82%	13.04%	8.05%	11.63%	
iii) No computer at home	54.43%	58.42%	49.59%	50.72%	59.73%	51.16%	
iv) It's cheaper	16.46%	12.38%	14.63%	11.59%	6.71%	12.79%	
v) Play with other friends	16.46%	12.38%	13.82%	17.39%	10.07%	8.14%	
vi) More features available	20.25%	12.87%	18.70%	17.39%	15.44%	16.28%	

Do you go to the cybercafés in groups?

	MALE			FEMALE		
Age between	11-13	14-16	17-18	11-13	14-16	17-18
i) Yes	20.25%	14.85%	17.89%	20.29%	12.08%	10.47%
ii) No	43.04%	33.17%	31.71%	30.43%	43.62%	47.67%
iii) Sometimes	36.71%	51.98%	50.41%	49.28%	44.30%	41.86%

Apparently most children do not regularly go to cybercafés in groups, only occasionally.

A consultation about child safety online held in Africa in 2010* shed light on the implications that frequenting cybercafés in groups has on child protection issues. When going in groups to a cybercafé, male children and youngsters usually feel more comfortable to download adult and other inappropriate content, as they have the support of their peers. They also feel validated about watching such materials as their friends seem to enjoy the same things. Moreover, sometimes their group covers a large area and others cannot see what they are viewing and downloading, not to mention that sharing the costs makes it cheaper. In the case of girls, they also feel more secure when exchanging information on dating sites, assessing dating candidates online, and exploring social networks together, whereas they may feel more embarrassed to use the Internet publicly for such purposes when they are alone.

^{*} Regional capacity building session on Make-IT-Safe conducted by ECPAT International in Togo in August 2010

Can you download any content you like from the cybercafé? (percentage of those who said YES)

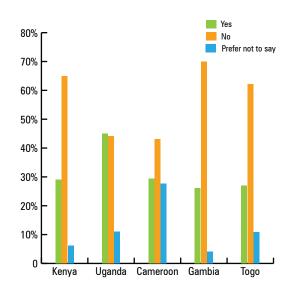
In Kenya, the answers from the children slightly contradict those given by cybercafé staff: more than 80% of the cybercafés said that customers cannot download pornography from their premises, while between 38% and 59% of the Kenyan children said that they can download whatever they wish. They may not have been interested in downloading pornography or illegal material – though this sheds some light on whether there are restrictions or not.

	MALE			FEMALE		
Age between	11-13	14-16	17-18	11-13	14-16	17-18
i) No parents watching	35.44%	34.16%	45.53%	36.23%	29.53%	23.26%
ii) Stay as long as you want	48.10%	51.98%	37.40%	44.93%	57.05%	50.00%
iii) No computer at home	16.46%	13.86%	17.07%	18.84%	13.42%	26.74%

Have you ever been approached by an adult you did not know at the café?

More than 25% of the respondents said that they felt uncomfortable with the approach by an adult while they were in the cafés, citing various reasons for that: such as the approach was inhibitive, that it interfered with their activities or the type of the online activities of the adults. The responses are fairly consistent across the countries.

In 2006, a French citizen was convicted in Togo on child pornography charges and sentenced to five years imprisonment and a fine of 20.000.000 FCFA. The abuser was the owner of a restaurant in the city of Lomé, where he used to photograph little girls. His accomplice, a local woman who provided him with the girls, was convicted to 30 months' imprisonment and a fine of 500.000 FCFA.



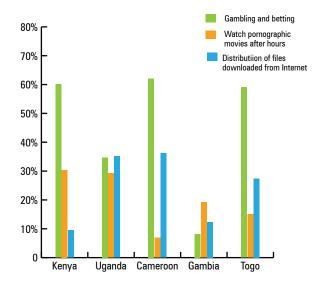
In March 2012, the Ugandan justice system convicted a 53-year-old Turkish man to two years imprisonment or a fine of 6 million shillings for molesting more than 50 girls and producing child pornography material. Following this case, the Ugandan government declared it would start doing background checks on tourists entering the country. There are many cases of prosecutions related to child pornography in African countries, but they often involve child sex tourists and rarely involve nationals. It is well-known that sex tourists seeking to abuse children and produce child pornography usually undertake a "grooming" process where they approach children in places where they gather — such as a cybercafé — and befriend them by, for instance, offering gifts as well as a mobile phone to establish access to them.

^{9.} ECPAT International. Togo: Global Monitoring Report on the status of action against commercial sexual exploitation of children. p.27. 2011. Accessed from: http://www.ecpat.net/EI/Pdf/A4A_II/A4A2011_Africa_TOGO_FINAL.pdf

Uganda People News. 'Government to Crack down Foreign Criminals . 29 March 2012. Accessed on 13th April 2012 from: http://www.ugpulse.com/uganda-news/people/government-to-crackdown-foreigner-criminals/24682.aspx

→ What are some of the activities that you have seen happening in a cybercafé?

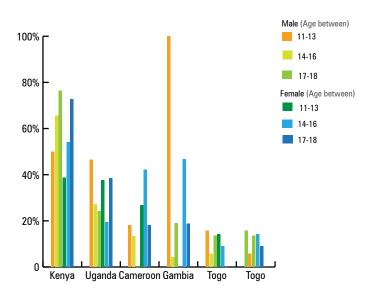
Children did report having seen people accessing pornography at the cybercafé at late hours, particularly in Kenya (30%) and Uganda (29%). They also saw other café customers gambling and betting. Again it is surprising that Kenya, the most advanced country in terms of ICT, displays poorer standards in terms of online safety for children.



7.3 FAMILY SETTINGS AND PARENTAL GUIDANCE

QUESTIONS TO CHILDREN

Do you have a computer with Internet connection at home? (percentage of those who said YES)

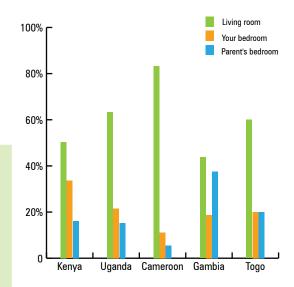


The answers corroborate the fact that Kenya is the most advanced country in terms of accessibility to ICT, as many homes already have a computer linked to the Internet in this country. The other countries surveyed show very low percentages in this regard.

The computer is located at:

Most children who have Internet access at home, in those countries surveyed, use their home computers in the living room, and about 30% have online access in the privacy of their bedrooms.

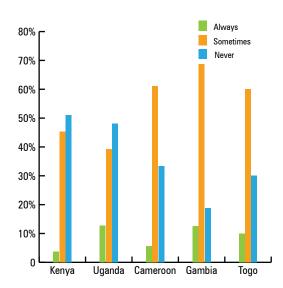
All over the world, many parents make the wrong assumption that their child is "safe" at home using their computer as opposed to being exposed to the dangers on the streets. This is incorrect, as having online access increasingly connects children with all sorts of people, information and influences. A number of families have chosen to keep the computers in the living room to better



monitor what their children do online, and to deter unsafe practices. When a computer is located in a house's living room, the chances of a child being contacted by abusers, accessing online pornography, or producing compromising images of him/herself are greatly reduced. However this might give parents a false sense of security, as children may behave in a safe manner at home but engage in vulnerable practices outside, such as in public cafés.

When you use the Internet at home is an adult always with you to see what websites you visit?

On average, 40% of all the children surveyed – from every age group, both boys and girls - are never supervised by their parents. Between 30% and 55% are "sometimes" supervised. Among the girls researched, between 40% and 67% are never supervised by an adult regarding the websites they visit. These are significantly large figures. Also, none of the 17-18 year old boys from any of the countries said that their parents were interested in verifying the websites they visit or taking time to explore such sites together.



Parental supervision is not simply monitoring the child's online activities: it can take the form of enjoying certain online activities together such as interactions through social networks and games, providing guidance regarding their safe use, helping children to be aware of risky behaviours and situations, and encouraging safe use of ICTs. In these situations it is much easier to get children to take note of advice such as refraining from disclosing personal information when going online, exercising caution when making friends in chat rooms and refraining from accessing adult material.

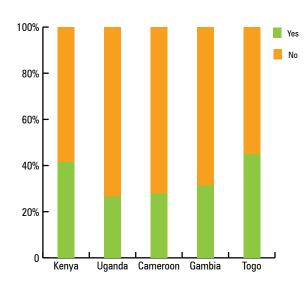
➡ Have you ever received any guidelines from your parents about how to use computers or the Internet at home?

On average, only 50% of each age group said that they received some kind of advice from their parents, especially those aged between 11 and 16. Around 30% said that they have never received any kind of guidance from their parents. This may indicate that a significant percentage of parents are not familiar with the risks posed by the Internet. Close to 10% do not consider their parents suitable to provide guidance. It is interesting to note that boys and girls of each age group were fairly consistent with their responses.

	MALE			FEMALE		
Age between	11-13	14-16	17-18	11-13	14-16	17-18
Yes	20.59%	10.45%	0.00%	6.90%	4.69%	2.44%
No	41.18%	55.22%	51.43%	51.72%	46.88%	31.71%
They don't know about computers	38.24%	34.33%	48.57%	41.38%	48.44%	65.85%
I don't see the need						

⇒ Have your parents ever asked you not to be on the Internet or use any of the online applications?

Absence of parental guidance is also noted here. When it comes to limiting access to the Internet and online applications, parents exhibit different attitude towards their children as they grow up. Not surprisingly, the 17-18 year old males are the least asked to restrain from their online activities; also with the girls the percentage is higher for younger ones and goes down as they get older. Parents seem to expect their children to be better able to deal with such matters as they grow older, which is not always true, as children need different types of guidance according to their age. Parents may also not want to confront their children as they get older because they are not familiar with various aspects of online interactions and do not wish to show ignorance to their more technically mature children.

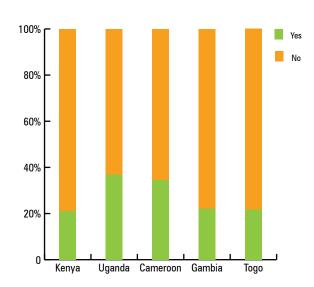


7.4 SCHOOL SETTING AND GUIDANCE FROM TEACHERS

QUESTIONS TO TEACHERS

Do you know how to install a content filter?

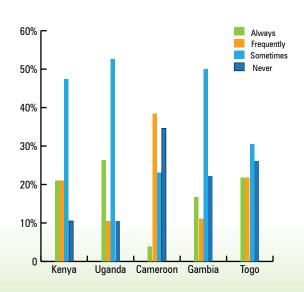
The fact that schools do not appear to have filtering systems installed indicates that children may be able to access whatever content they wish when using computers at schools - a major breach in online safety within the schools system. Furthermore, for teachers to offer preventive solutions and suitable education to children to combat online risks, it is essential that they are technically knowledgeable. In general, the teachers who took part in this research consider themselves average users of such tools and applications.



With the range of tools that children and young people use to access the online world, having filtering mechanisms on all services can be a challenge. Moreover it is very difficult to monitor the type of content they are accessing, the contacts they are making online and also information they are sharing about themselves - using their mobile phones, outside home, at school or in cybercafés. It is thus very important to, instead of just making it harder for children to engage in certain practices, develop a well designed set of guidelines to educate them about the potential harms, while building the capacity of relevant adults to effectively engage with them for that purpose.

Do you suggest the issue of Internet safety to your students?

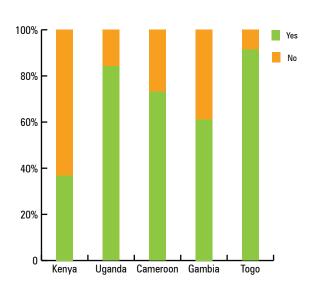
There is a significant variation between the countries examined when it comes to discussing Internet safety in schools. One element is surprising: the low percentage of school teachers in Kenya who provide guidance to children on online safety in schools, considering that Kenya is the most advanced among these countries in terms of ICT penetration. The lack of consistency in discussing Internet safety issues may point to the fact that, even if teachers are aware of certain risks online, they do not know how to provide guidance.



In Africa, as most households do not have computers or Internet access, children access the Internet at school, or at cybercafés. It is therefore essential that teachers increase their knowledge of ICT in order to take appropriate preventive measures to ensure online safety. Such strategies need to be incorporated into the mainstream school system. For example, through adopting a curriculum that addresses the various risks a child might face whilst online; passing on the right information to the child in a timely fashion before the child engages in risky behaviour (while avoiding "scare techniques"); monitoring Internet use by students; making use of filters to block inappropriate content and encouraging open discussions amongst children — It should be noted that greater harm than good may be caused if, due to negligence or incompetence, wrong messages are provided by teachers, causing students to develop a fear of exploring online technologies, which would deprive them of tools that can play and important role in advancing in their learning. Simply suppressing the use of mobile phones in schools, for instance, is counterproductive and may actually impede the establishment of child safe environment.

Do you provide guidance on Internet use?

Kenya also displays the lowest rate of guidance on Internet use provided by teachers. The Kenyan educational system appears to lack the policies and standards of other governmental departments. Schools in Togo, Uganda and Cameroon are more advanced in this regard.



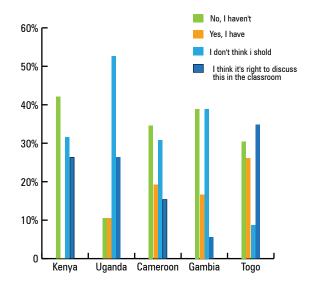
If yes, then on what topics?

Guidance on safe practices was not mentioned by most teachers — by 28% on average, with the higher rates for Togo (38%) and The Gambia (36%). Reporting illegal content was also a major concern in Togo (42%). Providing guidance on the ethical use of the Internet was second most commonly reported, except in Uganda and Togo. A major topic of concern was the authenticity of information.

	Kenya	Uganda	Cameroon	Gambia	Togo
i) Validity of sources	14.29%	31.25%	10.53%	27.27%	23.81%
ii) Reporting illegal content	28.57%	18.75%	5.26%	18.18%	42.86%
iii) Authenticity of the information	57.14%	6.25%	63.16%	36.36%	38.10%
iv) Discerning content for adults	28.57%	25.00%	10.53%	9.09%	28.57%
v) Organizing information	28.57%	12.50%	21.05%	18.18%	28.57%
vi) Safe practices	28.57%	31.25%	10.53%	36.36%	38.10%
vii) Safe use of social networks	28.57%	0.00%	10.53%	27.27%	23.81%
viii) Ethical use	42.86%	18.75%	42.11%	18.18%	33.33%

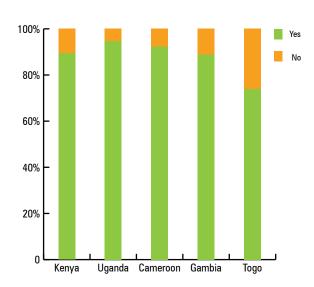
Have you talked about online pornography (involving adults and children) with your students?

Teachers in most countries refrain from talking about online pornography with their students, except for those in Uganda, where half of them have discussed the subject in class, followed by The Gambia with nearly 39% addressing these issue. About 15% do not think that it is appropriate to do so — with higher rates for Togo (26%) and Cameroon (19%). It would have been useful to find out whether their responses would have varied depending on the students age groups, but the general feeling is that such things would be better kept secret.



In order to tackle online risks, including the more challenging and contentious ones such as pornography, it is usually more effective to promote discussions and debates rather than keep these issues secret. Openly exchanging opinions is a good starting point to explain to children why certain contents and practices are inappropriate. Also, children should not be made to feel guilty if they stumble accross inappropriate content. They should be encouraged to discuss their experiences, should they wish to do so.

Do you think children are at risk when they interact online with strangers?



If you think there are dangers, which ones do you think are the most risky situations for a child or teenager?

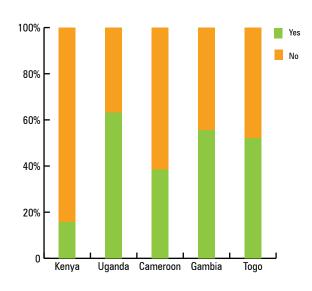
Posting photos that are revealing or without clothes (45%) and accepting strangers in chat (nearly 37%) are considered the most dangerous situations for children online. Teachers in Togo showed concern about most of the situations described, which suggests awareness of the array of online risks. Surprisingly though, none of the teachers in Uganda felt that there could be risks posed by chat forums and none of the teachers in Cameroon felt that there could be risks for children if they accept to meet strangers in real life. Teachers' responses about the possible risks to children through the use of mobile phones indicate limited awareness, as they worry primarily about avoiding distractions in class.

	Kenya	Uganda	Cameroon	Gambia	Togo
i) Use chat programs	23.53%	11.11%	33.33%	18.75%	11.76%
ii) Use social networks	29.41%	27.78%	4.17%	31.25%	29.41%
iii) Have email with identifiable name and last name	5.88%	11.11%	8.33%	6.25%	47.06%
iv) Chat in forums	11.76%	0.00%	12.50%	12.50%	11.76%
v) Accept strangers in chat	23.53%	22.22%	45.83%	43.75%	47.06%
vi) Play online with strangers	11.76%	5.56%	37.50%	31.25%	41.18%
vii) Post photos that are revealing or without clothes	35.29%	33.33%	54.17%	50.00%	52.94%
viii) Publish personal information	41.18%	22.22%	25.00%	18.75%	52.94%
ix) Establish linkages with strangers	35.29%	5.56%	54.17%	18.75%	47.06%
x) Accept to meet up with strangers in real life	76.47%	44.44%	0.00%	50.00%	11.76%

It is fundamental that teachers receive training on the various ways of using ICTs that might negatively affect children (such as 'sexting' i.e. sending sexualised photos of oneself to friends through messaging devices, contacting strangers through chat or social networks etc.), so that they can utilise this learning to better prevent and manage with risky situations.

Have you worked on prevention strategies with your students for safe online interaction?

Most teachers have not worked on prevention strategies, which confirms the answers to a previous question in which guidance on safe practices was not mentioned by most teachers. This is particularly the case in Kenya, and highlights the need to target this country in prevention / protection programming especially in view of its high ICT development.



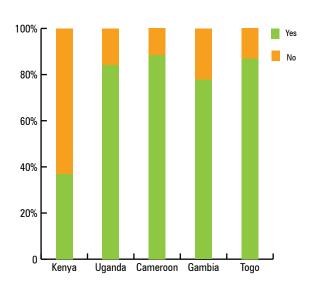
⇒ If you did, what type of self-protection strategies did you teach them?

The understanding about online vulnerabilities varies across teachers/countries. The study suggest teachers are not fully aware of the complete range of potentially risky behaviours, as they are selective as to the self-protection strategies they provide and do not address them all.

	Kenya	Uganda	Cameroon	Gambia	Togo
i) Use chat programs	23.53%	11.11%	33.33%	18.75%	11.76%
ii) Use social networks	29.41%	27.78%	4.17%	31.25%	29.41%
iii) Have email with identifiable name and last name	5.88%	11.11%	8.33%	6.25%	47.06%
iv) Chat in forums	11.76%	0.00%	12.50%	12.50%	11.76%
v) Accept strangers in chat	23.53%	22.22%	45.83%	43.75%	47.06%
vi) Play online with strangers	11.76%	5.56%	37.50%	31.25%	41.18%
vii) Post photos that are revealing or without clothes	35.29%	33.33%	54.17%	50.00%	52.94%
viii) Publish personal information	41.18%	22.22%	25.00%	18.75%	52.94%
ix) Establish linkages with strangers	35.29%	5.56%	54.17%	18.75%	47.06%
x) Accept to meet up with strangers in real life	76.47%	44.44%	0.00%	50.00%	11.76%

Do you discuss with your students about ethical use of Internet and mobile phones?

Kenya also displays the lowest rates with regard to guidance on ethical use of the Internet and mobile phones.



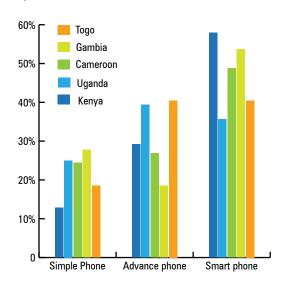
With the use of technologies children have become more...... choose up to three options.

All teachers in Kenya felt that children are prone to risky behavior online as opposed to only 30.43% in Togo – This contradicts the earlier finding regarding the extent to which they provide Internet safety instructions to students. The positive aspect of their becoming more communicative (58%) goes hand in hand with the negative aspect of being prone to risky behaviour (54%) – the two options that scored highest.

	Kenya	Uganda	Cameroon	Gambia	Togo
i) Communicative	36.84%	57.89%	57.69%	77.78%	60.87%
ii) Reserved	0.00%	10.53%	7.69%	11.11%	21.74%
iii) Idle	15.79%	10.53%	30.77%	55.56%	56.52%
iv) Active	21.05%	26.32%	34.62%	27.78%	43.48%
v) Violent	47.37%	21.05%	11.54%	16.67%	43.48%
vi) Quiet	10.53%	0.00%	15.38%	0.00%	0.00%
vii) Prone to risky behaviour	100.00%	52.63%	38.46%	61.11%	30.43%
viii) Confident	31.58%	42.11%	7.69%	22.22%	0.00%
ix) Outgoing	21.05%	21.05%	50.00%	11.11%	26.09%

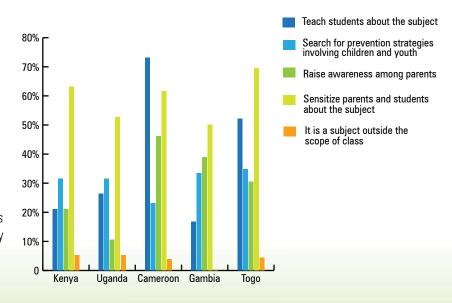
Do you know of any cases of grooming or sexual exploitation online?

Teachers in all countries had heard rumors about the occurrence of online sexual exploitation of children — and about 10% to 15% in Cameroon, The Gambia and Togo reported "several cases".



What role should the school play regarding the dangers associated to the use of new technologies?

The majority of the teachers in the countries surveyed do not agree with the need to develop prevention strategies in schools. In general, it seems that educating parents would be the preferred way in which schools can contribute to ensuring child safety online.

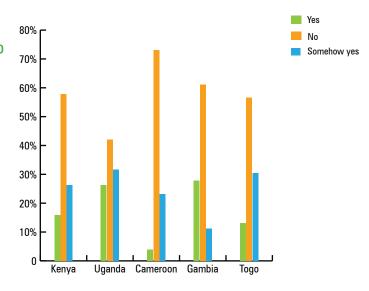


What do teachers need to learn about how to better use new technologies?

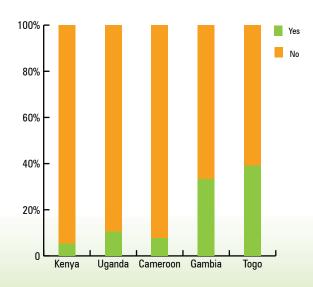
The teachers in Uganda, The Gambia and Togo gave a lower priority to receiving training on safe use of ICTs, in comparison to the other options.

	Kenya	Uganda	Cameroon	Gambia	Togo
i) Capacity building about technology	15.79%	47.37%	46.15%	27.78%	39.13%
ii) Capacity building about educational strategies using ICT	21.05%	42.11%	53.85%	38.89%	56.52%
iii) Time to surf the net	0.00%	5.26%	11.54%	0.00%	21.74%
iv) Capacity building on safe use of ICT	89.47%	31.58%	42.31%	33.33%	26.09%
v) Better access to ICTs at school	0.00%	21.05%	46.15%	5.56%	30.43%
vi) Better access to ICTs at home	10.53%	5.26%	38.46%	16.67%	26.09%

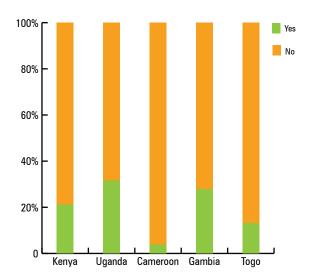
Does the school provide you with information and guidelines on how to protect children online?



Does your school have a referral mechanism for reporting cases of online sexual exploitation?

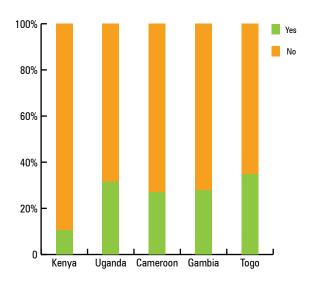


Does the school have clear policies on Internet safety that are codified and distributed?



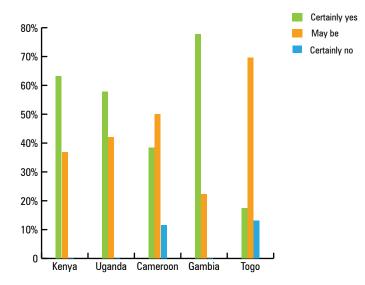
Does the school provide unrestricted Internet access to children and teachers - such as access to social networks, YouTube, file download services or web browsing of any site?

There is a clear lack of prioritization, within the school environment, to develop an online safety curriculum and implement measures to protect children while they use ICTs. Given the growing use of ICTs, particularly in Kenya, it would be expected that the adequate protection infrastructure would follow in schools, but that is not yet the case. Cameroon in particular scored very low, and also shows a high percentage of unrestricted Internet access.



Which standards should be used when it comes to developing curriculum and materials on online safety for children? The 'Western' countries favor a more liberal approach when discussing certain issues, which is considered inappropriate from the cultural standpoints of various other regions. The Internet is a global connectivity medium. It bridges cultural gaps and allows different communities and generations to communicated. Hence adapting a uniform model can be challenging and demands specific strategies. One particular approach involves drawing attention to certain commonalities that do transcend borders. Perceptions regarding sexuality vary across cultures, but the harm to children who disseminate intimate images of themselves or fall prey to abusive situations, are more or less universal.

⇒ Do you think having written policies would make it easier for the teacher to implement safety standards?



There are mixed feelings regarding the usefulness of having written policies governing the implementation of safety standards, with Kenya, Uganda and The Gambia being more open to it. These percentages coincide more or less with the relatively low importance teachers placed on receiving capacity building on safe use of ICT, and regarding the role of the school should play in using new technologies. Overall, most teachers do not consider guidance and policies on online safety to be a priority.

8. RECOMMENDATIONS FOR ACTION

- It is important to empower children in the online space, encouraging digital citizenship through carefully crafted programmes that acknowledge their cultural background and at the same time create mechanisms to assist those who might suffer harm online.
- Online abuse does not affect all children equally. Awareness raising materials must target the appropriate age and gender demographic, making them attractive and meaningful to their experiences online, acknowledging and respecting their motivations. These must be developed in a consultative manner that involves children and young people.
- Peer monitoring schemes needs to be developed, as children seek support from their peers when facing problems with ICTs.
- Help lines and reporting mechanisms for cases of online sexual exploitation need to be strengthened and there needs to be capacity building amongst relavent stakeholders.
- Children must be educated about the potentially harmful effects of certain actions when using ICTs. Certain actions in the virtual world can be as damaging as those in the real one.
- Children must be taught how to stop actions that may lead to uncomfortable and dangerous situations such as "grooming" i.e. having a stranger asking questions of a sexual nature so as to slowly break their resistance and finally obtain sexualised images of child or solicit sexual services.
- Parents need to improve their digital literacy and participating online activities with children to better assess and prevent possible harms.
- Cybercafés are, by far, the location where children in the researched African countries most frequently access the Internet. Codes of conduct must be developed and adopted to ensure child safety policies and practices are established and implemented within these venues.
- Detter mechanisms need to be in place regarding the rules and operations of cybercafés, in line with national ICT policies. It is important that the cybercafés in Africa follow a standard set of practices under close supervision of the authorities, so that their services can be made safer for children.
- The involvement of the private sector in promoting Internet safety is quite limited amongst the surveyed countries. Entities such as the ISPs, software companies, online service providers, social networks, mobile phone providers etc. must be increasingly involved in raising public awareness on child online safety. This includes developing appropriate resources and guidelines to help parents and children understand the risks posed and creating clear policies on the use of their services. Technical solutions on preventing exposure to inappropriate content must be disseminated.

- The use of social networks is also spreading to mobile phones. Both the mobile phone operators and the social network providers should develop tools and resource materials to train and educate children, about the risk and the use of privacy settings.
- Teachers must receive training on the various ways of using ICTs that might negatively affect children. Educational authorities must also develop online safety policies with measures such as setting up reporting mechanisms, introducing the topic of ICTs related child safety in the school curriculum, organising awareness raising events and installing filtering devices in the school computers etc.
- It is important to highlight the importance of providing opportunities to children through the using evolving ICT tools and technologies, and not to presume that all risks will lead to harm. Limiting the positive opportunities as a means of addressing/eradicating the risks is counter-productive.

9. LEGAL FRAMEWORK

In general, countries in Africa focus their efforts in combating child prostitution and child trafficking, and only a few have developed adequate legal and policy frameworks to combat child pornography and other manifestations of CSEC related to the use ofnew technologies. In addition, cases of child pornography are barely reported due to various reasons, which makes it more difficult to address the problem and develop specific prevention and protection measures.

This section focusing on the legal and regulatory framework will give an idea of the correlation between the legal standards present in the countries and some of the practices that was demonstrated in the earlier sections. For example a lack of legislation around grooming of children for sexual purposes or even downloading and possession of child abuse materials in a certain country might be factors that encourages or influences such behavior and lack of awareness of the criminal aspect of such acts may be demonstrated in the case of survey responses. The analysis of the legal framework may give the reader a closer inspection of certain traits and practices within the internet industry as well as how such gaps can relate to the situations that the children in these countries might be exposed to such as exposing themselves in compromised state on web cams, that are increasingly featuring in both home computers and in public cyber cafes.

Legislation must evolve as society changes: child abusers are already taking advantage of the new opportunities offered by the rapid evolution of information and communication technologies (ICTs). Therefore, governments must adapt their legislation and policies to address the use of ICTs in producing, accessing and viewing, possessing (including for one's private use) and disseminating child pornography as well as forms of sexual exploitation of children online, such as grooming (solicitation of children for sexual purposes), as defined and criminalized in recent legal standards addressing CSEC developed by the Council of Europe¹¹ and the European Union. The harmonisation of laws across different legal systems around the world and their effective enforcement are essential, otherwise some countries will be targeted by child sex offenders as "safe havens".

In view of the increasing incidence of CSEC - and in an effort to promote the harmonisation of laws addressing CSEC across countries - the international community has sought to enhance the related legal framework through, for example, the Optional Protocol on the sale of children, child prostitution and child pornography, adopted by the UN General Assembly in May 2000 and which entered into force in January 2002. The Optional Protocol extended the protection set in Art. 34 of the Convention on the Rights of the Child, by acknowledging and defining specific offences such as child pornography, child prostitution and the sale of children, and criminalising related activities. The countries that ratified these treaties are legally bound to reform their national legal framework and policies accordingly, besides having to report periodically to the Committee on the Rights of the Child, which monitors the implementation of the Optional Protocol. Until today, the Optional Protocol has been ratified by 163 countries.

At regional level, the Organisation of African Unity (replaced by the African Union since 2001), adopted in 1990 the *African Charter on the Rights and Welfare of the Child*. This regional legal standard, entered into force in 1999. Article 27 of the African Charter criminalizes child prostitution and child pornography and Article 29 prohibits the sale of children and child trafficking for any purpose, which includes sexual purposes. The implementation of the African Charter by State Parties is monitored by the African Committee of Experts on the Rights and Welfare of the Child. The African Charter has been ratified by 45 out of the 53 African States.

^{11.} Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007)

DIRECTIVE 2011/92/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA

Office of the United Nations High Commissioner for Human Rights. Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. Accessed on the 27th March 2012 from: http://www2.ohchr.org/english/law/crc-sale.htm

Article 2c of the *Optional Protocol* defines child pornography as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes". The criminalised activities are mentioned in Article 3c, and include producing, distributing, disseminating, importing, exporting, offering, selling or possessing child pornography.¹⁴

The States under review in this study have all ratified the *Convention on the Rights of the Child* without making any declarations or reservations as well as the African Charter on the Rights and Welfare of the Child. Nevertheless, this is not the case with regard to the Optional Protocol: as of January 2013, Kenya and Cameroon have not yet ratified the Protocol, ¹⁵ which constitutes a serious legal gap in their efforts to combat related crimes against children. In spite of not having ratified the Optional Protocol, both countries still have an obligation under Article 34 of the CRC ¹⁶ to undertake all measures possible to protect children from all forms of sexual exploitation and sexual abuse.

9.1 NATIONAL LEGAL FRAMEWORKS



CAMEROON

CHILD PORNOGRAPHY

Definition

Cameroon has adopted the *Law No. 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality*, which addresses child pornography and child sexual exploitation through the use of information and communication technologies .

Section 81.2 defines child pornography as any act visually available which represents a minor engaged in sexually explicit activity, any person with the physical features of a minor involved in sexually explicit acts; activities or real images representing a minor engaged in sexual activities. This definition is not compliant with the Optional Protocol as it does not cover simulated explicit sexual acts nor the representation of the sexual parts of a child. In addition, to be in line with Article 2.c of the OPSC, the Law relating to cybercriminality and cybersecurity

Office of the United Nations High Commissioner for Human Rights. Article 2 and 3 of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. Accessed on the 28th March 2012 from: http://www2.ohchr.org/english/law/crc-sale.htm

^{15.} United Nations Treaty Collection. Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, 11c. Accessed on the 28th March 2012 from: http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11-c&chapter=4&lang=en

Office of the United Nations High Commissioner for Human Rights. Convention on the Rights of the Child, Article 34. Accessed on the 28th March 2012 from: http://www2.ohchr.org/english/law/crc.htm

should also prohibit audio and written materials representing children engaged in sexual activity. Furthermore, the definition does not include virtual child pornography (cartoons, anime, drawings, computer generated images, etc. depicting children engaged in sexual activity) as it refers to real images of children engaged in sexual activity.

The Penal Code does not include provisions on child pornography, although Article 265 sanctions "obscene representations", which is too vague to penalise all forms of child pornography.

Prohibited acts relating to child pornography

Under Section 81.1 of the law *relating to cybersecurity and cybercriminality*, offering, producing, providing child pornography for publication as well as acquiring child pornography for oneself or for someone else using an information system; should be prohibited. Even though it appears that only importing and exporting of child pornography are not covered by Section 81.1, the law does not provide clear penalties for each of the above mentioned offenses. In addition, such acts are only punished if committed through the use of an information system.

Section 76 stipulates that an individual who uses electronic communications or an information system to design, carry or publish a child pornography message, can be sentenced to five to ten years of imprisonment and/or a fine of five to ten million CFA francs.

In addition, Section 80.1of the same law penalises "whoever for consideration or free of charge, uses electronic communications or an information system to publish, attach, with a fine of five to ten million CFA francs, and/ or imprisonment of one to five years", record or transmit an image showing acts of pedophilia. According to Section 80.2, the same penalties apply to those who uses whatsoever electronic means to offer, provide or publish, import or export an image or picture portraying pedophilia. Those penalties also apply to those who keep an image or picture portraying pedophilia in an electronic communication network or an information system (Section 80.3).

The reference to the term "pedophilia" in Sections 80.1; 80.2 and 80.3, which is not defined in the law, is confusing and misleading. Section 80.5 stipulates that above mentioned provisions equally apply to "pornographic pictures showing minors", which entails that acts relating to child pornography and images portraying pedophilia would be distinct offenses under this law. However, differences between those offenses is not clear due to the lack of definition of the term "pedophilia". Legal clarification is needed.

SEXUAL EXPLOITATION OF CHILDREN THROUGH THE USE OF ICTs

Regarding the sexual exploitation of children through the use of ICTs, Section 81.1 prohibits sexual proposals made by adults to minors under 15 through the use of an electronic communication network or an information system. The protection of children under 15 against solicitation for sexual purposes (grooming) is too limiting as it does not cover those upto 18 years of age and it does not provide any penalties for such an offense.

Section 83 criminalises the solicitation of a person for sexual purposes (grooming)by stipulating that a person who, by electronic means, makes sexual proposals to a person of the same sex can be sentenced to one to two years and/or a fine of 500.000 to one million CFA francs.¹⁷ Those penalties can be doubled if sexual proposals are followed by sexual intercourse (Section 83.2). It is of concern that this provision only applies when the proposal is made to a person of the same sex. Further protection is needed to ensure that this provision covers also the solicitation of children, for sexual purposes, irrespective of gender.

^{17.} Republic of Cameroon, Law No. 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon

CHILD PORNOGRAPHY

Definition

The *Children's Act* 2005 do not provide for a definition of child pornography which is a major gap that should be addressed as a priority. The Tourism Offense Act 2003 refers to child pornography as the taking, distribution or publication of indecent pictures of children, which is not consistent with the definition of child pornography contained in Article 2. Of the OPSC, especially as the term "indecent" is very broad and open to subjective interpretations by law enforcers

Prohibited acts relating to child pornography

In 2005, the Gambia adopted the *Children's Act*, which contains various provisions addressing CSEC, and specifically against child pornography. Section 31(1) (a) of the Children's Act prohibits "the use, procuring or offering of a child for prostitution, for the production of pornography and for pornographic performances".

Section 60 of the *Children's Act* prohibits the import, printing, publication, and sale of harmful publications, defined as "any book, magazine, film, picture, video or audiotape, print or other medium which is targeted at or likely to fall into the hands of a child and which contains pictures or stories that portray harmful information such as: (a) the commission of crimes; (b) acts of violence or cruelty; (c) incidents of a repulsive or horrible nature; (d) acts or words of an immoral character; or (e) obscene and indecent representation, in such a way that the work as a whole would tend to corrupt or deprave the child into whose hands it may fall". 18

The *Tourism Offences Act* (2003) also aims to protect children against child pornography and other forms of exploitation within the context of tourism. Section 8 of the *Tourism Offences Act* stipulates that "a tourist or any other person who engages in child pornography – the taking, distribution or publication of indecent pictures of children – can be imprisoned for five years".¹⁹ A person is regarded as distributing an indecent photograph if he/she gives up, exposes or offers it for acquisition to another person. Under this Act it is also prohibited to show pornographic pictures to a child, to make a child pose or perform for pornographic pictures or videos and to take indecent photographs of a child.²⁰

Even thought the terms used in the *Tourism Offences Act* (2003) to define acts relating to child pornography that are prohibited, are not exactly similar to the one used in Article 2.c of the OPSC, it appears that producing, distributing, disseminating, offering and selling of child pornography are prohibited by Gambian law. However, importing, exporting and possessing are not criminalized yet.

ECPAT International. Gambia: Global Monitoring Report on the status of action against commercial sexual exploitation of children. p.23. 2007. Accessed on the 4th March 2012 from: http://www.ecpat.net/A4A_2005/PDF/AF/Global_Monitoring_Report-GAMBIA.pdf

^{19.} Child Protection Alliance. Tourism Offences Act 2003. Accessed on the 4th March 2012 from: http://www.cpagambia.gm/Web/Leaflet%20Tourism%20Offences%20Act.pdf

ECPAT International. Gambia: Global Monitoring Report on the status of action against commercial sexual exploitation of children. p.23-24. 2007. Accessed on the 4th March 2012 from: http://www.ecpat.net/A4A_2005/PDF/AF/Global_ Monitoring_Report-GAMBIA.pdf

SEXUAL EXPLOITATION OF CHILDREN THROUGH THE USE OF ICTs

Gambian legislation fails to address forms of sexual exploitation of children through the use of ICT, especially sexual solicitations of children through the use of ICTs (grooming), as defined in Article 23 of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

Addressing this legal gap should be considered as a priority.



KENYA

CHILD PORNOGRAPHY

Definition

Neither the *Children Act* (2001) nor the *Sexual offense Act* (2006) contain any definition of child pornography. Section 16(1) of the *Sexual Offense Act* (2006) only refers to "obscene book, pamphlet,paper,drawing, painting, art, representation or figure or any other obscene object whatsoever which depict the image of any child". Under Section 16(3), such materials are deemed to be obscene if they are lascivious or appeals to the prurient interest or if its effect, or where it comprises two or more distinct items the effect of any one of its items, if taken as a whole, tends to deprave and corrupt persons likely to see or read them. Referring to "obscenity" to define child pornography is a major drawback as this term is very broad and open to many interpretations and not at all in line with Article 2 of the OPSC. Addressing this legal loophole should be considered as a priority in terms of legal reform.

Prohibited acts relating to child pornography

Section 16(1) of the *Sexual Offences Act* declares that "anyone, including juristic persons, who sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces, imports, exports or has in his or her possession any obscene book, pamphlet, paper, drawing, painting, art, representation or figure or any other obscene object whatsoever which depict the image of any child will be charged and sentenced to a term of not less than six years' imprisonment and/or to a fine of not less than 500.000 shillings". Additionally, a person may be convicted on related charges if he/she "advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be produced from or through any person; or offers or attempts to do any act which is an offence under this section".

Regarding prohibited acts relating to child pornography, Section 16 of the Sexual Offense Act is very comprehensive and fully compliant with Article 2.c of the OPSC even though the term "child pornography" is not adequately defined yet. It goes even beyond the scope of the OPSC by prohibiting the possession of child pornography even if not for the purpose of distribution and by specifically stipulating that companies (juristic persons), involved in producing, distributing, selling, etc. child pornography can be prosecuted.

SEXUAL EXPLOITATION OF CHILDREN THROUGH THE USE OF ICTs

Kenyan legislation fails to address forms of sexual exploitation of children through the use of ICT, especially sexual solicitations of children through the use of ICTs (grooming), as defined in Article 23 of the *Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*. Addressing this legal gap should be considered as a priority.



TOGO

CHILD PORNOGRAPHY

Definition

Article 392 of the *Children's Code* defines child pornography as "a representation, by whatever mean, of a child engaged in real or simulated sexual activities or any representation of a child sexual organs". "Child pornography" is punished with five to ten years of imprisonment.²¹ This definition of child pornography fully complies with Article 2.c of the *Optional Protocol*.

Prohibited acts relating to child pornography

The *Children's Act* criminalizes child pornography with penalties between 5 to 10 years. However, none of the acts relating to child pornography, as stipulated in Article 2.c of the OPSC (producing, distributing, disseminating, importing, exporting, offering, selling or possessing child pornography), are prohibited. Mere possession of child pornography should be prohibited. This constitutes a major legal gap which should be prioritized.

Even though the terms used in the *Tourism Offences Act* (2003) to define acts relating to child pornography that are prohibited, are not exactly similar to the one used in Article 2.c of the OPSC, it appears that producing, distributing, disseminating, offering and selling of child pornography are prohibited by Gambian law. However, importing, exporting and possessing are not criminalized yet.

SEXUAL EXPLOITATION OF CHILDREN THROUGH THE USE OF ICTs

Togolese legislation fails to address forms of sexual exploitation of children through the use of ICT, especially sexual solicitations of children through the use of ICTs (grooming), as defined in Article 23 of the *Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*. Addressing this legal gap should be considered as a priority.

^{21.} Journal officielle de la République togolaise, Loi portant code de l'enfant, 6 juillet 2007, accessed on the 4th March 2012 from: http://www.hsph.harvard.edu/population/fgm/togo.child.07.pdf



UGANDA

CHILD PORNOGRAPHY

Definition

According to Section 23(3) of the *Computer Misuse Act* 2011 "child pornography" includes pornographic material that depicts a child engaged in sexually suggestive or explicit conduct; a person appearing to be a child engaged in sexually suggestive or explicit conduct; or realistic images representing children engaged in sexually suggestive or explicit conduct. This definition is not fully in line with Article 2.c of the OPSC as it does not prohibit materials depicting the sexual parts of a child for sexual purposes. In addition, it does not prohibit virtual child pornography (cartoons, anime, drawings, computer generated images, etc. depicting children engaged in sexual activity) as it refers to realistic images of children engaged in sexual activity.

Prohibited acts relating to child pornography

Section 23(1) prohibits the production of child pornography for the purposes of its distribution through a computer, offering or making available child pornography through a computer, distributing or transmitting child pornography through a computer for himself or herself or another person; or unlawful possession of child pornography on a computer, Those who committed such offenses are liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

Even though mere possession of child pornography is prohibited and only importing and exporting child pornography are not included in Section 23(1), the above mentioned acts are prohibited only if they have been committed through the use of a computer, which substantially limits the scope of this provision. For example, the distribution of child pornography though publications is not covered by Section 23(1) or any other device, such as a mobile phone for example.

Section 166 of the Penal Code criminalises the traffic of obscene publications. The act of making, producing, convey, exporting, importing, putting in circulation or possessing any obscene writings, drawings, prints, paintings, printed matter, pictures, posters, emblems, photographs, cinematograph films or any other obscene objects, or any other object tending to corrupt morals will be punished with two years of imprisonment or a fine of 2.000 shillings.

However, these activities are only punishable if made for the purpose of trade, distribution or public exhibition. Moreover, the term "obscene representation" is vague, which does not provide enough protection to children.

SEXUAL EXPLOITATION OF CHILDREN THROUGH THE USE OF ICTs

The Ugandan law does not contain specific provisions addressing child grooming. The only provision in the *Computer Misuse Act* which could potentially address sexual exploitation and abuse through the use of ICTs is to be found in Section 24 addressing Cyber harassment. Section Section 24(2)(a) criminalises the use of a computer for making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent. According to Section 24(1), A person who commits cyber harassment is liable on conviction to a fine not exceeding seventy two currency points or imprisonment not exceeding three years or both.

However, the use of terms such as "obscene" and "indecent", which are very broad and vague and open to various interpretations, weaken the provision.

.

Since 2006, the International Center for Missing and Exploited Children (ICMEC) releases yearly reviews on legal improvements related to child pornography. The 2010 edition, the latest to date, assessed the situation in more than 190 countries around the world, including 52 African countries. Forty-nine countries in Africa fail to criminalise the mere possession of child pornography, while another 49 fail to define child pornography. Moreover, 44 countries have no laws criminalising computer-facilitated offences. South Africa is the only country in the continent where Internet Service Providers (ISP) are mandated to report child pornography material.²²

9.2 REGULATIONS FOR PRIVATE SECTOR STAKEHOLDERS

An effective repression of child pornography cannot take place without the involvement of key private sector stakeholders such as Internet Service Providers (ISPs), social networks, cybercafés, financial services companies, among others. The collaboration of these actors can either be regulated by the law or take place on a voluntary basis.

Because of their direct access to what is transiting on the network and the Internet, ISPs and cybercafés as well as social networks are very well positioned to stop the propagation of incidences of child pornography. Their engagement may take place in various ways, filtering and blocking access to websites being the most commonly used mechanism along with taking down of such content if it is in their jurisdiction. Additionally, the reporting of illegal content is mandatory in many jurisdictions, and failure to report can lead to prosecution and conviction.

Indeed, law enforcement and ISPs often work hand in hand to prevent users from having access to child pornography. For example, ISPs may block a list of illegal websites provided by police forces. If illegal material is found, notice will be given to the police for them to take measures accordingly. There is also the "notice and take down procedure", which involves reporting an illegal content to a tip line or directly to law enforcement authorities. Law enforcement then contacts the Internet hosting provider, which will either block access to the site or remove the harmful content.²³

^{22.} Gamuchirai Tagwireyi. Comprehensive Legal Approaches to Combat Child Pornography: An International and Regional Perspective. 2011. Accessed on the 10th April 2012 from: http://www.commonwealthigf.org/wp-content/up-loads/2011/03/ICIA-Conference-Paper-ICMEC-FINAL.pdf

^{23.} Catherine Beaulieu, ECPAT International. Strengthening Laws Addressing Child Sexual Exploitation – A Practical Guide. p. 91-92. 2008.

So far, the financial sector has been spared from the legal obligation to report child pornography related transactions and thus play a part in stopping the commercial production and dissemination of child pornography. There are nevertheless some praiseworthy initiatives coming from financial institutions that voluntarily undertook to support the fight against child abuse materials. The Financial Coalition against Child Pornography (FCACP) is an example: it aims to eradicate the commercial viability of child pornography by following the flow of funds and shutting down the accounts used by these illegal enterprises. Founded in 2006 by the International Center for Missing and Exploited Children and its sister organisation the National Center for Missing and Exploited Children in the United States of America, the FCACP collaborates actively with financial institutes such as credit card and payment processing companies and national and international law enforcement agencies to enable the criminal prosecution of child pornography users. Their competencies allow them to follow the money flow and interfere in the financial transactions by denying criminals the use of a legitimate international financial system. The FCACP has also been operational in the East Asia Pacific region, based out of Singapore, working with the financial sector, law enforcement, technology companies and NGOs.

Since the Internet is not confined to national boundaries, international cooperation, harmonized legislation and industry accountability are indeed essential.

Mandatory reporting of child pornography or blocking of websites is rarely regulated in Africa. Except for South Africa, no African country has imposed upon ISPs or IHPs the obligation to report harmful content. Some initiatives to this end are however emerging from civil society movements, such as in Togo, where the NGO WAO-Afrique, in collaboration with ECPAT International, launched the campaign "Make IT Safe". This campaign aims to protect children in their use of the Internet, in particular against sexual exploitation; its activities include the development of a code of conduct for cybercafés, which has been signed by different cafés around the country. Even so, the Forum of Child's Rights, a Togolese organisation, pointed out the absence of regulations and general control of cybercafés with a view to preventing access of child pornography and other illegal and harmful content by children. The Togo Government has acknowledged that the administrative structure in charge of controlling access to harmful content by children, including child pornography, is inefficient.

^{24.} Catherine Beaulieu, ECPAT International. Strengthening Laws Addressing Child Sexual Exploitation – A Practical Guide. p. 94. 2008.

^{25.} The National Center for Missing and Exploited Children. The Financial Coalition against Child Pornography- Factsheet. Accessed on the 13th April 2012 from: http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=3703

^{26.} Catherine Beaulieu, ECPAT International. Strengthening Laws Addressing Child Sexual Exploitation – A Practical Guide. p. 92. 2008.

^{27.} ECPAT International. Togo: Global Monitoring Report on the status of action against commercial sexual exploitation of children. p.11. 2011. Accessed on the 13th March 2012 from: http://www.ecpat.net/EI/Pdf/A4A_II/A4A2011_Africa_TOGO_FINAL.pdf

^{28.} Committee on the Rights of the Child. Deuxièmes rapports périodiques des États parties devant être soumis en 1997 :Togo. 11 May 2004. Accessed on the 13th April 2012 from: http://www.unhchr.ch/tbs/doc.nsf/%28Symbol%29/CRC.C.65.Add.27. Fr?OpenDocument

9.3 THE LEGAL POSITION OF THE CHILD VICTIM OF SEXUAL EXPLOITATION

A child victim has the right to be protected and preserved whenever he/she is exploited by others, regardless of the possible consent of the child to the crime. In fact, according to international legal standards, a child cannot consent to be exploited and as such can never be held responsible in these situations. In the specific case of child pornography, it is recognised that the child is not only a victim at the moment when the physical abuse was perpetrated but also whenever the images of the abuse are watched over and over again via the different technological means. Every time a child abuse picture is viewed or shared, the child represented on it is being re-victimised.²⁹

Nonetheless, in far too many countries children who are victims of CSEC are considered criminals and may face prosecution and condemnation, on top of being marginalised and stigmatised. Most African countries fail to provide legal assistance and support services to such children, and whenever these services exist, they are usually available to children who are victims of abuse and not of commercial sexual exploitation.³⁰

Throughout the world, very few children are able to seek justice and compensation when they are victims of sexual exploitation. Settling cases through the official complaint mechanisms is expensive and highly unsatisfactory in terms of the number of offenders actually facing conviction (only about 5 to 7 percent of reported cases). Hence it does not come as a surprise that the majority of victims prefer to solve their cases through informal processes such as out of court settlements, which also serve to protect their families from shame. These informal settlements weaken the official system as well as encourage impunity and repeated offending.³¹

The status, treatment and legal support afforded to the child victim of sexual abuse and commercial sexual exploitation in the countries under review in this research was difficult to assess. There is a pervading lack of data, and only a few countries have dealt with the question in their national legislation. The fact that children are not aware of their rights and rarely receive counseling often leads to further abuse. Furthermore, law enforcement is not provided with adequate training to properly deal with the child victims and the legal procedures.

^{29.} Special Representative of the Secretary General on Violence against Children. The Global Campaign on the OPSC. Accessed on the 30th March 2012 from: http://srsg.violenceagainstchildren.org/page/global-campaign-opsc

^{30.} UNICEF. Sexual Abuse and Exploitation of Children in West and Central Africa. 2008. Accessed on the 12th April 2012 from: http://www.unicef.org/wcaro/english/ESEWCAROFinalReport_EN_corrige.pdf

^{31.} UNICEF. Sexual Abuse and Exploitation of Children in West and Central Africa. 2008. Accessed on the 12th April 2012 from: http://www.unicef.org/wcaro/english/ESEWCAROFinalReport_EN_corrige.pdf

9.4 LEGAL RECOMMENDATIONS

The Governments of Cameroon and Kenya should both ratify the Optional protocol to the CRC on the sale of children, child prostitution and child pornography (OPSC)

National legislations should be harmonised with relevant international legal standards and the African Charter on the Rights and Welfare of the Child to ensure the highest possible number of prosecutions and convictions related to child pornography and other forms of sexual exploitation of children, as well as to facilitate collaboration among law enforcement agencies.

- A clear definition of "child pornography", in line with the Optional Protocol, should be adopted so that vague terms as "obscene" or "indecent" as well as legally undefined terms such as the term "pedophilia" are no longer employed;
- National legislations's definition of child pornography must encompass the broad range of material support used in the production and dissemination of child pornography, including audio, visual, written and electronic formats.
- National legislation must contain the whole range of illicit activities related to child pornography, as defined in article 3.c of the Optional Protocol, whether or not committed through the use of ICTs.
- Mere possession (possession for one's private use) of child pornography materials should be criminalized.
- The solicitation of children online for sexual purposes (child grooming) must be penalised.
- States must enforce actual legislation effectively and consistently, against local as well as foreign offenders.
- Training to combat child pornography and the sexual exploitation of children in ICTs must be provided to all government officials from law enforcement to judicial sectors, and corruption must be adequately punished.
- Regulations regarding the ISPs should be enacted where voluntary self regulatory approach is not present or non functional, so that they are mandated to remove child pornography content when requested, to report such content to law enforcement agencies and to safeguard evidence to facilitate police investigations.
- Internet café owners should be sensitised so as to engage themselves in the prevention of sexual exploitation of children online and child pornography, which includes adopting appropriate codes of conduct. Regulations should be issued to establish their responsibilities in combating CSEC.
- The rights of child victims must be upheld: children must never face prosecution or condemnation in cases of sexual exploitation.
- Adequate psychological assistance and support should be offered to children who are victimised in child pornography and sexual exploitation through ICTs, and the necessary measures taken to avoid social exclusion and stigmatisation.

ANNEXES

CHILDREN'S QUESTIONNAIRE

Thank you very much for agreeing to participate in this survey. Your feedback and inputs are very important for us to learn more about your experiences on online and Internet related things. Your ideas will allow the government and other relevant organisations to create a safer environment for you.

Anything you say will be treated confidentially and we will not ask for your name. When finished, please check to make sure you have answered all the questions.

Thank you so much for your help and your valuable opinion!

-		Personal information
1.	Age:	
2.	Sex:	
	☐ Male	☐ Female
3.	Name of your city	
4.	What grade/year are you studying at school?	
5.	Are you the only child in the family?	
	Yes	□ No
Please	e circle with O as necessary. Internet preferences	and practices
6.	Where do you usually access the Internet?	
	i) At home	ii) Cybercafé/Internet shop
	iii) At school	iv) Other
7.	Which place do you go to more frequently to use	the Internet?
	i) At home	ii) Cybercafé/Internet shop
	ii) At school	iv) Other

8.	How frequently do you access the Internet?			
	i) Every day	ii) Monday through Friday		
	iii) Few days a week	iv) Weekends and holidays		
9)	If you go to a cybercafé, then what time do you u	sually go there?		
	i) In the morning (9-12 am)	ii) During Day time (12-4 pm)		
	iii) In the evening	iv) 4-6 pm		
	v) Very late (6-10 pm)			
10)	Does the cybercafé manager allow you at any time	ne of the day?		
	i) Yes	ii) No		
	iii) Sometimes			
11)	Does the cybercafé owner charge you extra mone	ey to stay during late hours in the evening?		
	i) Yes	ii) No		
	iii) He actually gives me discount			
12.	How many hours a day do you use Internet?			
	i) Yes < 1 hour	ii) No 1 hour		
	iii) No 2 hours	iv) No 3 hours		
	v) No 4 hours	vi) No >5 hours		
13.	Do you have email?			
	i) Yes	ii) No		
14.	Do you have a blog (with photos and videos)?			
	i) Yes	ii) No		
15.	Do you belong to any social network (Facebook, questions.	My Space, Hi5 or others)? If yes, please answer the following		
	i) Yes	ii)No		
16a.	What do you find interesting about the social network that you use?			
16b.	Why did you choose this one over others?			
17.	How do you discover the websites you are interest	sted in? Please select only two options.		
	i) By myself	ii) My school teacher helps me		
	iii) A friend helps me	iv) My mom and/or dad help me		
	v) My older brother or sister help me			

18.	Using a computer takes up time that otherwise I would have spent on Choose only one option.						
		Study		Be with family			
		Be with friends		Read books			
		Play		Play sports			
		Other		Doesn't take up my time			
\Rightarrow	Mobi	le phone usage					
19.	Do yo	ou have a mobile phone? If you don't have a r	mobile	, go to question 28.			
	i) Yes	3	ii) No				
20.	If yes	s, what kind of mobile phone do you have?					
	i) Simple phone with text functions						
	i) Advanced phone with Bluetooth and video playing capacity and with a camera						
	iii) A	smart phone with connection to Internet					
21.	If you	ır answer to the previous question was iii) th	en ple	ase tell us if you can use the Internet from your phone			
	i) Yes	3	ii) I d	o not use it because it is very expensive			
	iii) I c	an access but only a few sites					
22.	Pleas	e tell us if you use your phone to exchange f	iles wi	th your friends by blue tooth or mms			
	i) \	⁄es	ii) No				
23.	If yes	s, what type of files do you usually exchange	?				
	i) Photos of me						
	ii) Photos of me that I have taken with the camera in the phone						
	iii) Photos of others that I have taken with my phone						
		nings such as music or video clips or photos to omewhere else.	that I h	nave downloaded from the Internet or copied from			
24.	What do you mainly use your mobile phone for? Please select up to two options.						
	i) To I	let your parents know where you are	ii) To	send text messages to friends and peers			
	iii)To	stay in touch with friends by calling them	iv)To	play games on the phone			
	v) To	browse the Internet					
	vi) To	download things such as: wallpapers, ringto	ones, v	ideos, music, photos etc.			
25.	Who	do you communicate with your phone more	?				
	i) You	ır parents	ii) Yo	ur friends and peers			

26.	Did your parents put rules on how you can use your mobile phone?					
	i) Yes	ii) No				
27.	If yes to the previous questions, what are the	rules about?				
	i) Have it on at all times	ii) Do not use it in class				
	iii) Do not give your number to strangers	iv) Do not take calls from unknown numbers				
	v) Other					
28.	Have you ever been contacted by someone the	hat you do not know, by mobile phone?				
	i) Yes	ii) No				
29.	If yes, it was:					
	i) By SMS	ii) Someone called me on my phone				
Your	views:					
How	important do you think a mobile phone is to you	u? Would you consider yourself lucky if you have one?				
-	Access from Cybercafés:					
30.	Roughly how many cybercafés do you have ir	n your neighbourhood?				
	i) Less than 5	ii) 5-10				
	iii) More than 10	iv) I do not know				
	v) We do not have a cybercafé in my area					
31.	Do you go to Internet cafés?					
	i) Yes	ii) No				
32.	If your answer was no, please tell us why.					
	i) My parents don't let me go	ii) Because I have to pay				
	iii) It is less private	iv) I already have a computer with connection at home				
	v) I don't like the people there					
33.	Mainly, what do you do at the Internet café?	Please select up to five options.				
	i) Play games	ii) Do homework				
	iii) Browse websites	iv) Read/send emails				
	v) Chat with others online	vi) Meet new people online				

	vii) Download music	viii) Participate in forums			
	ix) Learn to use programs	x) Read news			
	xi) Update blog	xii) Enter a virtual community			
	xiii) Use Facebook	xiv) Watch videos online			
34.	Why do you prefer to go to the cafés?				
	i) To browse the websites I want without my par	rents watching			
	ii) To browse the Internet for as long as I want				
	iii) Because I do not have computer or Internet a	t home			
	iv) Accessing from the Cybercafé is cheaper				
	v) We can play with other friends				
	vi) There are more features available on the Cybe	ercafé computer that we do not have in school or at home			
35)	While you are at the Internet cafés, do you recei	ve any help or instructions about how to use the Internet?			
	i) Always	ii) Yes, sometimes but I have to ask			
	iii) Never				
36.	Is there any material placed at the Internet cafe posters, brochures, screensavers etc.)?	é that gives you more information about risks online (such as			
	i) Yes	ii) No			
	iii) Not sure				
37.	Do you go to the cafés in groups?				
	i) Yes	ii) No			
	iii) Sometimes				
38.	Can you download any content you like photos or adult material such as pornography)?	from the cybercafé (such as games, videos, movies,			
	i) Yes	ii) No			
	iii) Only if I pay the café manager				
39.	Do you find the cybercafés to be comfortable ge	nerally?			
	i) Yes	ii) No			
	iii) No, but I have no choice				
10.	Would you go to a cybercafé even if you are not	comfortable with the environment?			
	i) Yes, because I really like to use the Internet, play games online etc.				
	ii) No				
	iii) Yes, when I am there with friends I can handle	e the situation			
11.	Have you ever been approached by an adult you	do not know at the café?			
	i) Yes	ii) No			
	iii) Prefer not to say				

42.	If the answer to the previous question is yes, did you like what he or she said?					
	i) Yes	ii) No				
	iii) Not sure					
43.	What are some of the other activities	that you have seen happening in a cybercafé? List all that you remember:				
	i) Distribution of files downloaded from the Internet					
	ii) Using the Internet to watch pornog	graphic movies				
	iii) Gambling and betting online					
•	Family Settings and parental guidance					
44.	Do you do have a computer with Inte	rnet connection at home? If you answer is no, go to question 62.				
	i) Yes	ii) No				
45.	At home your Internet connection is.					
	i) Dial up	ii) Broadband				
	iii) Wireless via satellite	iv) I do not know				
46.	The computer is located at:					
	i) Living room	ii)Your bedroom				
	iii)Parent's bedroom					
47.	Where would you prefer to use the co	omputer from?				
	i) Living room	ii) Reading room				
	iii) Your bedroom					
48.	What do you use the computer at you	ur house for? Please choose up to five options.				
	i) Play computer games	ii) Do homework				
	iii) Browse websites	iv) Read/send emails				
	v) Chat with MSN	vi) Meet new people online				
	vii) Download music	viii) Participate in forums				
	ix) Learn to use programs	x) Read news				
	xi) Update blog	xii) Enter a virtual community				
	xiii) Use Face book	xiv) Tweet				
	xv) Watch videos online					
49.	If any of the activities that is listed in roman number on it.	n the above question is new to you, which one is that? Indicate using the				

50.	When you use the Internet at home, is an adult always with you to see what websites you visit?				
	i) Always	ii) Sometimes			
	iii)Never				
51.	What do you like doing the most while using th	ne Internet at home? Please select up to 3 options.			
	i) The games that I play using computers	ii) Homework for school			
	iii) Browse websites	iv) Read/send emails			
	v) Chat with friends	vi) Meet new people online			
	vii) Download music and videos	viii) Participate in forums			
	ix) Learn to use programs	x) Read news			
	xi) Update blog/photo blog/video blog				
	xii) Enter a virtual online community (such as Sec	cond Life)			
	xiii) Use Face book	xiv) Tweet			
	xv) Watch videos online				
52.	What other things do you do on the Internet at	home? Please select all the options you want.			
	i) I Browse the websites I want without my parents knowing				
	ii) Set up a personal profile on social networks like Facebook and also look for new friends from other countries				
	iii) I use the webcam to talk to friends				
	iv) Play online games with others				
53.	What do you not like about having the Internet at home?				
	i) My parents monitor what I do online				
	ii) They tell me when I can use the computer				
	iii) They tell me for how long I can use the computer				
	iv) Having to share the computer				
54.	What do you like the most about using Internet	t at home?			
55.	Have you ever received any guidelines from you	ur parents about how to use computers or the Internet at home?			
	i) Yes	ii) No			
	iii) They do not know anything about computers so we cannot ask them				
	iv) I do not see the need for guidance				
56.	If your parents were knowledgeable about to interested to approach them for guidance? If no	the Internet and other computer-related things, would you be ot, why?			

57.	Have your parents ever asked you not to be on the Internet or use any of the online applications?				
	i) Yes	ii) No			
58) 	If yes, why did they do so?				
 59.	Have you ever seen your parents watching a or sites with lot of sexual content)?	dult content on the home computer (such as pornographic websites			
	i) Yes	ii) No			
	iii) Prefer not to say				
60.	Have you ever felt the compulsion to see su connection at home?	ich content (adult content including pornography) using the Internet			
	i) Yes	ii) No			
61.	Have you ever seen adult content on the International Have you ever seen adult content on the International Have you ever seen adult content on the International Have you ever seen adult content on the International Have you ever seen adult content on the International Have you ever seen adult content on the International Have you ever seen adult content on the International Have you ever seen adult content on the International Have you ever seen adult content on the International Have you ever seen adult content on the International Have you ever seen adult content on the International Have you ever seen adult content on the International Have you ever seen adult content on the International Have you ever seen adult content on the International Have you ever seen adult content of the International Have you ever seen adult of the Internat	ernet (pornography such as photos or videos of people having sex) at és with your friends or at their home?			
	i) Yes	ii) No			
62.	Do you know any friend of yours who has se	en such content online?			
	i) Yes	ii) No			
63.	If yes, did they share their experience with y	vou?			
	i) Yes	ii) No			
64.	Have you ever seen anyone of your age or y	ounger in such images or videos?			
	i) Yes	ii) No			
	iii) Prefer not to say				
-	School Setting				
65.	How many computers do you have at your s	echool?			
	i) None	ii) Less than 5			
	iii) Between 5 -10	iv) More than 10			
66.	What do you use the computers at school for	or? Please choose up to five options.			
	i) Play games	ii) Do homework and class work			
	iii) Browse websites	iv) Read/send emails			
	v) Chat with friends	vi) Meet new people online			
	vii) Download music	viii) Participate in forums			
	ix) Learn to use computer programs	x) Read news			
	xi) Update blog	xii) Enter a virtual community such as Second Life			
	xiii) Use Facebook	xiv) Tweet			
	xv) Watch videos online				

67.	At school have they taught you how to? Please select as many as you need.						
	i) Use an email account	ii) Build a blog or site					
	iii) Find information	iv) Use computer programs					
	v) Use internet safely						
68.	In your school, have you ever attended any	In your school, have you ever attended any event that talked about risks arising out of using the Internet online?					
	i) Yes	ii) No					
	iii) Our school has not organised such an e	vent in the past					
69.	If the answer to the previous question was	s yes, do you remember any of the risks mentioned?					
	i) Yes	ii) No					
70.	If yes, can you list some of them here:						
 71.	Nid they talk about some of the ways by w	hich you can address or reduce such risks?					
,	i) Yes	ii) No					
72.	Do you agree with such methods?	.,,					
,	i) Yes	ii) No – because they do not make sense					
	iii) No- because they do not work	iv) No – because we can handle such risks on our own					
	v) I do not see any real danger or risk by us						
73.	Do you think your teachers can help you le						
,	i) Yes, a lot	ii) Yes, a little					
	iii) Not at all						
\(\rightarrow\)	Type of behaviour online and vulnerabilities						
74.	Do you do any of these when using the Int	ernet or a mobile phone?					
	i) Add strangers to your chat or messenger programs (such as MSN, Yahoo, Skype, GoogleTalk etc.?)						
	ii) Post your home address, school or pho	ne number					
	iii) Publish your email visible to others	iv) Open attachments in emails from strangers					
	v) Use a webcam to talk with friends	vi) Use the webcam to meet strangers					
	vii) Threaten your classmates anonymously	/					
	viii) Post photos of yourself without clothes	s or in revealing poses					
	ix) Schedule to meet people you only have known online						
	x) Post photos of others without their con	sent					

75.	Has anyone tried to hurt you on the Internet thro	ugh the following?					
	i) Sending you inappropriate images or videos of adult pornography						
	ii) Asking you to pose in front of the camera wit	hout clothes on					
	iii)) Demanded that you receive the photos or vid with	eos that they send to you which you did not feel comfortable					
	iv) Asked you to add them to your friends list even though you did not want to						
	v) Posted bad things about you in text format or without your knowledge	uploaded your personal photos or videos on websites					
	a) Yes	b) No					
	c)Do not know	d)Prefer not to answer					
76.	If yes, in which manner has it happened?						
	i) By instant messaging (such as Yahoo, MSN o	chat, GoogleTalk, Skype etc.)					
	ii) In a chat room (if you do not know what a ch	at room is, please indicate here)					
	iii) By email						
	iv) On a social networking website (such as Face	ebook, Hi5, Myspace, Orkut, Bebo, Mixit etc.)					
	v) Online gaming website						
	vi) Some other way						
	vii) I have no idea						
77.	If that has happened, how upset were you about	the incident?					
	i) Very upset	ii) Just a bit upset					
	iv) Not at all						
78.	Did you talk to anyone about what had happened	1?					
	i) Yes	ii)No					
	iii) Prefer not to say						
79.	If you had said yes above, who would you approa	ach for this?					
	i) My parents	ii) My brother or sister iii) A friend					
	iv) A teacher at school	v) A policeman or a social worker or a counsellor					
	vi) Another adult that I trust	vii) Someone else					
80.	If you are still thinking about the incident that too happened to you?	k place, did you do any of the things below in response to what					
	i) I stopped using the Internet for a while	ii) I deleted all messages from the person					
	iii) I changed my privacy /contact settings	iv) I blocked the person from contacting me					
	v) I reported the problem (to a service provider,	clicked a button to report abuse on the internet etc.)					
	vi) None of these						
81.	In the last months have you acted in similar ways	s as above?					
	i) Yes	ii) No					

iv) Prefer not to say

iii) Do not know

- 82. If your answer was yes, what exactly did you do?
 - i) Post photos of someone without their consent
 - ii) Wrote something about them on the blog/website/forums that are not true
 - iii) Send them a link that contained adult pornography, knowingly so that they feel uncomfortable
 - iv) Others:
- 83. What would be the main reason for you to behave like that?
 - i) It is fun
 - ii) It does not hurt the other person if I do it through the Internet
 - iii) I see others doing it too
 - iv) Someone has done it to me, so I want to give it back to them
 - v) You cannot really harm someone through the Internet
- 84. Do you read any safety guidelines for using the Internet that is posted online?
 - i) Yes ii)No
 - iii) I am not aware of any such thing online iv) They are useless and too long v) Does not apply to me
 - vi) They are difficult to find and download
- 85. What do you think the big companies like yahoo, Google, Microsoft or others should do to help your online experience (circle all that apply):
 - i) They should make the products and services safer, so that we do not have to worry about it
 - ii) They should give us easier tools and guidelines
 - iii) Our services should not be mixed with adults
 - iv) Mobile phones and Internet use from computers should be free of nasty things such as pornographic websites and downloads
 - v) Make more interesting games and online applications that children can have more fun with
 - vi) Make technology more affordable, so that every child can have access to Internet
- 86. What do you think the cybercafés should do to make the Internet access from their cafés safer for children (circle all that apply)?
 - i) Provide a clean Internet service that does not give access to illegal images (such as pornography etc.)
 - ii) Do not allow anyone to pay money to download or access such materials
 - iii) Have safety materials available for children to study
 - iv) Have separate spaces for children and adults
 - v) Have specified times for children to use the café
 - vi) Provide assistance if someone is in distress due to something bad on the Internet
 - vii) They have no role to play, they do not understand online safety issues
 - viii) They care less about these as they need money from their customers

Well done! Your inputs were very useful and many thanks for all your help!!!

CYBERCAFÉS' QUESTIONNAIRE

Questionnaire for cybercafés

Dear cybercafés managers/owners,

ECPAT International is conducting a research on children's use of new technologies. We need your important contribution to be able to learn more about how boys and girls use computers, Internet and mobile phones. This will help us understand better what happens online and how we can work to make those experiences safer.

For this reason we invite you to answer a series of questions, allowing us to retrieve the opinion of hundreds of cafés managers/owners and build a profile of how children relate to technologies today.

Anything you say will be treated confidentially and we will not ask for your name. When finished, please check to make sure you have answered all the questions.

Thanks for your help and your opinion! ECPAT International

1.	Desc	ribe the type of clients that visit your café most often.
		Children (age group 10-15)
		Children (age group 15-18)
		Adults
		Both children and adults
2.		t are the operating hours of your café:
	0pen	ning time:Closing time:
3.	Wha	t kind of services do you offer in your café? Tick all that apply:
		File download services (such as movies, music etc.)
		Printing ,faxing, scanning and similar services
		Online gaming or local gaming
		Copy files (sharing and distributing already downloaded files)
4.	Do yo	ou have any policies or guidelines for the customers?
	a. Ye	
	C. INE	ever heard of such thing
5.		ustomers need to register or sign up before they can use your café?
	a. Ye	
	C. IT I	s optional

6.	If yes a. Yes	to the question above, was it mandated by the	he regulatory authorities? b. No, we decided to enforce it to protect ourselves			
7.		u have to sign a contract or an agreement be café association, the Ministry of Telecommun	fore you can start up a café (such as permissions from a local ications, the Ministry of Culture etc.)?			
	a.Yes c. Yes	, but you can also do without it	b. No.			
8.	envi	ronment?	able to you that says what you can do or not do in your café			
	a. Yes c. We	create our own guidelines and policies	b. No.			
9.	have t	o follow to use their Internet services?	r from time to time to remind you about the policies that you			
	a. Yes		b. Never			
10.		many computers do you have in your café?	. 44.00			
	a. 1-1 c. 20-		b. 11-20 d. More than 30			
11.	Do you a. Yes	· ·	s? If yes please go to question 12, otherwise go to question 13. b. No			
12.	Why c	did you create a separate space for children?	Tick all that apply.			
		So that children do not see adult content or	mix with adults			
		Adults are disturbed when children are around	und them and make noise			
		Adults specifically asked or prefer a more p	ersonal space			
		Children specifically asked or prefer a separ with friends)	ate space for themselves (such as for playing games or to chat			
		So that children used specific computers w	ith filters			
		So that I can monitor them through the serv	ver			
13.	Are yo	ou aware of any risks that children might face	while using the Internet ? b. No.			
	c. Yes	c. Yes, but I do not have much knowledge about it				
14.		answered yes to the previous question, carnet?	n you list what type of risks they might face while using the			

15.		you ever had a case in your cybercafé where a child/children was/were upset with something he/she/they or did on the Internet? b. No
16.	If the	answer to the previous question was yes, did they come to ask for help? b. No
17.	Do yo	ou currently have systems in place or knowledge of how to give them advice if they come to you for help? b. No
18.	Can s	Someone download or view pornography in your café? No (our café does not provide access to such things) Anyone can (as we have no control on what people are doing on their machines) Children cannot but adults can if they want (we have special access codes for them)
19.	a. No	d you mind if your customers go to other cafés that allow certain activities that you would not allow? b. In such case, I would change my policies on't know
20.	Do ch	nildren have specific times that they can come to the café? b. No, they can come anytime
21.	If you	r response to the above question was yes, what is the specific time they cannot come?
		kind of things do children love to do most during the time they spend in your café? Please check all that apply. Chat with others Upload photos on social networks such as Facebook, Hi5, Mixit etc. Watch videos on you-tube or similar sites Play games including online games Watch adult content not appropriate for their age such as pornography and websites with explicit sexual content Chat with others using the webcam Exchange files that they download from the Internet with each other through USB drives Download music, videos, other files such as software Browse the websites and check email Just come here to talk to other children and not use the computers Searching new friends Searching love partners Do researches for their studies
		Looking for avenues to travel or get scholarship Searching for sponsorship for studies, football

23.	What	are the main purposes of the adults who come to your café? Please check all that apply.
		Access all kind of online stuff without risking their identity
		Download content from the Internet that would be difficult to do from home because of the speed of the Internet
		Access content that would otherwise be difficult to see from home such as pornography
		Talk to others online, not disclosing such activities to their family members
		Play computer games with children
		Play computer games with other adults
		Searching new friends
		Searching love partners
		Do researches for their studies, business, work
		Looking for avenues to travel or get scholarship
		Searching for sponsorship for studies, football, business, work
24.	a. Yes	ou have webcams and microphones connected to your computers? b. No me computers
25.	If yes	, do the customers (both adults and children) use them?
26.		you ever seen anyone in the café (including a child) appear in front of the webcam in revealing poses or to take off their clothes (particularly when they are using a computer alone and not visible to others)?
		There was a case like that
		Never
		My café does not provide a setup that will make people comfortable doing that
		This is the first time I am hearing that such thing can happen in a public place like a cybercafé
27.		particular application or service provided by your café do you think is the most popular among children? the 2 most popular applications.
		Browsing the website
		Watching movies
		Downloading movies for viewing later outside the café
		Playing online or local networked games
		Using social networks such as Facebook for uploading photos, videos and posting comments etc.
28.		f the services mentioned above, which one do you think children are really addicted to and can go out of way to access?

29.		ere any noticeable difference observed by you b d by you above?	etween boys and girls in terms of the popular applications
30.	What	at could be the reason for such differences accor	rding to you?
31.	such	as access to any particular websites?	visiting your café not to provide certain types of services
	a. Ye	28	b. Never
32.	Did a	any parents ask you not to allow their children a	fter certain hours?
		Yes, in fact we get this request very often	
		Yes, but very rare	
		No - they would actually be very happy to hav	e the child not disturb them at home
33.		ıld you like to make your café safer for children?	
	a. Ye	28	b. No, it is already safe for them here
34.	Woul manr	·	dren use your café in a more secure and comfortable
		Yes, certainly	
		No Not if it takes time and we have to spend more	money on it
		•	mers away as they cannot view adult content in the café
35.	that va. Ye	will build your capacity to do so and help you w	ldren, would you be interested in taking part in a project ith technical support? b. No
36.	Woul	ıld you be interested in getting free software and	d other resources to help you run your café better
		IT companies?	
	a. Ye	es, that will be very helpful	b. No, thanks
37.	What	at kind of Internet connection do you have?	
		Dial-up modem	
	Broad	dband using	
		ADSL modem	
		Satellite connection – VSAT	
		Wireless connection from mobile provider	
		Any other	

 39. Is your cybercafé part of a larger association or network of cybercafés? a. Part of a bigger chain b. Individual shop 40. Are you the owner of the café, the manager or both? a. Owner b. Manager c. Both 41. What are their propositions to make cybercafés safer for children? 	38.	a. Less than 25% c. More than 50%	b. 25-50%			
a. Owner b. Manager c. Both	39.	, , ,	,			
41. What are their propositions to make cybercafés safer for children?	40.	a. Owner				
	41.	What are their propositions to make cybercafés safe	er for children?			

TEACHERS' QUESTIONNAIRE

Dear teacher,

ECPAT International is conducting a research on children's use of new technologies. We need your important contribution to be able to learn more about how boys and girls use computers, Internet and mobile phones. This will help us understand better what happens online and how we can work to make those experiences safer.

For this reason we invite you to answer a series of questions, allowing us to retrieve the opinion of hundreds of teachers and build a profile of how children relate to technologies today.

Anything you say will be treated confidentially and we will not ask for your name. When finished, please check to make sure you have answered all the questions.

Thanks for your help and your opinion!

ECPAT International

iii) Sometimes

١.	Age:				
2.	Sex:				
	☐ Male		Female		
3.	Name of your city				
4.	What grades do you teach at school?				
	i) Primary school	ii) S	Secondary (High) school		
5.	In relation to new technologies (Internet, mobiles),	do yo	u consider yourself to be:		
	i) Advanced user (very knowledgeable)	ii) A	Average user		
	iii) Inexperienced				
6.	What do you use the computer for? Please choose use	up to	five options.		
	i) Play games	ii)	Teach students and check their work online		
	iii) Browse websites	iv)	Use emails		
	v) Keep in contact with friends and relatives thro	ugh d	chat programs		
	vi) Meet new people online	vii)	Download music		
	viii) Participate in forums	ix)	Learn to use programs		
	x) Read news	xi)	Update blog		
	xii) Enter a virtual community	xiii)	Use Facebook		
	xiv) Tweet	xv)	Watch videos online		
7.	Do you know how to install a content filter?				
	i) Yes	ii)	No		
8.	Do you suggest the issue of Internet safety to your	stude	nts?		
	i) Always	ii)	Frequently		

iv) Never

9.	Did your students ask for orientation on criteria for searching information on the Internet?					
	i) Always	ii)	Frequently			
	iii) Sometimes	iv)	Never			
10a.	Do you provide guidance on Internet use?					
	i) Yes	ii)	No			
10b	If yes, then on what topics?					
	i) Validity of sources	ii)	Reporting illegal content			
	iii) Authenticity of the information	iv)	Discerning content for adults			
	v) Organising information	vi)	Safe practices			
	vii) Safe use of social networks such as how to p	rotec [.]	t the personal profile			
	viii) Ethical use of the Internet					
11.	Are you interested about the online interactions of	of you	r students?			
	i) Yes	ii)	No			
12.	How have you shown this interest?					
	i) Group discussion on Internet use	ii)	Students have shown me the sites they frequent			
	iii) Chat with other teachers	iv)	I have observed students interacting on chat programs			
	v) I visited student's blogs	vi)	I spoke to students about safe Internet use			
13.	Have you talked about online pornography (both of adults and involving children) with your students?					
	i) No, I haven't	ii)	I don't think I should discuss the issue in class			
	iii) Yes, I have	iv)	I think it is right to discuss this in the classroom			
14.	Do you think children are at risk when they intera	ct onl	ine with strangers?			
	i) Yes	ii) ſ	No			
15.	If you think there are dangers, which ones do you think are the most risky situations for a child or teenager?					
	i) Use chat programs	ii)	Use Facebook or other social networks			
	iii) Have an email with an identifiable name and last name					
	iv) Chat in forums	v)	Accept strangers in chat programs			
	vi) Play online games with strangers					
	vii) Post photos of themselves that are revealing in nature or without clothes					
	viii) Publish personal information (name, mobile number etc.)					
	ix) Establish linkages with strangers					
	x) Accept to meet up with strangers in real life					
16.	Do you know cases of children who had safety is	sues	caused by virtual interactions?			
	i)Yes	ii)	No			
17.	How important do you think it is to build understause of ICTs?	nding	and capacity on self-protection online and responsible			
	i) Very	ii)	Somehow			
	iii) A little	iv)	None			
18.	Have you worked on prevention strategies with y	our st	tudents for a safe online interaction?			
	i) Yes	ii)	No			

19.	If you did, what type of self-protection strategies did you teach them?					
	i)	Only talk with friends	ii	Avoid publishing personal information		
	iii)	Do not participate in open forums	i	v) Avoid getting in touch with strangers		
	v)	Do not meet offline strangers you've met online	e v	vi) Using privacy settings		
	vii)	Do not share personal photos online that could	d be	misused		
	viii)	Any other messages				
20.	Do y	ou discuss with your students about ethical use	of th	ne Internet and mobile phones?		
	i)	Yes	ii)	No		
21.	If you	u do, what do you talk about?				
	i)	Respect other's feelings when publishing photo	os ar	nd comments		
	ii)	Respect different opinions in forums	iii)	Do not intimidate others by hiding your identity		
22.	Who	do you think uses the Internet and mobiles with	n mo	re knowledge and ability?		
	i)	Always teachers	ii)	Mostly teachers		
	iii)	Always students	iv)	Mostly students		
23.	Wha	t technological tools do you think the students u	ise n	nore frequently?		
	i)	Email				
	ii)	Chat and messenger programs such as MSN, V	Y aho	o messenger, Skype etc.		
	iii)	Social networks	iv)	Blogs		
	v)	Text messages by phone	vi)	Search engines		
24.	With	the use of technologies children have become i	more	e choose up to three options.		
	i)	Communicative	ii)	Reserved		
	iii)	Idle	iv)	Active		
	v)	Violent	vi)	Quiet		
	vii)	Prone to risky behaviour	viii)	Confident		
	ix)	Outgoing				
25.	Do y	ou know cases of grooming or sexual exploitatio	n on	ıline?		
	i)	There was a case at the school	ii)	There were several cases at the school		
	iii)	I heard rumors	iv)	Heard rumors of cases through a colleague		
	v)	I do not know about this subject				
26.	Does	s your school have a referral mechanism for repo	rting	g cases of online sexual exploitation?		
	i)	Yes	ii)	No		
27.	Wha	t is the role the school should play regarding the	dar	ngers brought about by new technologies?		
	i)	Teach students about the subject				
	ii)	Search for prevention strategies that involve ch	nildre	en and youth		
	iii)	Raise awareness among parents				
	iv)	Sensitize parents and students about the subject	ect			
	v)	It is a subject outside of the scope of class				
28.	Wha	t do teachers need to learn about how to better	use	new technologies?		
	i)	Capacity building about technology	ii) C	apacity building about educational strategies using ICTs		
	iii)	Time to surf the net	iv) (Capacity building on safe use of ICTs		
	v)	Better access to ICTs at school	vi) E	Better access to ICTs at home		

29.	Does the school provide you with information and guidelines on how to protect children online?			
	i)	Yes	ii) No	
	iii)	Somehow yes		
30.	Does the school have clear policies on Internet safety that are codified and distributed?			
	i)	Yes	ii) No	
31.	Do you think having written policies would make it easier for the teacher to implement safety standards?			
	i)	Certainly yes	ii) Maybe	
	iii)	Certainly no		
32.	Does the school provide unrestricted Internet access to children and teachers such as access to social networks, Youtube, file download services or web browsing to any site?			
	i)	Yes	ii) No	
33.		f no, does it have transparent mechanisms to explain why certain services are not available to children and the eachers?		
34.	Do you think children should be allowed to use mobile phones in the school?			
	i)	Yes	ii) No	
35.	If no, why do you think so?			
36.	What is your school's current policy on allowing school children to use mobile while they are in the school		nildren to use mobile while they are in the school?	
•••••				
•••••				

ECPAT International really appreciates your contribution in this effort and wants to express the most sincere thanks to you for all your help!!!







ECPAT International

328/1 Phayathai Road Ratchathewi, Bangkok 10400 THAILAND Tel: +662 215 3388, +662 611 0972

Fax: +662 215 8272 Email: info@ecpat.net | media@ecpat.net

Website: www.ecpat.net