Key field research findings

Assessment of the National Response to Child Online Sexual Exploitation in Kenya using the WePROTECT Model National Response framework

Final draft

08 October 2021

Maestral.

Table of Contents

Acknowledgements

Maestral International would like to thank the following individuals for their invaluable contributions to the development of this assessment report and the National Plan of Action on Online Child Sexual Exploitation and Abuse (OCSEA):

Rose Mwangi, DCS, Faith Manyala and Monika Sandvik-Nylund, UNICEF Kenya, TWG on COP, Caroline Parmet, TdH Netherlands, facilitators of the child participation sessions, other individuals who reviewed the report. Last but definitely not least, Maestral would like to thank all the individuals and organizations who generously gave their time and shared their experiences and ideas in interviews, online surveys and focus group discussions.

The Maestral Team included team leader Atieno Odenyo, and team members Leonora Borg, Fatma Abdullahi and Sian Long.

The TWG further wishes to acknowledge the role of all the stakeholders and DCS and AHTCPU staff that generously gave their time to participate in the assessment interviews, focus group discussions and online surveys. Their valuable contribution influenced the outcome of this assessment and contributed to the development of the National Plan of Action on OCSEA.

Glossary

App: a computer program or piece of software designed for a particular purpose that you can download onto a mobile phone or other mobile device.[1]

Child sexual abuse materials (CSAM) includes, but is not limited to, "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," as well as the use of a child to create such a representation.[2] CSAM can be broadened to include sexual exploitation of children in travel and tourism; online enticement; trafficking of children for sexual purposes; child sexual molestation; misleading domain names or words; and solicited or unsolicited obscene material sent to a child.[3]

Child sexual exploitation is a type of child abuse that happens when a child is performing, and / or another or others are performing on them, sexual activities sometimes in exchange for something (e.g. food, accommodation, drugs, alcohol, cigarettes, affection, gifts or money).[4]

Commercial sexual exploitation of children comprises sexual abuse by the adult and remuneration in cash or kind to the child or a third person or persons. The child is treated as a sexual object and as a commercial object. It constitutes a form of coercion and violence against children and amounts to forced labour and contemporary form of slavery.[5]

Content blocking: can be done nationally, by Internet Service Providers (ISPs), organisations and schools and individuals. Content is usually blocked through filtering based on key words, URL-based filtering, and Hash matching. However, too strict blanket blocking can be viewed as an infringement of human rights; and content blocking does not work on the Dark Web.[6]

Cyber/cyberspace/online space: involving, using, or relating to computers, especially the internet.[7]

Cyber-bullying: bullying with the use of digital technologies which can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted. Examples include: spreading lies about or posting embarrassing photos of someone on social media; sending hurtful messages or threats via messaging platforms; impersonating someone and sending mean messages to others on their behalf. Face-to-face bullying and cyberbullying can often happen

[1] University of Cambridge (2021). Cambridge University Dictionary, https://dictionary.cambridge.org/
[2] International Centre for Missing and Exploited Children, 2018, Child sexual abuse material- model legislation and global review, page 10
[3] ECPAT, 2018, Trends in Online Child Sexual Abuse Material
[4] Interagency Working Group on Sexual Exploitation of Children (2016), 'Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Retrieved from http:// luxembourgguidelines.org/.
[5] ANPPCAN, Study on Sexual Exploitation of Children in Travel and Tourism in Kenya, 2015 Interagency Working Group on Sexual Exploitation of Children (2016), 'Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Retrieved from http://luxembourgguidelines.org/
[6] ECPAT, 2018, Trends in Online Child Sexual Abuse Material
[7] University of Cambridge (2021). Cambridge University Dictionary, https://dictionary.cambridge.org/

alongside each other. But cyberbullying leaves a digital footprint – a record that can prove useful and provide evidence to help stop the abuse.[8]

Cyberlocker: a third-party online service that provides file-storing and file-sharing services for various types of media files and data.[9]

Cyber Tipline: NCMEC reporting system for the online exploitation of children

Dark Web: Intentionally concealed content accessed through web browsers that are designed to protect individuals' identity, for example through encryption. The Onion Router (TOR) is one such example. However, as noted by the Global Commission on Internet Governance, the Dark Web also gives freedom of information to individuals, which is particularly important to those in repressed regimes.[10]

Grooming: when someone builds a relationship, trust and emotional connection with a child or young person so they can manipulate, exploit and abuse them. Children and young people who are groomed can be sexually abused, exploited or trafficked. Anybody can be a groomer, no matter their age, gender or race. Grooming can take place over a short or long period of time – from weeks to years. Groomers may also build a relationship with the young person's family or friends to make them seem trustworthy or authoritative.[11]

Image host: a platform/website that allows individuals to upload images. Once you have uploaded them, the images are said to be hosted and you can access them online. Image hosting allows you to make the images available to a broader audience and embed them to another website. The images are hosted on the cloud, rather than on one single server so that it is spread across several servers in multiple locations and connected through the internet.[12]

Internet forum, a website that provides an online exchange of information, questions and answers between people about a particular topic. It is also called a discussion board or discussion group, and uses Web browser for access.[13]

Live-streamed child sexual abuse: "images or videos permanently recorded from a live broadcast stream; in which the child(ren) consciously interacted with a remote other(s); and which met the… threshold for action as child sexual abuse material.[14]

Massive Multi-User Online Role-Playing Games (MMORPGs): encourage individuals to form strong relationships online in order to advance through the games. Both text and chat are used and there is often the option of using cryptocurrency to purchase items (such as extra

[8] https://www.unicef.org/end-violence/how-to-stop-cyberbullying
[9] Techopedia: https://www.techopedia.com/definition/27694/cyberlocker
[10] UNICEF, 2017, State of the World's Children – Children in a Digital World
[11] National Society for the Prevention of Cruelty against Children (NSPCC) UK (2019), https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/#what-is
[12] Geekflare (Nov 24, 2020). 11 best image hosting sties for personal to business. Retrieved from: https://geekflare.com/best-image-hosting/
[13] PC Mag Encyclopedia. https://www.pcmag.com/encyclopedia/term/internet-forum
[14] Internet Watch Foundation, 2017, Distribution of Captures

lives) in the game. Players create their own profiles which enables adults who want to groom children to create profiles that help them to do so – often pretending they are children.[15]

Online child sexual exploitation: a type of sexual abuse. When a child is sexually exploited online they may be persuaded or forced to create sexually explicit photos or videos or have sexual conversations.[16] The production, dissemination and possession of child sexual abuse material (CSAM: which are known in many jurisdictions as 'child pornography'); online grooming or active sexual solicitation of children; sexting; sexual extortion of children (also known as 'sextortion'); revenge pornography; exploitation of children through online prostitution, and live streaming of sexual abuse. We can also make a distinction between cyber-enabled and cyber- dependent crime.[17]

Online child sexual abuse: when a child or young person is forced or tricked into sexual activities online - for example, a child could be forced to make, view or share child abuse images or videos or take part in sexual activities on conversations online.[18]

Online platform: a digital service that facilitates interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet.[19]

Pop-ups: Pop-ups are small windows that 'pop up' over the top of web pages in your internet browser, **– often used by advertisers to get your attention or by viruses to trick you into clicking on them[20]. Pop-ips are** a form of online advertising focused on attracting Web traffic.[21]

Pre-pubescent: the time prior to a child reaching puberty.

Sexting: when someone shares sexual, naked or semi-naked images or videos of themselves or others or sends sexual messages. It's online abuse if a child or young person is pressured or coerced into creating or sending these types of images.[22]

Splash page: a warning page to users trying to access CSAM to act as a deterrent. It can provide a warning, offer of support (such as where to get help), encourage reporting of illegal content, and create a feeling of risk in offenders.[23]

TOR: short for 'The Onion Router', is both a software and a network that helps maintain anonymity on the internet.[24] Other similar software is Riffle, Freenet and I2P. An analysis by

---

[15] ECPAT, 2017, Online Child Sexual Exploitation: an analysis of emerging and selected issues
[16] National Society for the Prevention of Cruelty to Children (NSPCC): https://learning.nspcc.org.uk/child-abuse-and-neglect/child-sexual-exploitation
[17] ECPAT, 2018, Trends in Online Child Sexual Abuse Material, page 8
[18] National Society for the Prevention of Cruelty to Children (NSPCC): https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
[19] OECD library https://www.oecd-ilibrary.org/science-and-technology/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation_19e6a0f0-en
[20] http://www.bbc.co.uk/webwise/guides/about-popups
[21] https://www.techopedia.com/definition/15480/pop-up-ad
[22] National Society for the Prevention of Cruelty to Children (NSPCC): https://learning.nspcc.org.uk/research-resources/briefings/sexting-advice-professionals
[23] ECPAT International (2017). Child online sexual exploitation: an analysis of emerging and selected issues. Journal April 2017 https://www.ecpat.org/wp-content/uploads/2017/04/Journal_No12-ebook.pdf
[24] ScienceDirect (2017). https://www.sciencedirect.com/topics/computer-science/onion-router

the U.S. Federal Bureau of Investigation (FBI) of one TOR-based website found that it hosted "approximately 1.3 million images depicting children subjected to violent sexual abuse."[25] Whilst content sits both on the web and Dark Web, the Dark Web, particularly sites like TOR, make tracing those who upload, download and view CSAM extremely difficult.

Virtual/crypto currency: for example, Bitcoin, is often used to pay for CSAM including livestreaming. Users can remain anonymous and use can be encrypted, making it challenging to track both the buyer and seller. The creator of Bitcoin remains anonymous. Cryptocurrency is also used to persuade or encourage children to participate in CSAM, as well as demanding payments (and/or more CSAM) from children to prevent the release of CSAM onto the internet, particularly to friends and family.[26] Block chain is the technology that enables the existence of cryptocurrency. Not all cryptocurrencies operate on a block chain, and not all block chains utilize cryptocurrencies as part of their design.[27]

Web host: or web hosting service provider, is a business that provides the technologies and services needed for the website or webpage to be viewed on the Internet.[28]

[25] U.S. Department of Justice, 2016, The National Strategy for Child Exploitation Prevention and Interdiction
[26] ECPAT International (2017), Online Child Sexual Exploitation: an analysis of emerging and selected issues. Retrieved from:
[27] https://blog.makerdao.com/the-benefits-of-cryptocurrency-and-blockchain-technology/. https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html#:~:text=Blockchain%20is%20the%20technology%20that,cryptocurrency%20(among%20other%20things).&text=A%20cryptocurrency%20is%20a%20medium,verify%20the%20transfer%20of%20funds.
[28] https://www.website.com/beginnerguide/webhosting/6/1/what-is-web-hosting?.ws

Acronyms

CA	Communications Authority (Kenya)
CBO	Community-based organization
CEOP	Child Exploitation and Online Protection
CSAM	Child Sexual Abuse Material
CSEA	Child sexual exploitation and abuse
CSEM	Child Sexual Exploitation Material
DCI	Department of Criminal Investigations
DCS	Department of Children Services
ECPAT	Every Child Protected Against Trafficking (NGO)
GBV	Gender-based violence
GSMA	Global System of Mobile Communications Association
ICMEC	International Center for Missing & Exploited Children
ICT	Information and Communications Technology
INHOPE	The International Association of Internet Hotlines
ISP	Internet Service Provider
ITU	International Telecommunications Union
IWF	Internet Watch Foundation
KE-CIRT	Kenya Computer Incident Report Team
NCCS	National Council for Children's Services
NCMEC	National Center for Missing and Exploited Children
NECMEC	U.S. National Center for Missing & Exploited Children
NGO	Non-government organization
NPA	National Plan of Action to Address Online Child Sexual Exploitation and Abuse
OCSEA	Online child sexual exploitation and abuse
SOP	Standard Operating Procedures
TELCO	Telecommunications company
VAC	Violence against children

1. Introduction

Maestral International was contracted by UNICEF Kenya to support the Government of Kenya, in particular the Department of Children's Services (DCS) and the Communications Authority (CA), through the Technical Working Group on Online Child Sexual Exploitation and Abuse (OCSEA) to:

- undertake an assessment of the current national response to OCSEA using the WePROTECT Model National Response plan to identify gaps and new opportunities in implementation; and
- develop a National Strategy and Costed Plan of Action on Online Child Abuse and Exploitation that will guide partners in the areas of program intervention

This report summarizes the field research findings from consultations with key stakeholders in Kenya and the relevant findings from the desk review that precedes this report.[29]

1.1 Context in Kenya

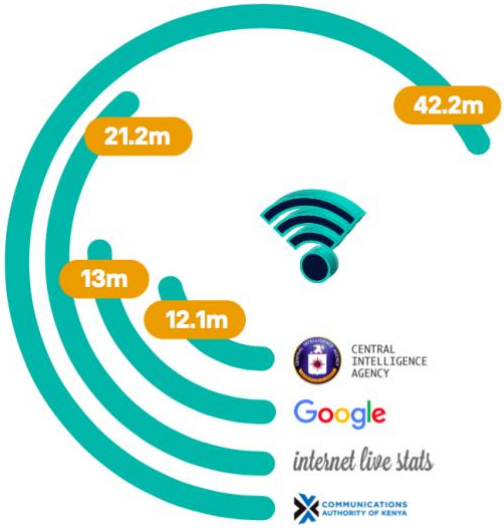
The online world is changing rapidly. In Kenya, internet is available widely, with three in every ten households having internet in the home. The Communications Authority of Kenya estimates that mobile use is currently at 100% with a total of 46.6 million subscribers[30]. The fast pace of mobile use has resulted in the increase of internet users. It is estimated that Kenya has experienced a 676% increase in internet use since 2005[31]. However, it is worth noting that the methodologies used to define and derive the number of internet users in Kenya has raised questions and double-counting and methodologies that sample from the population still leave questions as to the exact number of internet users countrywide[32]. The following is an illustrated overview of the various internet user estimates:

[29] Maestral International. (2019). *Desk Review: Assessment of the National Response to Child Online Sexual Exploitation in Kenya using the We Protect Model National Response framework.* Report submitted to UNICEF Kenya and Department of Children's Services, November 2019.

[30] Communications Authority of Kenya (2018). Third Quarter Sector Statistics Report 2018/2019 (July-September 2018).

[31] ECPAT International (2013). Understanding African children's use of Information and Communication Technologies (ICTs) – a youth-led survey to prevent sexual exploitation online

[32] Nendo (2019). The State of Mobile Data Insights & Highlights



Source: *The State of Mobile Data Insights & Highlights*

The findings of the KIHBS survey, released in 2018, show that three in every four individuals aged 18 years and above owned a mobile phone with an average number of 1.3 SIM cards per person[33]. Three in every ten households had internet connectivity and use of internet in mobility was reported as the most common place of use of internet. The internet was used mainly for social networking[34]. According to the Bloggers Association of Kenya (BAKE) State of the internet report 2017, WhatsApp has 12 million users, YouTube 8 million, Facebook 7.1 million users and Instagram at 4 million users.[35]

A report by Nendo, describes the "5 'S's of the Kenyan Internet"[36]:

- **Search** - Google is Kenya's most-visited website and most-frequently used search engine **Sport** - Sports betting company SportPesa has been the most "Googled" word by Kenyans every year from 2016 to 2018
- **Social** - Facebook is the second-most-visited website in Kenya and the largest social media site with over 8.5 million users
- **Sex** - Kenya has two adult websites in its top 10 most-visited sites. This is greater than any other East and Central African country
- **Stories** - The country has a growing appetite for content spanning news, entertainment and video. The vertical photo/video format of "stories" is also increasing in popularity

Most children in Kenya have access to the internet through a smart phone, tablet or computer (in or outside of the home).[37] Smart phones and home internet have become much more affordable; and online platforms, apps and games encourage online interaction.[38] Children learn new skills rapidly, and the internet provides visual and ready information for a tech-

[33] Kenya National Bureau of Statistics (2018). Kenya Integrated Household Budget Survey 2015-2018
[34] Ibid.
[35] BAKE (217). State of the Internet in Kenya
[36] Nendo (2019). The State of Mobile Data Insights & Highlights
[37] ChildLine KII, 09.03.2020; Small group discussion, 03.03.2020; desk review
[38] Small group discussion, 03.03.2020

savvy generation.[39] However, many do not have the information, knowledge or skills to keep themselves safe online, and recognize and respond to concerns. The online world is, for many parents and carers, a reality which they have little knowledge of, or do not have the capacity or time to monitor.[40] There are many opportunities for building children's knowledge of online risks and tools to stay safe online, including through schools, after-school groups and online itself.[41]

Online Child Sexual Exploitation and Abuse (OCSEA) includes: child sexual abuse materials (CSAM); live online child sexual abuse or live streaming; online grooming of children for sexual purposes; sexting; and sextortion. There are also other emerging cyber-related crimes such as cyber-bullying; online radicalization; children being addicted to pornography; identity theft/impersonation; and exposure to inappropriate content online such as gambling.[42]

There is already a lot of important work taking place to prevent and respond to concerns online. Kenya's development of a National Plan of Action against OCSEA (NPA) allows for the identification, coordination and collaboration of multiple stakeholders to create a more harmonized, complimentary and holistic approach that empowers children and all those who support them to use the internet safely and tackle OCSEA[43], as well as an opportunity to understand everyone's responsibility in keeping children safe online through an approach addressing both prevention and response to OCSEA.[44] The process, with the participation of a wide range of stakeholders, including children and young people, is a huge step towards having a skilled and resourced workforce, backed by clear legislation and guidance, to tackle OCSEA in ways that prioritize children's safety and well-being.[45]

It is vital that children can reap the benefits of the internet and uphold their right to access information,[46] whilst knowing how to stay safe online and report concerns and disclosures.[47] Focusing on OCSEA is vital, but there is also a need to look more widely, to include cyber-bullying and preventative strategies, such as awareness raising with children, parents/carers, the police and judiciary, teachers, social workers, faith leaders and the wider community.[48]

1.2 Development of Kenya's National Plan of Action to Address OCSEA

This report sets out the key findings from the initial desk review, key informant interviews (KIIs), national level stakeholder consultation in Nairobi and a consultation with Internet Service Providers (ISPs).

The key findings outlined in this report (as of June 26, 2020) are based on:

- 43 KIIs with NGOs, ISPs and Government between February and May 2020 *(see appendix A for a full list of KIIs to date)*

[39] Small group discussion, 03.03.2020
[40] The Office of the Director of Public Prosecutions, KII 03.02.2020; Directorate of Criminal Investigations (DCI), 05.03.2020
[41] Small group discussion, 04.03.2020
[42] Directorate of Criminal Investigations (DCI), 05.03.2020
[43] Small group discussion, 03.03.2020 and 04.03.2020; The Office of the Director of Public Prosecutions, KII 03.02.2020
[44] Directorate of Criminal Investigations (DCI), 05.03.2020
[45] Small group discussion, 04.03.2020
[46] KAARC KII, 18.03.2020
[47] Directorate of Criminal Investigations (DCI), 05.03.2020
[48] Watoto KII, 27.01.2020

- Two stakeholder meetings held in Nairobi on 3-4 March and 5-6 March 2020, coordinated by DCS, Terre des Hommes Netherlands (TdH NL) and UNICEF, with over 35 participating stakeholders organizations, bringing together key stakeholders including UN agencies, NGOs, government sectors, Kenya's specialist police force (Cyber Crime Unit), ISPs and Telcos *(see appendix B for meeting agendas)*
- A summary of the key elements of the desk review used to contextualize stakeholder observations
- A summary of responses by 151 respondents in a survey for the Department of Children Services staff countrywide
- Fourteen focus group discussions (FGDs) with children aged 13 to 17 years in Garissa, Kisumu and Mombasa in March 2021 with a total of 112 children
- An online survey administered to children aged 7 to 17 years that elicited ten responses.

Location	DCS	Gov't	NGO	ISP teacher	Training inst.	Teacher	Com memb.	Young person	F	M	Children 13-17 yrs	F	M
National	2	3	6	1	2				14	6	10		
Garissa	2	1	4			2	3	2		10	48	24	24
Kisumu	3	1	3			1				3	32	16	16
Mombasa	1									1	32	16	16
Nakuru			1						1				
Total	**8**	**5**	**14**	**1**	**2**	**3**	**2**	**2**	**24**	**20**	**112**	**56**	**56**

The report identifies key strengths and gaps in the response thus far and proposes recommendations that will inform the subsequent National Plan of Action Against OCSEA.

Constraints

The initial field research strategy included four week-long visits to Nairobi, Garissa, Kisumu and Mombasa counties, during which KIIs were to be conducted with parents and caregivers, community members, community-based organizations (CBOs), children and young people and (possibly) informal discussions with child survivors of OCSE. Prior to being able to conduct field research, Covid-19 emerged, and with it a number of restrictions, resulting in the team not being able to undertake the country and field research as planned. Maestral sought alternative methods to collect data, such as online surveys and virtual/phone interviews. Whilst several online surveys were developed, it was not possible to gather meaningful inputs from the following essential stakeholders, in part due to lack of ability to reach those not already in touch with NGOs or CBOs, and because the emergency response to COVID-19 superseded other activities, including participating in interviews:

- parents and caregivers
- community members, community leaders and CBOs

The following sectors were also difficult to secure adequate number of interviews with due to time, availability and COVID restrictions:

- Education sector

- ISPs
- Media and communications sector

The views of children and adolescents are fundamental to a robust national and local prevention and response to OCSEA. Although the initial plans to conduct an extensive participatory assessment exercise in four counties was not possible due to COVID-19 restrictions, it was considered imperative that their views did inform the NPA on OCSEA. In March 2021, twelve FGDs were held with children aged 13 to 17 years in Garissa, Kisumu and Mombasa. Additional FGDs were planned in Turkana but COVID-19 restrictions prevented them from taking place. Workshops with children under 13 years old did not take place due to (1) the content of the FGDs (2) the short amount of time remaining on the project to conduct these and (3) the continuing COVID-19 restrictions. An online survey was shared with multiple actors to access children's online views. Although there were few responses, the content of the responses was rich and has added to the data to inform the NPA.

The key findings are presented using the WePROTECT national model response *(see Appendix C)*,[49] looking at each of the different stakeholder groups in line with the research gathered through KIIs and face-to-face meetings.

The conclusion summarizes the key themes that cut across all stakeholder groups, using the WePROTECT enablers as a foundation stone, in the form of key findings and recommendations for development of the National Strategy and Action Plan.

2. Key findings in line with the WePROTECT national model response

2.1 Policy and Governance

Key findings from desk review

[49] The WePROTECT Global Alliance to End Child Sexual Exploitation Online (www.weprotect.org) is an international movement dedicated to national and global action to end the sexual exploitation of children online. The Kenyan government is an Alliance member. It has four key objectives:

1 Securing high level commitment by governments, the technology industry, international and national civil society organizations to tackling this crime
2 Support comprehensive national action through the We Protect Model National Response and the Fund to end violence against children
3 Galvanizing global action by catalyzing and driving critical interventions needed to end child online sexual exploitation
4 Strategy & governance, including securing a long-term future and a clear & stable governance structure.

- Legislation and policy can be divided into preventive and protective. (see Figure 1 below). [50]

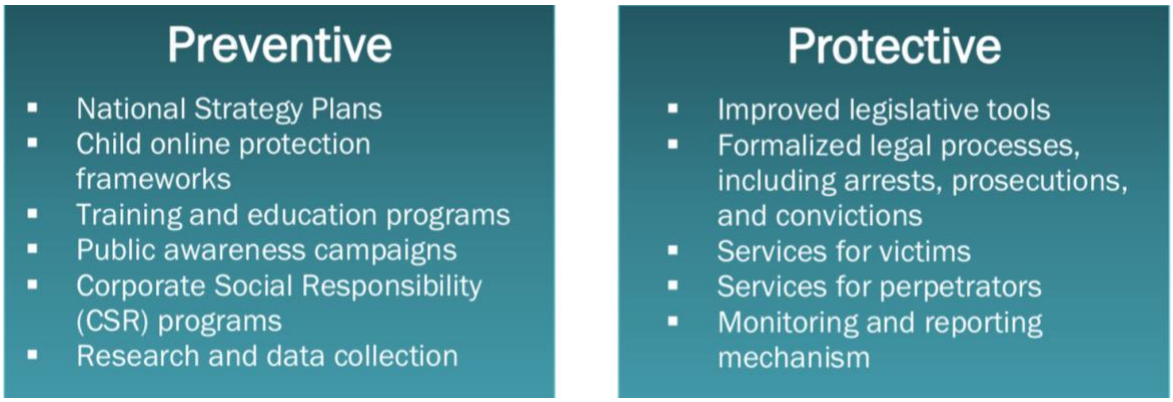


Figure 1 Child sexual abuse material - model legislation and global review, 2018

- Tackling OSCEA and CSAM requires a multi-faceted, cross-sectoral approach that includes both preventative and protective elements, based on an understanding of the role played by individual offenders, the individuals and groups facilitating the exploitation and, gender, social, cultural, economic and institutional constructs that contribute to creating an environment in which sexual exploitation of children is either ignored, tolerated, or even accepted".[51]
- Kenya's overall legislative framework sets out children's rights, through the 2010 Constitution and Bill of Rights, the Children's Act (2001), Sexual Offences Bill (2006), Employment Act (2007), Victim Protection Act (2014), Cybercrimes and Computer Misuse Act (April 2018/March 2020), Kenya Information and Communications Act, CAP 411 A (revised 2015), and the Kenya Information and Communications Amendment Bill (July 2019). The draft amendment to the Children's Act, (Draft Children's Bill, 2018) specifically mentions OCSE and CSAM, although not yet enacted.
- Kenya is compliant with legislation on CSAM (has specific legislation, defines CSAM, recognizes technology-facilitated CSAM and simple possession offences), with the exception of legislation requiring ISP reporting.
- As with all laws and policies, it is essential to provide sufficient resources to translate policy into action. In the case of OCSEA, there is a particular need to have robust and up-to-date capacity in country. Identifying, apprehending and sentencing perpetrators is extremely challenging due to the multiple platforms available to them, various ways of being anonymous online, the use of encrypted identities, currency and websites, and the vast number of perpetrators globally. An additional challenge is that a website can be hosted in one country, the abuse take place in another, and then accessed and shared in multiple countries. To increase the identification of victims, more resourcing must be put into law enforcement to enable them to specifically address this.[52]

Findings from consultations

Legislation and policies

[50] International Centre for Missing and Exploited Children, 2018, Child sexual abuse material- model legislation and global review
[51] IAWG, cited in ECPAT, 2018, Demand summary paper 1: Defining the demand for the sexual exploitation of children, p.4
[52] Interpol & ECPAT. (2018). *Towards a Global Indicator on Unidentified victims in Child Sexual Exploitation Material.*

The Cyber Crime and Computer Misuse Act of 2018 is a huge step forward in tackling OCSEA, as it explicitly addresses child pornography, cyber stalking and cyber bullying. However, gaps remain in legislation, such as recognizing and responding to grooming,[53] having no clear legislation that regulates cyber cafes and video dens in some counties, and having a harmonized legislation and guidance framework to address both gender-based violence (GBV) and OCSEA.[54,55] See appendix D for a summary of the relevant legislation and policies.

Translation of legislation relating to OCSEA into implementation remains a challenge[56] and there is need for more inter-departmental collaboration within government departments and sectors.[57]

- The coordination of policy and procedure on OCSEA is currently primarily at national level, and there is a gap between national and county levels, where implementation of legislation occurs.[58] To bridge this implementation gap, it is essential that there is a sufficient, allocated budget for OCSEA to develop good practices and enable them to be applied across the country.[59]
- It is important that all relevant stakeholders are aware of existing legislation, understand it and how to use it to support children and tackle OCSEA.[60] Improved implementation requires that all relevant stakeholders understand the legislation and how to apply it in practice.[61]

Priorities identified by stakeholders to enhance legislation include:

- Create more awareness of relevant legislation and build capacities of key duty bearers to implement existing legislation
- Enactment of the draft amendments to the Children's Act
- Implement the Cybercrimes and Misuse of computer Act
- Introduce more child-friendly justice procedures

Child consultations did not explicitly focus on legislation and policies, but a number of relevant recommendations were made:

- Children thought that the following safety measures should be in place: better filtering of inappropriate and illegal content, including blocking certain websites and apps (Phoenix was named) "Ban apps that mislead and entice children online" and content (such as inappropriate content on YouTube)
- Legislation that would enforce restrictions on apps such as age, locking accounts of those who perpetrate OCSEA, having more apps that are educational for children and providing forums to educate parents, caregivers and other stakeholders
- regulating where children access the internet, especially cybercafes, was seen as important.

[53] ECPAT KII, 27.01.2020
[54] KAARC KII, 18.03.2020; Small group discussion, 04.03.2020
[55] TdH NL(2018). The Dark side of the Internet for Children
[56] African Institute for Children studies (AICS), meeting 03.03.2020
[57] Small group discussion 04.03.2020
[58] The Office of the Director of Public Prosecutions, KII 03.02.2020
[59] African Institute for Children studies (AICS) meeting 03.03.2020
[60] ACHTPCU meeting, 05.03.2020
[61] The Office of the Director of Public Prosecutions, KII 03.02.2020; ECPAT KII, 27.01.2020; KAARC KII, 18.03.2020; African Institute for Children studies (AICS) meeting 03.03.2020

2.2 Criminal Justice

Kenya became the first country in Africa to set up a specialist branch of the police to specifically focus on OCSEA. The Anti-Human Trafficking and Child Protection Unit (AHTCPU) Cyber Unit operates under the Directorate of Criminal Investigations (DCI). The unit in Nairobi opened in 2019, and the Mombasa unit was launched in March 2020, with a third planned in Kisumu. The AHTCPU investigates reports of both offline and online child sexual exploitation and abuse, advises other officers across Kenya on OCSEA investigations, takes on OCSEA cases reported to other police stations but that have been poorly investigated, coordinates with Interpol, and liaises with the children's department and other non-state actors in identifying and rescuing sexually abused children.

The AHTCPU is equipped with some hi-tech tools and expertise to remove child abuse material from view, identify survivors and locate and arrest the offenders. Kenya is the first African country to be linked to Interpol's ICSE database and the International Victim Identification network which helps identify child victims and perpetrators. So far in 2020 there have been seven court cases and 15 active investigations.[62] However, a country-wide data management system is important in order to be able to mine existing databases for information to support investigations.[63]

There is a DCS officer seconded to the AHTCPU and the unit strives to partner with specialist agencies so that cases are reported to, and followed up by the Cyber Unit. [64] This includes KE-CIRT (Kenya Computer Incident Report Team), the Department of Children Services, and the National Center for Missing and Exploited Children (NCMEC) Cyber Tip Line. The unit requires more resources, as the demand in high, to increase their operational capacity, and in further building the capacities of staff.

The field research findings on **training needs for the criminal justice sector** noted that, while there has been some training provided, it is not across the board, and it is often ad-hoc.[65] For example, Watoto delivered training before the first OCSEA arrests in 2019 to prepare prosecutors for understanding the cases put before them, and the AHTCPU received training from Interpol. Where training had occurred, this was often offered to only one police officer in the Gender Protection Unit, resulting in loss of knowledge when that police officer is transferred or leaves the post.[66] However, there is a need for systematic capacity building of the police force as a whole and to develop a plan to retain and build on knowledge, particularly specialist knowledge for the AHTCPU, such as victim identification.[67] Informants noted a need for coordinated training on OCSEA and relevant legislation, for police and judiciary, [68] and for combined training of multiple stakeholders in order to investigate and prosecute OCSEA. [69]

[62] NFR Stakeholders meeting March 3-6, 2020
[63] Small group discussion 04.03.2020; ACHTPCU meeting, 05.03.2020
[64] ChildLine KII, 09.03.2020; ECPAT KII, 27.01.2020; Watoto KII, 27.01.2020; Small group discussion, 04.03.2020
[65] ChildLine KII, 09.03.2020; The Office of the Director of Public Prosecutions, KII 03.02.2020
[66] ACHTPCU meeting, 11.03.2020, Kisumu KII 17.04.2020
[67] ACHTPCU meeting, 11.03.2020
[68] ECPAT KII, 27.01.2020; KAARC KII, 18.03.2020; The Office of the Director of Public Prosecutions KII, 03.02.2020; small group discussion 03.03.2020
[69] Small group discussion, 04.03.2020

A lack of knowledge across the wider justice system has resulted in reports of both the police and judiciary not understanding the severity or impact of OCSEA due to (often) the lack of physical contact with a child. For example, if OCSEA is reported to the police (not the AHTCPU), there may be problems when filling out charge sheets as police officers are unsure of what the crime is if there is no contact.[70] If the police do not recognize OCSEA as a serious crime, there is a risk that they will not respond appropriately, follow up or conduct a thorough investigation.[71] "If you go to a police station and report OCSEA it is unclear where/how the police take action."[72] This in itself has resulted in a very high case load for the AHTCPU, further stretching its resources and staff. Often, a combined lack of knowledge about OCSEA in both police officers and child protection professionals reduces the likelihood that OCSEA will be identified and referred across the two sectors.[73]

During a training of trainers of prosecutors, most prosecutors were surprised when they realized what goes into an investigation on OCSEA – their perception was that if there was nothing physical taking place, it is not valid as an offence under the sexual offences act. Due to this lack of knowledge, OCSEA is given less importance, as the crime is too far removed, in a virtual reality, and they do not fully realize the impact and consequences of the offence on a child.[74] The judiciary needs to appreciate what cybercrime is, or understand why the prosecution needs more time for investigations, why they need to review victims' or perpetrators' Facebook posts, and grant the orders to do so, and why it needs to be done with speed.

As is the case with all frontline workers, it is important that the **police and judiciary are given support** to deal with the intense emotional pressures faced when dealing with OCSEA. Investigating child sexual exploitation and abuse cases, and the prolonged, chronic and ongoing exposure to potentially traumatic incidents and CSAM materials, can cause high levels of stress and anxiety, burnout, leading to secondary traumatic stress (the emotional response experienced when an individual is exposed to the first hand trauma of others), which can also place someone at risk of developing post-traumatic stress disorder. While counselling services have been extended to parts of the public sector, it is not provided for within the police service. Officers have been referred for counselling services but are having to pay for this service out of their own pockets.

Observations from the field research also relate to the need to **review and refine existing prosecution measures**. Prosecution of perpetrators is challenging because: (1) evidence that is admissible in court is difficult to obtain and often requires covert investigations with cooperation from multiple countries; court orders to seize evidence can take time to process, and despite a loose collaboration with ISPs there is often a delayed response on data requests to them, which can prevent access to the evidence required to investigate and prosecute;[75] (2) the preparation of cases takes months or years; (3) most survivors wish to remain anonymous, resulting in cases being unable to go through the legal system;[76] (4) those that

[70] ChildLine KII, 09.03.2020; KAARC KII, 18.03.2020; Office of; ACHTPCU meeting, 11.03.2020
[71] The Office of the Director of Public Prosecutions, KII 03.02.2020
[72] ECPAT KII, 27.01.2020
[73] Kisumu KII, 15.04.2020
[74] The Office of the Director of Public Prosecutions, KII 03.02.2020
[75] ACHTPCU meeting, 05.03.2020
[76] ChildLine KII, 09.03.2020; The Office of the Director of Public Prosecutions, KII 03.02.2020

do go to court often fail to prioritize the well-being of child witnesses.[77] And whilst the system tends to be more perpetrator-focused than survivor-focused, the process still results in many perpetrators being able to continue to offend.[78] For example, cases are prosecuted using the same procedure as contact cases and the perpetrator may be granted bail.[79] Where the perpetrator is the parent or caregiver, and the case does not get reported or progress, the child remains at risk of daily abuse. Where a case is progressed, attention must be given to making sure the child is in a safe environment with the minimal amount of disruptions to their everyday life (for example, being able to attend school if it is safe to do so), otherwise they become a victim of the system for a second time (re-victimization).[80] This point highlights the need for a coordinated response across criminal justice and child protection and other sectors.

Children outlined the need for better enforcement of legislation by the criminal and justice systems: - "Enforce law on online content and how to handle it"; "Arrest and charge those who abuse children online", and specific policies that enable children to stay safe online - "Come up with policies that limit children's access to so much information".

One of the most challenging issues is **handling cases where the perpetrator is a child**, as the law requires both survivor and perpetrator to be treated as children.[81] Another challenging situation is where adults use older children to gain access to younger children, so that older children are inadvertently involved in grooming other children whilst being groomed themselves.[82] Overall, **perpetrator rehabilitation requires more focus within the response**. Effective perpetrator rehabilitation includes the development of rehabilitation tailored to online offending, and clear guidance on how to manage and support ex-offenders once they have served their sentence.[83] While sexual offenders are meant to be monitored by the police for five years from their release date, there is limited capacity to put this into practice effectively. It is questionable whether prisons communicate to the police when offenders are released, and whether police then have capacity to monitor.[84] During the data collection there were conflicting views on whether the sexual offenders register should be made public, and this will require more consideration.[85]

The data collection highlighted the need for investing in training, effective prosecution and support systems so that the AHTCPU can have sufficient reach and capacity and the wider police force has received adequate training to act on OCSEA reports and properly investigate. This is necessary if the criminal justice system is to have the capacity to respond to OSCEA reports in line with best practice.

2.3 Survivors and potential child victims

Key findings from desk review

[77] Small group discussion 04.03.2020
[78] ChildLine KII, 09.03.2020
[79] The Office of the Director of Public Prosecutions, KII 03.02.2020
[80] The Office of the Director of Public Prosecutions, KII 03.02.2020
[81] Eveminet Communications meeting, 05.03.2020; small group discussion 04.03.2020
[82] Small group discussion 03.03.2020; KII Kisumu 16.05.2020
[83] Small group discussion 04.03.2020; 05.03.2020
[84] Small group discussion 04.03.2020
[85] Small group discussion 04.03.2020

- A large number of children – 55% - have accessed adult pornography online, the largest percentage of a five-country survey;[86]
- Kenya has many of the drivers that have been identified in other countries, notably economic drivers such as poverty and economic inequalities, migration to hotspots areas in search of livelihoods such as urban areas, tourist locations and industries and; social drivers such as disruption in supportive family and home environments, violence against children, cultural norms and traditional gender roles; [87] and insecurity. Hosting of large number of vulnerable refugee populations including unaccompanied minors, and economic marginalization of certain geographic areas in the country;
- Globally, between 2006-2014, almost two thirds of the children identified as victims of OCSEA were female, and since 2010, the number of self- taken images each year exceeded more than 40% of the total number of images identified by Interpol.[88]
- The abuse of the one third of global OCSEA victims who are male tends to be more violent.[89]
- The global trend is difficult to track but it appears that the current trends in OCSEA and CSAM include an increased demand for violent material,[90] and an increase in demand for images and video of pre-pubescent children.[91] A significant majority of CSAM are of pre-pubescent children. In the US, in 2015 almost two-thirds (64%) of online images were of pre-pubescent children, 9% were of infants and toddlers, and 27% were of pubescent children. These figures are similar in a study in 2017 by INHOPE.[92]
- Most online abuse is of a single victim, rather than a group.[93]
- The impact of COVID-19, with more children online, has seen an 106% increase in NECMEC registered reports of suspected OCSEA in March 2020, compared to March 2019; a 200% increase in posts registered by Web-IQ (specialist cyber security company) on known sexual abuse forums linked to downloadable images and videos hosted on the Clearnet between February 2020 – March 2020; a reduction registered by the IWF in the number of URLs taken down after being identified as CSAM between March 16 – April 16 Isolation measures have increased the difficulties in processing reports of online abuse. In Kenya, as a proxy indicator, the National Council on the Administration of Justice, in their April 1st, 2020 press statement, highlighted a 35.8% increase in sexual offences reported in the month of March, immediately following the restrictions announced by the Government

Findings from field research

The findings are separated into perspectives of children and then perspectives of other key informants.

[86] ECPAT International (2013). Understanding African children's use of Information and Communication Technologies (ICTs) – a youth-led survey to prevent sexual exploitation online

[87] ECPAT International (2013). Understanding African children's use of Information and Communication Technologies (ICTs) – a youth-led survey to prevent sexual exploitation online

[88] Quayle, Jonsson, Cooper, Traynor and Svedin (2018), Children in Identified Sexual Images – Who Are they? Self- and Non-Self- Taken Images in the International Child Sexual Exploitation Image Database 2006–2015, quoted in ECPAT, 2018

[89] Interpol & ECPAT. (2018). *Towards a Global Indicator on Unidentified victims in Child Sexual Exploitation Material.*

[90] ECPAT, 2018, Trends in Online Child Sexual Abuse Material

[91] ibid

[92] INHOPE, 2017, 2016 Annual report

[93] ibid

Children confirmed that they have widespread online access. FGDs with feedback from both boys and girls (whose perspectives were the same and so have not been disaggregated in this report) reported that:

- Most children who participated in the FGDs said they mainly use the internet in cyber cafes, though some buy bundles of data for smart phones (theirs, their friends' or their parents'), use a computer or laptop at home and at school. Children said COVID-19 has greatly increased children's access to the internet as they now have computers and/or smartphones in order to engage in online learning - "Most of the children had access to smart phones because online learning required them to have smart phones". Many participants said that they and their friends have webcams.
- Most children said they regularly use YouTube, Facebook, Messanger and Instagram. SnapChat and TikTok are also popular; other named apps include Omegle, Likee, Phoenix, Twitter, Telegram, Opera Mini, IMO and online games.
- The importance of online platforms for showcasing talents and making money through getting subscribers or followers was cited by several participants.
- Children noted that the internet has provided the opportunity for online learning and revision, keeping in contact with friends and making new ones, keeping them entertained including online gaming and skills development, enabling them to showcase and develop talents such as comedy and dance, and earn money through having subscribers, followers, likes and comments.
- Participants outlined a variety of perceived risks of being online, including addiction to the internet, keeping children away from their studies, wasting time and affecting sleep. Online bullying was highlighted as a key risk - "If you upload something onto a platform and get negative comments it gives emotional disturbance and can lead to suicide and mental health problems" and linked to this, having reputation damaged online - It ruins your reputation if you make friends who eventually turn their backs on you".

The feedback from adults noted the following information:

All children are at risk of online abuse and exploitation, but some are more vulnerable. Children with disabilities and special needs can be more vulnerable online because they can look for (and find) less prejudice, more acceptance and more friendships online. [94] Consideration must be made of the potential radicalization of children online, particularly those who are vulnerable because they have a lack of recognition or validation in the home.[95] Other children more exposed are those who use computers, tablets and/or phones without supervision, site blockers or firewalls – they are using the internet without appropriate safeguards in place.[96] These risks occur both when children have their own phones, tablets and laptops, or borrow an adult's.[97] Some adolescent girls rely on boyfriends, often older men, for receiving phones and/or data,[98] and hide it at their neighbours place using it without

[94] Small group discussion, 03.03.2020
[95] KAARC KII, 18.03.2020
[96] ChildLine KII 09.03.2020; ECPAT KII, 27.01.2020
[97] ECPAT KII, 27.01.2020
[98] Dadaab KII, 30.04.2020

the knowledge of the parent[99]; and are tempted to share intimate photos via phone or online in return for money or goods.[100]

One group of children felt to be at greater risk of OCSEA was the group of boys and girls who do not transition to secondary school after standard 8, especially poor or vulnerable children.[101]

Children living in or from refugee and displaced communities are reported to face particular risks of OCSEA, either arriving in Kenya due to online trafficking, or exposed to OCSEA on arrival. [102] *"Some children are trafficked to Nairobi on promise they will be given work, and end up being exploited. There are many young girls crossing over from Somalia, when they are intercepted we are told that people lured them online and told that when they arrive in Kenya they would be married, but they end up as commercial sex workers."*[103] *"I know girls who end up trusting men who are abroad because they're sent money. They ask for photos of their naked privates. The girls are coerced and eventually share the photos only to have them blackmailed."* Issues of blackmail after sharing pictures was mentioned by several informants.[104] One project is supporting adolescent single mothers: *"They have varied nationalities – south Sudanese, Ugandans, Somalis - but there is a common story amongst them. They met their husbands or boyfriends over internet or social media. Some they went into relationships because someone promised to buy them a phone. The perpetrators desert or divorce them once they get pregnant and they are left with a lot of burdens on their own."*[105] The potential risks are increased because of the large numbers of unaccompanied separated children who are not registered as refugees on arrival in Kenya and are less likely to be in contact with service providers.

Trafficking is not only a challenge in refugee communities but in other large urban areas or areas of significant mobility. *"OCSEA borders child trafficking. Children are trafficked online. You can't separate these two issues, they are closely linked."* [106]

Children often raise concerns about cyber-bullying with specialist NGOs. Most children do understand what is involved and what the risks are. However, children are less aware of the potential risks of sexual issues online. Children are reportedly widely engaged in 'online dating' (a term used by children).[107] Children also do not view online grooming as abuse because there is no physical touching that takes place.[108] Some children then go on to meet the person doing the grooming (perpetrator, usually an adult) in person. Online grooming was the biggest reported OCSEA concern by children to ChildLine in 2019.[109]

All children interviewed in the FGDs and online survey were aware of OCSEA risks, as well as wider online risks such as early exposure to relationships, hacking, cybercrime, involvement

[99] KII Kisumu 15.04.2020
[100] Dadaab KII, 22.04.2020
[101] Dadaab KIIs, 14.04.2020 and 30.04.2020
[102] Dadaab KII, 14.04.2020
[103] Dadaab KII, 15.04.2020
[104] Dadaab KIIs, 14.04.2020 and 22.04.2020
[105] Dadaab KII, 22.04.2020
[106] Mombasa KII, 17.05.2020
[107] Watoto KII, 27.01.2020; small group discussion 03.03.2020
[108] KAARC KII, 18.03.2020
[109] ChildLine KII 09.03.2020; small group discussion 03.03.2020

in drugs, joining cults and blackmail - “Some ladies trap you by use of messages and photos and even photo-shop as evidence of you being responsible for their pregnancy”. Whilst some children referred more broadly to OCSEA as “exposure to negative information” and “bad things”, many were aware of specific risks including online ‘predators’ – “the possibility of someone taking naked pictures and putting them on Facebook and WhatsApp”; “[children are] told to text personal information then they ask you to meet with them then they kidnap you”. Participants also cited pop-up pornography and sexual videos, ‘bad companies and ISPs’, account hacking to groom and blackmail, child sexual abuse material (CSAM). One participant noted, “It makes children know more things than adults” whilst another said “Most of the parents don’t have control of their children online”.

Some informants directly involved in working with children on OCSEA issues noted that, whilst there are some awareness-raising efforts with children, these do not tackle wider internet issues such as cyber-bullying. More needs to be done on issues such as sexting, sextortion, posting and grooming.[110] As the children’s feedback shows, the risks are being widely felt.

The online survey highlighted the high levels of exposure. Half of the respondents said they have engaged with a stranger online and one person said their friend had. Two said they mainly do so through online gaming. Whilst half have never seen anything that upset or worried them on the internet, the other half have seen inappropriate images of adults, 40% have also seen inappropriate images of children and 30% have been bullied online. One participant said they have been asked for inappropriate images of themselves and had sent them.

A link was noted between children who are accessing the internet for shopping or using online lending platforms and trading websites, that are often not credible. Children may be tempted to share personal data.[111] “Just by having access to internet and visiting sites she’s not prepared for e.g. dating sites, this sets her for a whole spectrum of violence and abuse in her life.”[112] In FGDs with children, the potential for ‘making money online’ was cited many times as a positive.

Children were reported as facing risks not only of OCSEA but online radicalization, and the challenges were similar – limited parental knowledge or engagement, broader social and economic pressures.[113]

Gender perceptions play a role in how OCSEA is viewed and responded to - there is a common assumption that girls are more at risk, whereas concerns about boys are downplayed because it is assumed that he will be ok.[114] Most cases reported to Childline thus far are female. However, it is important to note that boys may be less likely to talk about concerns or only share with their peers.[115] Boys tend to play games online more frequently whereas girls tend to look more at fashion, giving signals to predators online and making it easier for them to be

[110] Watoto KII, 27.01.2020; small group discussion 04.03.2020
[111] Dadaab KII, 22.04.2020; OCSEA Stakeholder meeting 03.03.2020
[112] Dadaab KII, 21.04.2020
[113] Dadaab KII, 21.04.2020; KII Garissa 18.04.2020
[114] ECPAT KII, 27.01.2020; The Office of the Director of Public Prosecutions, KII 03.02.2020
[115] ChildLine KII, 09.03.2020; small group discussion 03.03.2020

groomed.[116] Kenyan society tends to be stricter about girls' behaviours and freedom of movement and tend to think boys are less vulnerable both online and offline, so possibly boys are also vulnerable as they are less monitored.[117] One frontline worker reported that only in few situations had he encountered boys who were abused; it was more common for boys to be introduced to pornographic content, by adults showing them material but then the adult does not proceed to abuse the boys, though the, boys themselves go and abuse girls their own age.[118] Interestingly, analysis of the feedback from the twelve single-sex focus group discussions with children in Garissa, Kisumu and Mombasa found that their responses and experiences were very similar.

Several key informants noted that (usually) girls are using online platforms to share their photos with potential abusers. Sometimes girls are asked or encouraged to share intimate photos. *"A common practice is to see a big group of young girls in hotels taking selfies for their "friend" outside the country, and there has been instances of sharing pornographic photos."*[119]

A concern noted by more than one informant was the link between phone access and transactional relationships, with phones and data being a 'gift' from boyfriends.[120] concern noted for the refugee Somali community is the practice of "Occasional marriage", in which a man from the diaspora connects with girls as young as 14 years, through online platforms, or sometimes collected via a woman who is paid to collect the girl from the refugee camp, or urban areas, and then officially married by a religious leader. The illegal 'marriage' happens during the months of July to August (summer holidays for the diaspora man coming from Europe or North America), the couple stay in a room together in Nairobi, for three months, and then the man returns to his own country, leaving the girl abandoned. Informants noted many of these cases, which almost always go unreported.[121] Another key informant noted that marriage with a potential husband abroad was sometimes brokered by parents for money.[122]

An area of concern that was raised by multiple informants is concern over the widespread access to and related risks of pornography. It was noted that a recent report on the use of school computers found that a lot of school computers are being used for watching pornography, as well as for gambling.[123] Children were observed to be accessing inappropriate content due to peer pressure to view CSAM, adult pornography or other inappropriate material online.[124] *"Not all kids have a mobile, but there will always be someone with a smart phone, so you see them in groups by the football pitch, ages 14-18."*[125]

There were reports of gangs using online platforms for better communication, and videoing initiations which could involve rape of girls (some of whom are also gang members).[126] Some gangs also have online profiles on Facebook and Instagram, but though these have been

[116] The Office of the Director of Public Prosecutions, KII 03.02.2020
[117] ECPAT KII, 27.01.2020
[118] KII Kisumu 16.04.2020
[119] Dadaab KII, 15.04.2020
[120] Dadaab KIIs, 15.04.2020 and 30.04.2020
[121] Dadaab and Garissa KIIs, 15.04.2020
[122] Dadaab KII, 30.04.2020; KII Garissa 18.04.2020
[123] Eveminet Communications, meeting 05.03.2020
[124] ChildLine KII, 09.03.2020
[125] Dadaab DCS KII, 15.04.2020
[126] KAARC KII, 18.03.2020; KII Nakuru 2020

reported to the police and online platforms, to date (at the time of interview) these had not been responded to.[127] Children are also putting themselves more at risk through getting tattoos on parts of the body that are usually not exposed. The tattoo studio takes photos of their art and their [under 18] clients, and post the images on Facebook – identifying them in person. This puts children at risk of identification, stigmatization, shaming and makes them more vulnerable to grooming, sextortion, cyberbullying and online abuse.[128]

The field research highlighted children's low levels of awareness of the risks posed by the internet, and limited knowledge about what to do. Most children are currently not empowered to protect themselves, do not know what online behaviours are illegal, and do not know how to get support or report concerns/disclosures.[129] This finding was partially endorsed by feedback from the children's consultation, although children confirmed widespread use, awareness of some of the risks and a desire for more support to stay safe. Many children were unaware of the safety measures in place to protect children online. Some of the measures outlined included reporting to a responsible adult including the police, changing settings to be the most secure they can be and setting passwords, and parental control of what children look at online. Children were also aware they can access support numbers, counselling and guidance. Not going to 'bad sites' was also discussed as a safety measure. Children did also note that they thought that their parents were unlikely to know what was going on: "most of the time we use the internet without their [parents'] knowledge."[130]

Support services and referral to services

One gap noted by stakeholders is understanding the needs of child survivors and knowing what to do to support them. Survivors of OCSEA require specialist support and interventions. Comprehensive survivor services are crucial, applying a case management approach in supporting children from identification through to case closure. Training and resources for child support services is essential. Service providers implementing support services for children have not yet been trained on OCSEA or developed programs that address the issue holistically, so there is often not high quality, tailored support services available to survivors.[131] Many in the social service and child protection sector are less informed of OCSEA than other forms of abuse, despite a big increase in knowledge since 2017.[132] A lack of support has resulted in cases of children committing suicide after reporting.[133] Tailored support can lead to an increase in reporting because children know their concern is taken seriously and they will be safeguarded.[134]

Children in FGDs brought up the need for emotional support, although no children surveyed or interviewed reported accessing this support themselves: And the need for improved

[127] KAARC KII, 18.03.2020
[128] KAARC KII, 18.03.2020; The Office of the Director of Public Prosecutions, KII 03.02.2020
[129] ECPAT KII, 27.01.2020; ChildLine KII, 09.03.2020; ILab meeting, 05.03.2020; The Office of the Director of Public Prosecutions, KII 03.02.2020
[130] FGD with children, see summary report Appendix F.
[131] ChildLine KII, 09.03.2020
[132] ECPAT KII, 27.01.2020
[133] ECPAT KII, 27.01.2020; The Office of the Director of Public Prosecutions, KII 03.02.2020
[134] The Office of the Director of Public Prosecutions, KII 03.02.2020

victim/survivor support throughout the judicial procedure was highlighted: “Offer free legal support to children who are abused by the perpetrators”; “guidance and counselling”.[135]

Reporting

This results in many cases not being reported.[136] Even where children do want to report, procedures are unclear to both children and adults.[137] Reporting levels will remain low until a clear, easy-to-use procedure understood and used by children is in place.[138] Children have also said they feel guilty for reporting and do not receive support to help them cope with these feelings, or with any trauma they have experienced.[139]

Confusion around reporting, and reluctance to report was highlighted by children. Most FGD child participants said that they would report online concerns to a teacher; some said they would talk to the police, parents, the child rights officer in the community, relatives, a neighbour, the village elder, church elder, friends - “We find it easy to deal with our peer groups or friends instead of reporting to any authority”; “Most youths tend to confine and confide with friends and peers. They are not ready to share with friends and guardians, teachers, sheiks, preachers. This is because older people perceive us as criminals whilst using the net.” Child FGD participants noted the following barriers to reporting abuse and/or exploitation

- fear of parents’ responses was the highest, with children reporting fear of punishment - “When the parents are strict, instead of helping you they decide to punish you. This may prevent reporting”- including blaming the child - “Fear that when they tell parents they will be thoroughly beaten and get accused of watching pornography” or thinking ‘ill’ of them and potential consequences- “If I tell my mother she will take away the phone”.
- threats/blackmail from the perpetrator was the second highest reported barrier - embarrassment and ‘loss of dignity’, “fear my reputation might be ruined”
- One child reported that the “harshness and strictness of parents, police and public” prevented them from reporting
- Someone else said “Friends tell you not to report”.
- Another issue was the fear of losing a sponsor who the child perceives will change their life for the better.[140]

Currently, reporting procedures from community to service providers are unclear. Where individuals have a personal contact within the DCI they feel more able to report.[141] The Communications Authority Kenya has a web page where OCSEA can be reported and people are learning to report via Twitter and Facebook and tag the DCI AHTCPU, which then responds more quickly.[142] However, AHPTCU are receiving reports directly to their personal phones, which is unsustainable. There is an upward trend of adults reporting OCSEA but still very

[135] FGD with children, see summary report Appendix E.
[136] ECPAT KII, 27.01.2020
[137] ECPAT KII, 27.01.2020
[138] ECPAT KII, 27.01.2020
[139] Watoto KII, 27.01.2020; The Office of the Director of Public Prosecutions, KII 03.02.2020
[140] FGD with children, see summary report Appendix E.
[141] ECPAT KII, 27.01.2020; Watoto KII, 27.01.2020; small group discussion 03.03.2020
[142] Watoto KII, 27.01.2020

minimal reporting from children.[143] Without a clear, country-wide reporting procedure, under-reporting will continue.[144]

Emotional Counseling

Some specialist organizations such as Childline offer free/low cost counselling for the survivor and, where needed, the family and school class (if children in school have also been affected). However, counselling is expensive and families cannot afford it.[145] There is a survivor support fund,[146] and a key survivor helpline is ChildLine 116.

Social services and child protection workforce

DCS has an important role to play in coordinating action on OCSEA and ensuring all partners and stakeholders are engaged. At county and sub-county levels, they have an important role to raise awareness, identify OCSEA, refer cases and ensure effective case management of victims/survivors. There is need to build capacity of country and sub-county DCS staff on OCSEA, roll out case management system, and strengthen referral pathways. Furthermore, the social service workforce for child protection needs to be adequately resourced to prevent and respond to OCSEA and wider child protection issues in general. Standard Operating Procedures should take into consideration OCSEA.

Informants highlighted capacity constraints locally, due to limited numbers of children's officers and, in some locations, few or no CBOs supporting child protection; as well as ongoing challenges with cultural acceptance of harmful cultural practices, limiting ability to ensure outreach and response.[147] In this context, addressing OCSEA is most effective within the context of strengthening the broader child protection system.

It is important that frontline social workers are given support themselves. For example, ChildLine provides mandatory counselling to the counsellors. This means that counsellors have sufficient support to be able to help children. There is also a briefing session at the start and end of each session. However, this is not practiced in all organizations or in the public sector, and is heavily dependent on funding.[148]

The voice of the survivor is key to the development of an effective strategy and national action plan. There are specialist NGOs and CBOs who work with survivors and support them to tell their stories whilst prioritizing their safety and well-being.[149] However, there needs to be more done to empower children to advocate for their right to be safe online.[150]

2.4 Social awareness and action on OCSEA

One of the key challenges outlined by several key informants is a general lack of awareness about OCSEA amongst children, parents and caregivers, faith and community leaders, teachers and some social workers. Whilst there are some initiatives to raise awareness, their

[143] Watoto KII, 27.01.2020
[144] ECPAT KII, 27.01.2020
[145] ChildLine KII, 09.03.2020; ECPAT KII, 27.01.2020; KAARC KII, 18.03.2020; Small group discussion, 04.03.2020
[146] Directorate of Criminal Investigations (DCI), 05.03.2020
[147] Garissa County KII, 15.04.2020
[148] ChildLine KII, 09.03.2020; KAARC KII, 18.03.2020
[149] ECPAT KII, 27.01.2020
[150] ECPAT KII, 27.01.2020; KAARC KII, 18.03.2020; small group discussion 04.03.2020; Code IP Trust, 05.03.2020

coverage is not country-wide and they are dependent on donor funding; and those living in cities tend to be better informed.[151]

Eighty percent of children in the online survey felt that the community and religious leaders could do more to educate children on internet safety, 60% felt community and religious leaders could help them set up blocks and learn about the risks themselves and 50% said they wanted leaders to teach parents about internet safety, monitor public computers and support children to teach their parents about online safety. There were similar responses for the role teachers can play, though 90% felt that teachers need to learn more about internet safety so they can better protect children. 90% felt that if they know more about internet safety themselves, they can better support their friends to stay safe online. 70% also felt this will help them to set up blocks, educate their friends and know how to report concerns.

Some key informants noted that OCSEA also links to the broader child protection challenges in communities, in which cultural norms and taboos prevent discussion of risks. In contexts in which norms around child marriage are not challenged, unsafe online activity is normalized.[152] Informants noted that community leaders would tend to 'cherry pick' the OCSEA issues that they wished to engage with, supporting restrictions to early exposure to sexual content, for example, whilst condoning or sometimes facilitating online access to early marriage.[153]

Effective outreach in communities, including to parents and caregivers, allows for in-depth discussions around key issues such as taboos of talking about sex and can bring about long-term behavior changes.[154] Some NGOs and CBOs work on keeping children safe online and there have been several campaigns however, these need to be more regular, through more collaborative cross-sector partnerships.[155] Informants noted the importance of having child-friendly resources for online protection, noting that the information from the Communications Authority was useful and could be translated into a child-friendly version.[156]

NGOs need to support and complement the government's legislation, policies and strategies[157] and continue to highlight the importance of prevention, which is not given as much focus as response currently.[158]

Within communities there are multiple stakeholders who can help keep children safe online and tackle OCSEA, although more is needed to train these stakeholders specifically on OCSEA. Stakeholder identification needs to include both formal and informal community structures.[159] Community members may have been trained to receive child protection reports but have rarely been trained on OCSEA.[160] Given that such community structures are often the first responder, this is particularly key.[161] It would therefore be important to raise awareness of child protection committees and the location, ward and area advisory councils.

[151] ChildLine KII, 09.03.2020; ECPAT KII, 27.01.2020; small group discussion, 04.03.2020
[152] Dadaab KII, 22.04.2020
[153] Dadaab and Garissa KIIs, 15.04.2020 and 29.04.2020
[154] ChildLine KII, 09.03.2020; small group discussion 04.03.2020
[155] ECPAT KII, 27.01.2020
[156] Garissa County DCS KII, 15-14.2020
[157] ECPAT KII, 27.01.2020
[158] ChildLine KII, 09.03.2020; The Office of the Director of Public Prosecutions, KII 03.02.2020; Small group discussion, 04.03.2020
[159] Small group discussion 04.03.2020
[160] ECPAT KII, 27.01.2020
[161] The Office of the Director of Public Prosecutions, KII 03.02.2020

When there is increased awareness, there is increased reporting, and there needs to be the capacity and knowledge to handle this.[162] [163]

Multiple informants noted the challenges of supporting children to talk about risks. Across society, there are reservations about talking about sex and it is considered a taboo subject, so often children do not disclose sexual-related concerns.[164] One informant noted that children are more likely to speak to a grandmother or older generation, who are much less informed.[165] Stigma attached to OCSEA also prevents reporting: "People will look at the child as if they have been complicit in the issue. If their images are out there they may be looked at as prostitutes."[166] One informant noted that in faith communities there are people other than parents who children can and do talk to.[167]

Children felt that there should be action on social media and highlighted lack of awareness. "The government should talk to parents regarding their children, especially those with social media accounts".[168]

One important observation about child reporting is that, for reporting to increase, children also need to feel they can continue with their normal lives once a report has been made. This includes not being stigmatized within the community for reporting, as well as having access to support services such as counselling.[169] This requires a collective commitment to recognizing and responding to the risks faced by children. As one informant noted, adults need to move away from the mentality of 'it is not my problem, its somebody else's child, I am minding my own business'.[170]

Parental responsibility, knowledge and action on OCSEA was a significant theme. Parents and caregivers can both inadvertently and purposefully put children at risk of harm, by: (1) being unaware of the risks themselves (and therefore not making devices child-safe, limiting the time spent on devices, or educating their children on staying safe online, and posting images and/or text that identifies their child and puts them at risk of harm);[171] (2) downloading porn which children can then access;[172] (3) choosing to cover up online abuse or not reporting it, often due to societal taboos around sex;[173] (4) taking CSAM and/or live-streaming sexual abuse of their children, often for financial benefit. A common theme in the KIIs was parents not having a phone themselves and often being illiterate, sometimes not knowing where their children got phones and not setting screen limits. *"Parents tell us that sometimes they wake up at night, and see lights on in the kids rooms as late as 3.00 am and wonder what the children are doing."*[174] In contexts in which children are brought up in extended families,

[162] ChildLine KII, 09.03.2020
[163] KII Kisumu 16.04.2020
[164] ChildLine KII, 09.03.2020
[165] ChildLine KII, 09.03.2020
[166] ECPAT KII, 27.01.2020
[167] ECPAT KII, 27.01.2020
[168] FGD with children, see summary report Appendix E.
[169] ECPAT KII, 27.01.2020; The Office of the Director of Public Prosecutions, KII 03.02.2020
[170] The Office of the Director of Public Prosecutions, KII 03.02.2020
[171] ECPAT KII, 27.01.2020, Watoto KII, 27.01.2020, Eveminet Communications meeting, 05.03.2020, ChildLine KII, 09.03.2020; The Office of the Director of Public Prosecutions, KII 03.02.2020; small group discussion 06.03.2020
[172] ChildLine KII, 09.03.2020
[173] ECPAT KII, 27.01.2020; KAARC KII, 18.03.2020
[174] KII, Garissa County, 15.04.2020

children may have access to phones or credit without their immediate caregiver knowing.[175] The feedback highlighted how poverty needs to be tackled in line with addressing OCSEA to minimize the production of CSAM and streaming due to financial necessity.[176] On the other hand, families experiencing high levels of poverty are less able to afford technology that enables internet access, so whilst there might be less access to the internet in the home, children still use cyber cafes and video dens.[177] In refugee camps, there are a large number of unregulated video dens, for example, and other venues were also regularly used for sharing pornography, such as miraa (khat) dens.[178]

These observations were also mirrored by child FGD participants. Children noted the generation gap that means that children may wish for more informed support: "many parents are illiterate and outdated so they are incapable of problem-solving online issues".[179]

Case study: School response to OCSEA

Some schools have developed their own responses. In one boarding school, the school decided to act when they observed that boys were regularly accessing pornographic materials via their mobile phones and in some cases uploading videos of themselves doing sexual acts for payment. The school provided individual counselling to one child in such a case, and referred for external counselling support. They decided to address the problem more broadly. They invited parents and explained the risks and emphasized the importance of talking about the issue to children. They also involved local Sheikhs, who was already aware that OCSEA was a common problem locally. He gave guidance from a religious perspective and is supportive. The school trained class teachers in OCSEA and how to handle it and set up a system of peer to peer counselors, to help identify students at risk. The Parent Teacher Association disseminate information on OCSEA through social media platforms. The local Children's Officer visited the school and informed them of reporting guidelines and they now work together.

(Source: KII, Garissa County, 15.04.2020)

Some schools have recognized the importance of schools supporting awareness raising on OCSEA and safer use of the internet. Private school counsellors report that children are raising concerns around cyber-bullying, identity theft and grooming.[180] Some schools have introduced their own codes of conduct around online safety and restrict use of phones.[181] Some companies have partnered with schools to increase accessibility to the internet, such as Zuku supporting connectivity, and the government's free laptop for every child scheme, and Liquid Communications working with a 100 schools through the Universal Service Fund (USF) connectivity project, managed by the CA. However, there have not always been safeguarding considerations underpinning those projects.[182] Despite these positive trends, there is little evidence of teachers communicating their concerns about a child to the parent/caregiver,[183] and there is a paucity of training on OCSEA for teachers. One teacher in Kisumu who had been trained (on the ChildLine curriculum) found that it gave her a strong knowledge of what OCSEA is, how she may identify it and, very importantly, how to support children and report cases.[184] There also appears to be a lack of coordination in the development of online safety curriculum - for example, ChildLine with TdH, Code IP Trust and

[175] KII, Garissa County, 15.04.2020
[176] ChildLine KII, 09.03.2020; ECPAT KII, 27.01.2020; Watoto KII, 27.01.2020; small group discussion 03.03.2020
[177] ChildLine KII, 09.03.2020, ECPAT KII, 27.01.2020; small group discussion 03.03.2020
[178] Abdi, SCCO, Dadaab
[179] FGD with children, see summary report Appendix E.
[180] Eveminet Communications meeting, 05.03.2020
[181] Garissa County KII, 15.04.2020
[182] Small group discussion, 03.03.2020
[183] The Office of the Director of Public Prosecutions, KII 03.02.2020
[184] Kisumu KII, 17.04.2020

ECPAT have all developed curricula for schools, but it has been done separately[185] The online safety curriculum is not compulsory for teachers, making the need to sensitize teachers a priority. [186] Any teacher training needs to be accompanied by head teacher/principal awareness raising to ensure buy-in and to allay a regular concern amongst many that talking about online safety may encourage children to experiment.[187]

2.5 Industry

Key findings from the desk review

- Globally there is still not yet a clear consensus on how to ensure that children's rights online are protected, without restricting the right of children and other users to access information and freedom of expression.[188]
- There is growing consensus in relation to the importance of industry proactively promoting digital citizenship among children and developing products and platforms that facilitate children's positive use of ICTs, including development of locally relevant content, particularly that which is targeted towards children, including those with vulnerabilities such as a minority language.[189]
- Globally it is noted that the wider private sector also has a key role to play, particularly phone and other communications companies in advancing industry-wide ethical standards on data and privacy, as well as other practices that benefit and protect children online. [190]
- Due to its tech ecosystem, Kenya is a hub for innovation in mobile technology. Many of these innovations and tech start-ups are started and driven by young people.

Field research findings

Despite the fact that internet use is growing globally on a daily basis, there are no adequate safeguards in place within the industry.[191] Specific observations about safeguards include the following:

- There is minimal local blocking or filtering of appropriate content.[192]
- There is a need for more child-friendly methods of communicating important information, especially because children do not read terms and conditions on internet usage.[193]
- Pop-ups of a sexual nature continue to cause concern, particularly on sites that are for, or attract children to them.[194]

The online industry has some awareness of OCSEA and implement projects to address OCSEA, as well as key partnerships. Safaricom has a partnership with the AHTCPU, and has identified a focal point for better liaison with the unit to aid reporting of concerns and investigations. Some of the large online platforms such as Facebook partner with NGOs to put in place

[185] NFR Stakeholders meeting March 3-4, 2020. ChildLine KII, 09.03.2020, Code IP Trust, ECPAT KII, 27.01.2020
[186] ECPAT KII, 27.01.2020
[187] Kisumu KII, 17.04.2020
[188] ibid, page 8
[189] UNICEF, 2017, State of the World's Children – children in a Digital World, page 11
[190] ibid, page 11
[191] ECPAT KII, 27.01.2020
[192] Watoto KII, 27.01.2020
[193] Eveminet Communications meeting, 05.03.2020; The Office of the Director of Public Prosecutions, KII 03.02.2020
[194] Small group discussion 03.03.2020

measures that proactively safeguard children online, such as tools, videos and warnings about unsafe behaviours and content. Some telephone companies (TELCOs) and tech companies are delivering awareness-raising projects across Kenya.

The Communications Authority (CA) is the regulator of the ICT industry in the country. A key milestone for the CA, was the development of the Cybercrimes and Computer Misuse Bill. The CA has been working on OCSEA since 2015, and as they are a communications regulatory authority they focus only on online aspects of child sexual exploitation. The CA, as the ICT regulator is mandated to protect consumers of ICT services including children. Given the CA have a monitoring and regulative role they have put a monitoring network in place.

In 2014, the CA launched a child online protection awareness campaign – Be the COP, to raise awareness of the risks that children are exposed to online. The partners in the implementation of the Be the COP campaign include the Department of Children Services, The Cradle, Kenya Girl Guides Association, Kenya Scouts Association, Kenya Association of Professional Counselors, UNICEF, Google, Plan International, Terre des Hommes NL, Childline Kenya, GSMA and mobile service providers Orange, Airtel and Safaricom.

KE-CIRT, though multi-sectoral, is located within the CA. In 2016, CA partnered with the International Telecommunications Union (ITU) to develop a national strategy on OCSEA. As part of this process, stakeholder consultations were held and a report of this is available. CA are looking into setting standard for operators and to develop guidelines for this.

The Kenya Information and Communications Regulations 2010, Universal Access and Service established the Universal Service Fund (USF). The objective of this fund include:

1. Promote communications infrastructure and services rollout in rural, remote and under-served areas
2. Ensure availability of communication services to Persons with Disabilities, women and other vulnerable groups.
3. Support the development of capacity building in ICTs and technological innovation;
4. Support expansion of communication services to schools, health facilities and other organizations serving public needs; and
5. Facilitate development of and access to a wide range of local and relevant content.

The USF is managed by the Universal Service Advisory Council and the Communications Authority. All operators contribute a statutory 0.5% of their annual turnover. Operators can access these funds to implement programs to promote access to under-served communities to close the access gap. CA has so far invested approximately two million USD since Aug 2015, through supporting partnerships, sponsorships, awareness programs and children's activities.

Stakeholders were of the view that CA needs to be more active in its regulatory role, coordinating efforts to prevent everyone working in silos, and that they also need to impose consistent monitoring, criteria for blocking and safeguarding standards.

Technology service providers of Kenya (TESPOK) brings together ISPs, social media platforms and mobile operators and it has 73 licensed operators as members, though they also work with community operators. TESPOK has been addressing Child online safety since 2009.

TESPOK members feed into KE-CIRT – its members produce the data that CA reports on. They work with KE-CIRT office to communicate with social media on taking down content and they are tracking and tracing providers and consumers, confirming you are the IP address, IME number, and provides this information to the AHTCPU.

There are many ISP and tech startups that work on generating education content and resources for children. EDTECH is a platform bringing together organizations in the industry to discuss key issues including online safety.

However, for the coordinating platforms and networks to be truly effective, they need all organizations in the online industry to join the coordinating platforms.[195] Whilst the industry launched and signed a charter outlining their commitment to protect children in the online space, good practices are not yet being seen across the board,[196] nor is it felt the industry is doing enough at present.[197]

The field research did, identify many good examples of a) partnerships that both develop the knowledge of the industry regarding OCSEA, and b) the industry developing knowledge within society. For example:

- Childline has trained TELCOs and social media companies;
- Watoto has a partnership with the Communications Authority to help raise awareness of online safety, a partnership with Safaricom and a three-year partnership with Facebook to raise awareness;[198]
- Google has awareness raising projects online, including Web Rangers, implemented through the Kenya Scouts organization and Be Internet Awesome;
- Eveminet Communications, Darasa Online and ILab/Strathmore have projects targeted at parents/carers and educators;[199] , iLAB/Strathmore has coding clubs for children and is developing locally-relevant content for parents and teachers.
- Safaricom who has a parental control tool and partners with the Internet Watch Foundation to take down illegal sites;
- Liquid Telcom and IBM support young people to develop their skills online.

Suggestions for enhancing the safety of the internet for children include:

- Embedding safeguarding in the design and roll-out phases of websites, apps and platforms;
- Having a two-step verification process;
- Using special filters to block illegal images (Google does this); developing more child-specific sites such as Google Families and YouTube Kids;
- Having clear, easy-to-use reporting mechanisms on sites using a trusted flagger program; and
- Signposting to support services such as ChildLine.[200]

[195] TESPOK, meeting 05.03.2020; EDTECH, meeting 05.03.2020
[196] Small group discussion, 06.03.2020
[197] ECPAT KII, 27.01.2020; ChildLine KII, 09.03.2020; Watoto KII, 27.01.2020; Eveminet Communications meeting, 05.03.2020
[198] Watoto KII, 27.01.2020
[199] Eveminet Communications, meeting 05.03.2020
[200] Small group discussion 06.03.2020

Innovative technology solutions that directly impact on children's ability to stay safe online also need developing and implementing,[201] including giving guiding messages online such as not to share too much personal information including passwords, or put up images of themselves;[202] developing a sim card for minors;[203] and developing a chatbot or texting service for children to report online concerns.[204]

Additional suggested industry interventions include consideration of how best to reach their target audiences, including consideration of cost (such as whether they charge for intervention programs, guidance or firewalls), location and accessibility (are tools easy for those who are less ICT-literate to access, if face-to-face is it at a time target audiences such as parents are available?).[205] As one example, Eveminet Communications are contracted to give talks on cyber safety in schools but, due to the cost, this is mostly private and international schools.[206]

There is a lot more the industry must do to effectively address OCSEA as a sector:

- They need to continually engage government on emerging online threats;[207]
- Escalate cases and provide data and IP addresses to the police as evidence;
- Expedite reporting and takedown of CSAM; suspend offending accounts; signpost to relevant stakeholders such as survivor support services;
- Collaborate with international organizations such as the GSMA;
- Update software frequently to help prevent misuse;
- Develop universally agreed monitoring so that everyone in the online industry is tracking in the same way, and giving more robust data and locally-generated research. This needs to include TELCOs, social media sites, online platforms, custodians of databases, software providers and developers, content providers, access device providers, and cyber security providers.[208]

There is still no legislation in Kenya that mandates online platforms to cooperate with investigations and provide data that is key to assist prosecutions.[209]

Companies, through corporate responsibility programs, can also be doing more, such as financially supporting organizations and the government to roll out programs on OCSEA and supporting Safe Internet Day. However, there is currently not much campaigning to get them on board.[210] There are useful guidelines such as the USA's COPA Act[211] giving best practice SOPs for the online industry.[212]

The industry sometimes perceive the child protection sector as applying a 'sledgehammer' approach to the industry, and that the child protection sector does not listen to its concerns

[201] Directorate of Criminal Investigations (DCI), 05.03.2020
[202] ChildLine KII, 09.03.2020
[203] Watoto KII, 27.01.2020
[204] Small group discussion 04.03.2020
[205] Eveminet Communications, meeting 05.03.2020
[206] Eveminet Communications, meeting 05.03.2020
[207] Small group discussion 06.03.2020
[208] Small group discussion 06.03.2020
[209] The Office of the Director of Public Prosecutions, KII 03.02.2020
[210] ECPAT KII, 27.01.2020
[211] Child Online Protection Act, USA, 1998 - with the purpose of restricting access by minors to harmful content on the internet
[212] IBM meeting 05.03.2020

and challenges.[213] It is important instead to work with the industry in partnership and listen to their views and challenges. There needs to be a balance, but without compromising the rights and safety of children.[214] "If digital platforms use in correct way, digital media and technology has the likelihood of becoming a pivotal moment for all children."[215]

2.6 Media and communications

Key findings from the desk review

- A growing trend is the advertising of legitimate (sometimes well-known) brands on CSAM websites. The Internet Watch Foundation noted "a disturbing trend in which ads are being posted online alongside child sexual abuse imagery".[216]
- The role of the media is vital – how they portray the pros and cons of the internet and empower children to stay safe online is key. "Media stories about the potential impact of connectivity on children's healthy development and well-being should be grounded in empirical research and data analysis".[217]

Field research findings

Children's stories are not being comprehensively included on digital media. Whilst acknowledging that children's stories should be told online, media and communications agencies are worried about how to safeguard the children involved, including informed consent, copyright issues, and the need to authenticate stories. Additionally, there is potentially a lack of interest from the wider readership on children's stories.[218] There are some positive examples, such as Mtoto News – a child participation platform where children generate content.[219]

The media could and should play a greater role in raising awareness of OCSEA.[220]

Funding for all of media and communications, including the online industry, needs to be increased and coordinated for a more consistent approach.[221]

3. Summary of findings from an online survey on OCSEA for DCS staff

An online survey on OCSEA for DCS staff was administered with 22 questions related to OCSEA. There were 151 respondents, of which 99 answered all survey questions,

There was a gender balance among the survey respondents. However, though it was a nationwide survey, most respondents work in Nairobi county, while some chose not to specify. Most were sub-county children's officers (51%) though respondents covered a wide

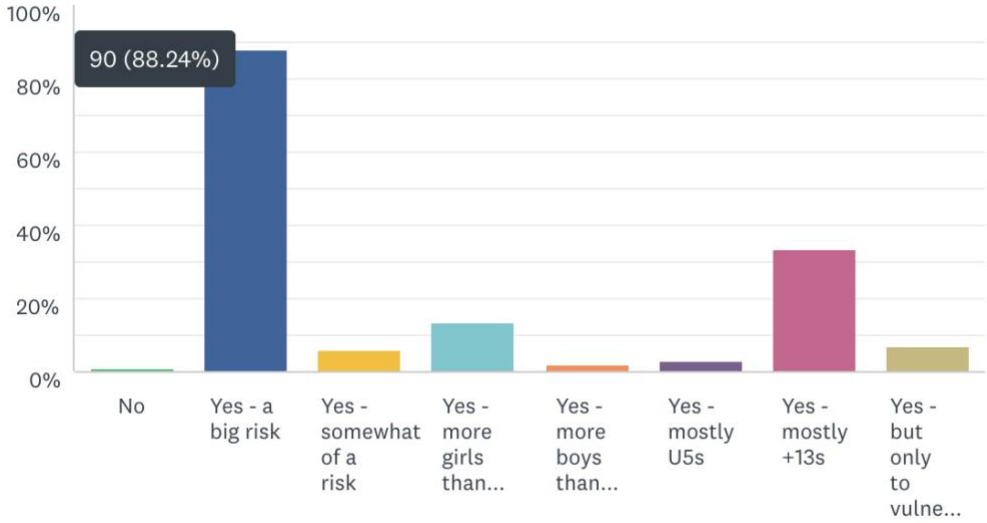
[213] NFR ISP Stakeholders meeting March 5-6, 2020
[214] Directorate of Criminal Investigations (DCI), 05.03.2020
[215] Small group discussion, 05.03.2020
[216] UK Government, 2018, Advertisers urged to help tackle online child sexual exploitation, https://www.gov.uk/government/news/advertisers-urged-to-help-tackle-online-child-sexual-exploitation
[217] UNICEF, 2017, State of the World's Children – Children in a digital world, page 11
[218] Small group discussion, 04.03.2020
[219] Mtoto News, meeting 05.03.2020
[220] ChildLine KII, 09.03.2020
[221] Eveminet Communications, meeting 05.03.2020

variety of roles within the DCS. 47% have worked in children's services for over ten years and no respondents had worked in children's services for less than a year.

Defining OCSEA

Most respondents defined OCSEA as online sexual exploitation (89%) and most also included child sexual abuse materials (CSAM) (76%). Some included sexting (66%), cyber-bullying (64%) and sextortion (59%). However, only half the respondents considered online grooming (52%), live-streaming of OCSEA (55%) and online trafficking (46%) as aspects of OCSEA. Three respondents used the term 'child pornography'[222].

Understanding the risk of OCSEA in Kenya

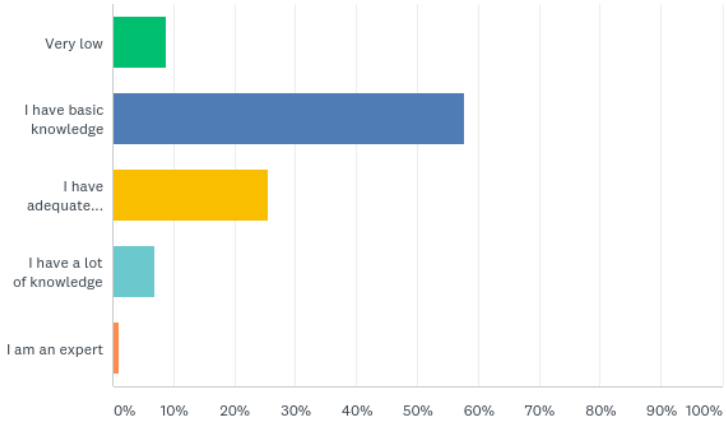


Most (88%) see OCSEA as a big risk to children in Kenya. However, 33% believe it is more of an issue for children aged 13 or over. 14% think that girls are more at risk than boys.

Respondents' level of knowledge of OCSEA

58% of respondents have a basic knowledge of OCSEA; only 1% defined themselves as experts. 83% have not received training on OCSEA and some commented on how they have built up their knowledge through their own research.[223]

[222] 3 of 7 respondents who ticked 'other', question 6
[223] Based on 52 comments, question 8



Those who had been trained received on average a two-day training[224]. Only 2% of those not trained have training scheduled.

ANSWER CHOICES	RESPONSES	
Yes	14.71%	15
No but it is scheduled	1.96%	2
No	83.33%	85
TOTAL		102

Case management experience

33% of respondents had handled at least one OCSEA case. The majority of those who had supported a child victim of OCSEA referred the child to counselling and/or the police/DCI.[225] Some of the respondents stated that the case were identified through Child Helpline (116), the chief's office, community leaders and the children's office.

Processes, procedures and tools to address OCSEA

The most common response to what processes, procedures and tools respondents used to address OCSEA was that they were unsure (16%). Respondents covered several different tools and processes; the most common was referring victims/survivors to counselling (15%); the second most common was identifying, engaging and referring victims/survivors (12%). 11% referred the case to the police.

74% of respondents use the same procedures and tools for handling OCSEA cases and other child protection cases. *"Every case is unique and requires different interventions e.g some would call for police intervention for eventual prosecution while others may need professional counseling, parental support, supervision with or without court orders etc. Tools: case record sheets, case book, written promise forms, social inquiry report, form C1".*

[224] Based on 14 comments, question 9
[225] Based on 27 comments, question 10

However, whilst acknowledging that all child protection cases need to prioritise the victim/survivor and involve referral and often counselling, many said there are not (as far as they are aware) specialist procedures for handling OCSEA cases.[226]

Most respondents would use the Children Act (2001) and the Sexual Offenses Act (2008). Only 10 respondents (13%) were aware of the Cyber Crime Act (2018) and 11 (14%) said they didn't know what legislation and guidance exists for managing OCSEA cases.

75% said they either don't, or are not sure, they have the capacity, procedures and tools to handle OCSEA cases. Some participants acknowledged that the OCSEA landscape rapidly changes, others raised the complexity of online abuse; several said that they lack the training to handle OCSEA cases effectively.[227] Some of this feedback included: *"It is an emerging area that is not well budgeted;" "It's a new area and I need training to confidently handle OCSEA"* and *"I would need to have SOPs to be able to operate under a structured framework and to be able to offer proper technical guidance to other agencies like the police."*

Preventing and addressing OCSEA

When looking at preventing OCSEA, the most common response was to place responsibility on parents/care givers for controlling or limiting children's access to the internet (23%); however, only 8% of respondents highlighted the importance of providing training/guidance to parents. This may be due to the fact that the officers lack the necessary knowledge themselves, as highlighted above, to provide the relevant guidance to parents. Training and guidance for children was seen as important by 11% of respondents. Counselling was the second most common prevention intervention (20%).

Counselling was the most available service for victims/survivors (84%), with 43% of respondents also being aware of extended counselling services for families and friends involved. There was also support to go through the court process according to 50% of respondents, though only 1% was aware of any financial support for victims/survivors. Four respondents said they knew of no services in their area for OCSEA victims/survivors.[228]

Some of the barriers to victims/survivors accessing support include lack of knowledge on support services (86%); cost (70%); stigma (66%); location (50%); and a lack of response from essential service providers (46%). Key requirements for improving support to victims/survivors includes training for service providers (17%); community sensitisation (15%), increasing capacity (13%), and offering free or low-cost counselling (10%). 61% of respondents said that training and/or capacity building would help them to better support victims/survivors of OCSEA.

Individuals work with a lot of different organisations to prevent and address OCSEA, particularly parents/care givers (79%), local police (77%), courts (70%), child protection volunteers (67%), AACs (66%), NGOs/CBOs/FBOs (61%), schools (60%), ChildLine (60%), community members and faith-based leaders (53%). The least used were KE-CIRT (8%) and one-stop centres (14%).

[226] Based on 51 comments, question 12
[227] Based on 58 comments, question 14
[228] 4 of 9 respondents who ticked 'other', question 16

Most respondents said that training/capacity building (43%), and networking (24%) are the two priorities for improving cross-organisational and cross-sector collaboration. SOPs that outline clear roles, responsibilities and contact details for signposting (12%) was also highlighted as being key.

National Plan of Action top priorities

Looking first at what respondents saw as the highest priority, they want to see capacity building, training and guidance of all stakeholders, including parents and care givers, children, the wider community, and professionals. The capacity of services needs to be improved, including funding, equipment, online databases and personnel. Training and guidance for parents/care givers was seen as the top priority (13%), with training and guidance for children also important (11%). More comprehensive laws that are better enforced was also seen as key by 10%.

The emphasis on training and capacity building is even more apparent in priorities 2 and 3, with respondents placing different stakeholder training as the five most important areas (parents, children, communities, professionals and overarching capacity building).

Pulling together respondents' answers from priorities 1, 2, and 3, the top priorities are:

1. To increase the knowledge and skills of communities, including children and their parents/care givers to prevent and respond to OCSEA (100 respondents)
2. To increase the capacity and knowledge of the child protection workforce, including DCS, police, judiciary, schools, NGOs. Capacity include workforce numbers, funding, specialist equipment and access to online databases (56 respondents)
3. To improve legislation, regulation, reporting, referral and case management procedures to ensure a comprehensive procedure that prioritizes the well-being of the victim throughout (53 respondents).

4. Summary of findings from global Disrupt Harm Study Kenya, 2020

Kenya was one of 13 countries[229] part of the global Disrupt Harm Study[230], undertaken in 2021. The study found that:

- Though data on number of cases is yet not provided at national level, the Anti Human Trafficking and Child Protection Unit (AHTCPU) of the Directorate of Criminal Investigations alone handled 3,160 cases in 2018 and 4,133 in 2019.
- Between 2017 and 2019, the Kenyan law enforcement authorities received an average of 13,572 CyberTips per year from globally popular online platforms based largely in the United States via the U.S. National Center for Missing and Exploited Children (NCMEC)
- In 2020, the number was 14,434. Almost all of these reports concerned apparent cases of the possession, manufacture and distribution of CSAM in Kenya.

[229] The countries of focus in the Eastern and Southern Africa region are: Ethiopia, Kenya, Mozambique, Namibia, South Africa, Tanzania, and Uganda. The countries of focus in the Southeast Asian region are: Cambodia, Indonesia, Malaysia, the Philippines, Thailand, and Vietnam

[230] Partnership to End Violence Against Children, ECPAT, INTERPOL, UNICEF (2021). Disrupting Harm in Kenya. Evidence on Online Child Sexual Exploitation and Abuse

- While Facebook submitted 93% of the reports, numerous other electronic service providers also submitted reports, suggesting the misuse of a range of platforms by OCSEA offenders.
- Research using Google Trends points to interest in CSAM in Kenya including image and video content depicting sexual activity with and between teenagers, with children, and with babies
- Internet-using children in Kenya are regularly subjected to OCSEA. According to children and frontline workers, most offenders of OCSEA are someone the child already knows and these crimes can happen offline, online or both
- Many children in Kenya did not tell anyone the last time they were subjected to OCSEA. Children tend to disclose to people they know rather than reporting to a helpline or the police.
- Among children who were subjected to OCSEA through social media, Facebook and WhatsApp were the most common platforms where this occurred.
- The law enforcement, justice and social support systems have inadequate awareness, capacity and resources to respond to cases of OCSEA.
- Important OCSEA-related legislation, policies and standards are not yet enacted in Kenya.

5. Conclusion

5.1 Concluding observations

The majority of the challenges outlined in the KIIs and FGDs with both adults and children are those highlighted in the WePROTECT model as Enablers – in Kenya, this study has found:

- There are many great initiatives to both raise awareness of, and tackle OCSEA, but insufficient **cross-sector, multi-disciplinary collaboration and coordination** and too many organizations working in silos.
- There is a specialist branch of the police, but within the wider judiciary, a lack of **willingness to prosecute, functioning justice system and rule of law** due to a lack of knowledge on OCSEA and its impact on children.
- There is an understanding of the need for a **supportive reporting environment** and good examples of this, but an unclear reporting procedure, lack of sufficient trained social service workforce and police, and only a few examples of survivor support services and these are not country-wide. Child barriers to reporting need to be addressed, including fear of harsh punishment from parents or caregivers, and fear of reprisals online.
- Due to a lack of nationwide capacity-building, children, parents/caregivers, the public and child protection professionals are not **aware of the risks and scale of the issue;** but there are pockets of society that are, including the AHPTCU, specialist NGOs and some organizations within the online industry.
- Whilst funding has been given to the set-up and running of the AHPTCU, there needs to be an allocation of **sufficient financial and human resources** for all relevant stakeholder groups to build a knowledgeable, resourced workforce across Kenya
- The Cyber Crimes and Misuse of Computers Act is a huge step towards having **national legal and policy frameworks in accordance with the UNCRC and other international and regional standards** but there are still gaps in both policy and implementation.

- There is a need to create universal terminology and data collection SOPs to build **data and evidence on OCSEA** in Kenya**.**

5.2 Recommendations

The following recommendations have been translated into proposed interventions in the draft National Plan of Action to address OCSEA, to be reviewed and validated by stakeholders.

5.2.1 Policy and governance actions to increase OCSEA prevention and protection

- Sufficient, allocated budget to develop good practices and enable them to be applied across the country
- All relevant stakeholders know what the legislation is and how it works together to support children and tackle OCSEA (public and sector-specific information so people understand and know how to apply;
- Training for stakeholders to be able to apply the legislation within their work
- During the data collection there were conflicting views on whether the sexual offenders register should be made public, and this will require more consideration.

Coordination:

- Between DCS and CA, clear roles and mandates
- Coordination of ISP providers and TELCOs (through TESPOK)

5.2.2 Strengthening the criminal justice system to respond to OCSEA

- Joining up data systems on both perpetrators and child survivors (including the police national computer system), and having the capacity to mine existing databases for information to support investigations.
- The AHTCPU requires more resources to increase their operational capacity, including on using forensic tools such as Celebrite.
- Appropriate funding and psychosocial support for staff at AHPTCU: Although counselling was arranged for AHPTCU officers, they have been asked to pay for this personally. The lack of immediate access to funding has also resulted in the police using their own money to pay for essential items for survivors and their families, such as milk and food.
- Training on online grooming

5.2.3 Strengthened support to survivors and potential child victims

- Targeted services in areas where children are being trafficked online, across borders and into potential sex work in larger cities
- There is need to build capacity of county and sub-county DCS staff on OCSEA, roll out case management system, and strengthen referral pathways. Furthermore, the social service workforce for child protection needs to be adequately resourced to prevent and respond to OCSEA and wider child protection issues in general. Standard Operating Procedures should take into consideration OCSEA.
- Ensure an effective Case Management system is in place
- Develop and implement referral pathways

- Coordinated training on OCSEA and relevant legislation for police and judiciary, who must both know and uphold legislation
- Combined training of multiple stakeholders in order to investigate, prosecute and provide support services for child survivors.
- Understanding the needs of child survivors and knowing what to do
- Where a case is progressed, attention must be given to making sure the child is in a safe environment
- Overall, perpetrator rehabilitation requires more focus within the response.
- Recommendation to know more about gendered risks and vulnerabilities, identify gender-sensitive training for officials, provide gender-sensitive responses

5.2.4 Actions to enhance social awareness and action on OCSEA prevention and protection

- Awareness raising and training on online grooming for children, their caregivers and service providers
- Targeted interventions to reach children in hot spot areas or specific ages and genders, including: reaching children who are about to drop out of school after standard 8
- Focus on parent awareness raising, through forums such as PTAs, parenting programs, religious channels of communication, including an understanding of both the positives and risks that children are aware of.
- Support awareness, training and policies in the education sector to reduce children's access to and use of CSAM and to enhance reporting and responses
- More needs to be done on issues such as sexting, sextortion, posting and grooming.
- Consider need to integrate OCSEA into traditional legal processes as

5.2.5 Safeguards and actions in the industry and media

- They need all organizations in the online industry to join coordinating platforms
- Suggestions for enhancing the safety of the internet for children include:
  - embedding safeguarding in the design and roll-out phases of websites, apps and platforms;
  - having a two-step verification process;
  - using special filters to block illegal images (Google does this); developing more child-specific sites such as Google Families and YouTube Kids;
  - having clear, easy-to-use reporting mechanisms on sites using a trusted flagger program; and
  - signposting to support services such as ChildLine.
- Innovative technology solutions
- Additional suggested industry interventions include consideration of how best to reach their target audiences,
- Financially supporting organizations and the government to roll out programs and supporting Safe Internet Day.
- The media could and should play a greater role in raising awareness of OCSEA.
- Communications Authority needs to be more active in its regulatory role, coordinating efforts to prevent everyone working in silos. They also need to impose consistent monitoring, criteria for blocking and safeguarding standards.

- Funding for all of media and communications, including the online industry, needs to be increased and coordinated for a more consistent approach.

Bibliography

African Network for the Prevention and Protection against Child Abuse and Neglect (ANPPCAN) (2015). *Study on Sexual Exploitation of Children in Travel and Tourism in Kenya*. Retrieved from: http://www.anppcan.org/wp-content/uploads/2016/12/SECTT-Kenya.pdf

BAKE (2017). State of the Internet in Kenya

Communications Authority of Kenya (2018). Third Quarter Sector Statistics Report 2018/2019 (July-September 2018).

ECPAT International (2013). Understanding African children's use of Information and Communication Technologies (ICTs) – a youth-led survey to prevent sexual exploitation online. Retrieved from: https://www.ecpat.org/wp-content/uploads/legacy/ICT%20Research%20in%20AFRICA_p1.pdf

ECPAT International (2017). *ECPAT International Journal*, Issue 12, April 2017. Online Child Sexual Exploitation: an analysis of emerging and selected issues'. Retrieved from: https://www.ecpat.org/wp-content/uploads/2017/04/Journal_No12-ebook.pdf

ECPAT International (2018). *Trends in Online Child Sexual Abuse Material.* Retrieved from: https://www.humandignity.foundation/wp-content/uploads/2018/11/ECPAT-International-Report-Trends-in-Online-Child-Sexual-Abuse-Material-2018.pdf

Geekflare (24 November 2020). 11 best image hosting sites for personal to business. Retrieved from: https://geekflare.com/best-image-hosting/

Interagency Working Group on Sexual Exploitation of Children (2016). 'Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse'. Retrieved from http:// luxembourgguidelines.org/

International Centre for Missing and Exploited Children (2018). Child sexual abuse material- model legislation and global review. Retrieved from: https://cdn.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18-1.pdf

Internet Watch Foundation (2018). Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse. Retrieved from: https://www.iwf.org.uk/sites/default/files/inline-files/Distribution%20of%20Captures%20of%20Live-streamed%20Child%20Sexual%20Abuse%20FINAL.pdf

Interpol & ECPAT. (2018). Towards a Global Indicator on Unidentified victims in Child Sexual Exploitation Material. Retrieved from: https://www.ecpat.org/wp-content/uploads/2018/03/TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL-Summary-Report.pdf

Kenya National Bureau of Statistics (2018). Kenya Integrated Household Budget Survey 2015-2018

Maestral International. (2019). Desk Review: Assessment of the National Response to Child Online Sexual Exploitation in Kenya using the We Protect Model National

Response framework. Report submitted to UNICEF Kenya and Department of Children's Services, November 2019.

National Society for the Prevention of Cruelty against Children (NSPCC) (2019). https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/#what-is

Nendo (2019). The State of Mobile Data Insights & Highlights

Quayle, Jonsson, Cooper, Traynor and Svedin (2018). *Children in Identified Sexual Images – Who Are they? Self- and Non-Self- Taken Images in the International Child Sexual Exploitation Image Database 2006–2015*, quoted in ECPAT International (2018).

Terre des Hommes Netherlands (2018). *The Dark Side of the Internet for Children. Online Child Sexual Exploitation in Kenya - A Rapid Assessment Report, February 2018.* Retrieved from: https://www.datocms-assets.com/22233/1600704755-tdh-nl-ocse-in-kenya-research-report-feb-2018.pdf

UNICEF (2017). *State of the World's Children – Children in a Digital World.* Retrieved from: https://www.unicef.org/reports/state-worlds-children-2017

UNICEF (2017). *Children's participation in local governance*. Retrieved from: https://www.unicef.org/sites/default/files/2019-12/UNICEF-Child-Participation-in-Local-Governance.pdf

U.S. Department of Justice (2016). *National Strategy for Child Exploitation Prevention and Interdiction*. Retrieved from: https://www.justice.gov/psc/national-strategy-child-exploitation-prevention-and-interdiction

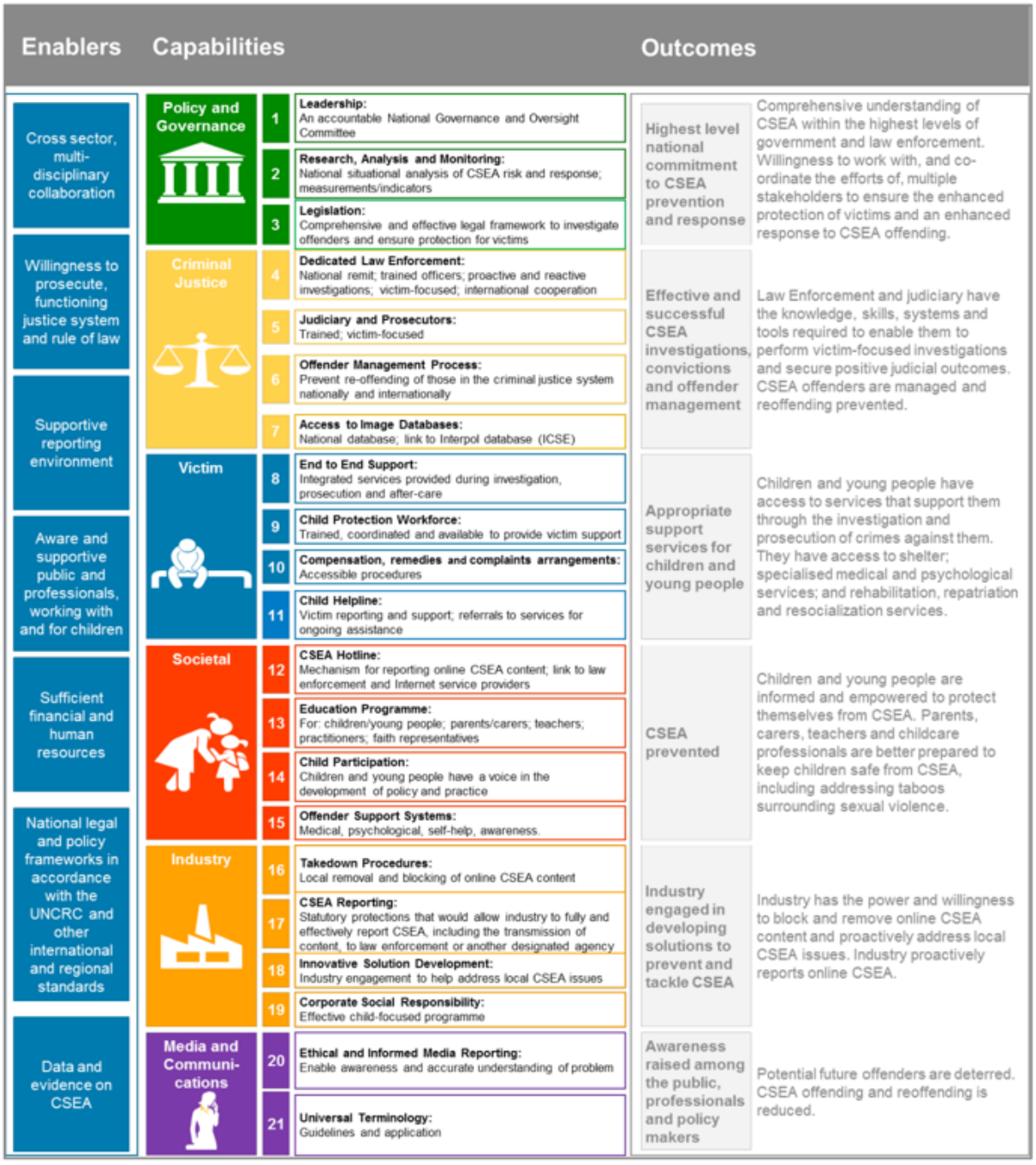
Appendix A: List of Key Informant Interviews

	Organization	County	Date
1	Project officer, ECPAT International	National	27.01.2020
2	Project officer, Watoto Network	National	27.01.2020
3	Children's Division, Office of the Director of Public Prosecutions	National	03.02.2020
4	DCS	National	03.02.2020
5	AICS	National	04.03.2020
6	Project offier, Childline Kenya	National	09.03.2020
7	Eveminet Communications	National	10.03.2020
8	Head of AHTCPU	National	11.03.2020
9	Head of Cyber crimes unit, AHTCPU	National	11.03.2020
10	Data Analyst, AHTCPU	National	11.03.2020
11	Investigations officer, AHTCPU	National	11.03.2020
12	Intelligence Officer, AHTCPU	National	11.03.2020
13	Communications Authority	National	11.03.2020
14	Project Officer, Kenya Alliance for the Advancement of Children - KAARC	National	18.03.2020
15			
16	Lecturer, Data security iLab, Strathmore University	National	19.03.2020
17	Digital learning unit, iLab, Strathmore University	National	19.03.2020
18	Program manager, African Advanced Level Telecommunications Institute, AFRALTI	National	21.03.2020
19	IT trainer, African Advanced Level Telecommunications Institute, AFRALTI	National	21.03.2020
20	Project officer, UNICEF Education	National	23.04.2020
21	County Children's Coordinator	Kisumu	15.04.2020
22	Children's officer, Kisumu children's remand home	Kisumu	15.04.2020
23	Former Counselor, Childline Kenya	Kisumu	16.04.2020
24	Teacher, Lake Primary School	Kisumu	17.04.2020
25	Police Gender Desk, Central Police station	Kisumu	17.04.2020
26	Sub county children's officer, Kisumu central	Kisumu	17.04.2020
27	Project officer, AICS/Childline Kenya, Kisumu west	Kisumu	17/04.2020
28	Counselor, Childline Kenya	Kisumu	17.04.2020
29	County Children's Coordinator, DCS	Garissa	15.04.2020
30	Programme Coordinator, Womankind	Garissa	15.04.2020

	Organization	County	Date
31	Teacher (Maths/Physics/Guidance counsellor), Garissa High school National Boys school	Garissa	15.04.2020
32	Sub county children's coordinator, DCS, Dadaab	Dadaab, Garissa	15.04.2020
33	OC crime, Garissa Police	Garissa	15.04.2020
34	Pyschosocial counselor	Garissa	15.04.2020
35	Teacher, NEP Girls high School	Garissa	17.04.2020
36	Programme Manager, Dadaab Field office, Save the Children	Dadaab, Garissa	21/04.2020
37	Programme Manager, Dadaab Field office, Save the Children	Dadaab, Garissa	21/04.2020
38	Community advocate, youth leader, chairperson civil society organization	Garissa	22.04.2020
39	Field Coordinator, Dadaab Field office, Terre Des Hommes Foundation	Dadaab, Garissa	22.04.2020
40	Garissa Community Religious Leader in Garissa town Bula Hagar	Garissa	24.04.2020
41	Refugee Community Religious Leader	Dadaab, Garissa	29.04.2020
42	Student, Form 2, Hagadera High School	Dadaab, Garissa	30.04.2020
43	County Children's Coordinator, DCS	Mombasa	19.05.2020
	OCSEA National Stakeholder meeting	Nairobi	3-4.03.2020
	ISP OCSEA Stakeholder meeting	Nairobi	5-6.03.2020
	EdTech Online Meet Up OCSEA	Nairobi	15.05.2020
	We Protect OCSEA and COVID-19 Webinar	UK	21.05.2020

Appendix B: Meeting agendas

Appendix C: WePROTECT national model response



Appendix D: Kenya's legislation and policies on OCSEA[231]

	Legislation
1	Constitution of Kenya, 2010
2	Children's Bill, 2001
3	Sexual offences Act, 2006
4	Cybercrimes and Computer Misuse Act, March 2020
5	Data protection Act, 2019
6	Kenya Information and Communication Act, 2013
7	Victim Protection Act, 2014
8	Stage and Films Play Act, 2012
9	Basic Education Act, 2013
	Policies
1	Children Policy, 2010
2	ICT Policy, 2019
	Plans
1	VAC- Prevention and Response Plan 2012
2	Sexual Exploitation of Children 2018-2022 and the draft NPA on VAC 2020

Appendix E: Existing Definitions Legal Framework Kenya

Terminology	Definition	Document
"Promotion of sexual activity with a child"	A person including a juristic person who— 1. (a) manufactures or distributes any article that promotes or is intended to promote a sexual offence with a child; or 2. (b) who supplies or displays to a child any article which is intended to be used in the performance of a sexual act with the intention of encouraging or enabling that child to perform such sexual act, is guilty of an offence and is liable upon conviction to imprisonment for a term of not less than five years and where the accused person is a juristic person to a fine of not less than five hundred thousand shillings.	Sexual OffencesAct3 of 2006. Ch 62A, Revised Edition 2012. Section 12
"Child Prostitution"	Any person who— 1. (a) knowingly permits any child to remain in any premises, for the purposes of causing such child to be sexually abused or to participate in any form of sexual activity or in any obscene or indecent exhibition or show; 2. (b) acts as a procurer of a child for the purposes of sexual intercourse or for any form of sexual abuse or indecent exhibition or show; 3. (c) induces a person to be a client of a child for sexual intercourse or for any form of sexual abuse or indecent exhibition or show, by means of print or other media, oral advertisements or other similar means;	Sexual OffencesAct3 of 2006. Ch 62A, Revised Edition 2012. Section 15

[231] NFR OCSEA Stakeholder meeting March 3-4, 2020

	4. (d) takes advantage of his influence over, or his relationship to a child, to procure the child for sexual intercourse or any form of sexual abuse or indecent exhibition or show; 5. (e) threatens or uses violence towards a child to procure the child for sexual intercourse or any form of sexual abuse or indecent exhibition or show;	
"Child pornography"	(1) Any person including a juristic person who— (a) knowingly displays, shows, exposes or exhibits obscene images, words or sounds by means of print, audio-visual or any other media to a child with intention of encouraging or enabling a child to engage in sexual acts; (aa) 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 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; 2. (b) imports, exports or conveys any obscene object for any of the purposes specified in subsection (1), or knowingly or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation; 3. (c) takes part in or receives profits from any business in the course of which he or she knows or has reason to believe that any such obscene objects are, for any of the purposes specifically in this section, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation; 4. (d) 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 5. (e) offers or attempts to do any act which is an offence under this section, is guilty of an offence of child pornography and upon conviction is liable to imprisonment for a term of not less than six years or to a fine of not less than five hundred thousand shillings or to both and upon subsequent conviction, for imprisonment to a term of not less than seven years without the option of a fine. (2) This section shall not apply to— (a) a publication which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, art, representation or figure is in the interest of science, literature, learning or other objects of general concern;	Sexual OffencesAct3 of 2006. Ch 62A, Revised Edition 2012. Section 16

	(b) any book, pamphlet, paper, writing, drawing, painting, representation or figure which is kept or used *bona fide* for religious purposes; (d) any representation sculptured, engraved, painted or otherwise represented on or in any ancient monument recognised as such in law; and (c) activities between two persons of over eighteen years by mutual consent. (3) For the purposes of subsection (1), a book, pamphlet, paper, drawing, painting, art, representation or figure or any other object shall be deemed to be obscene if it is 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 who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it. [Act No. 7 of 2007, Sch., Act No. 6 of 2009, Sch.]	
"Child Pornography"	A person who, intentionally — 1. (a) publishes child pornography through a computer system; 2. (b) produces child pornography for the purpose of its publication through a computer system; 3. (c) downloads, distributes, transmits, disseminates, circulates, delivers, exhibits, lends for gain, exchanges, barters, sells or offers for sale, lets on hire or offers to let on hire, offers in another way, or make available in any way from a telecommunications apparatus pornography; or 4. (d) possesses child pornography in a computer system or on a computer data storage medium, commits an offence and is liable, on conviction, to a fine not exceeding twenty million or to imprisonment for a term not exceeding twenty five years, or both. "child pornography" includes data which, whether visual or audio, depicts — 1. (a) a child engaged in sexually explicit conduct; 2. (b) a person who appears to be a child engaged in sexually explicit conduct; or 3. (c) realistic images representing a child engaged in sexually explicit conduct;	Computer Misuse and Cybercrimes Act No 5. 2018. Section 24
"Exploitation"	includes but is not limited to— (a) keeping a person in a state of slavery; (b) subjecting a person to practices similar to slavery; (c) involuntary servitude; (d) forcible or fraudulent use of any human being for removal of organs or body parts; (e) forcible or fraudulent use of any human being to take part in armed conflict; (f) forced labour;	Counter Trafficking in Persons Act, No. 8 of 2010. Section 2

	(g) child labour; (h) sexual exploitation; (i) child marriage; (j) forced marriage.	
"Protection from sexual exploitation"	A child shall be protected from sexual exploitation and use in prostitution, inducement or coercion to engage in any sexual activity, and exposure to obscene materials	Children Act 2010, Revise Edition 2012. Part II, section 15
"Cyber harassment"	A person who, individually or with other persons, wilfully communicates, either directly or indirectly, with another person or anyone known to that person, commits an offence, if they know or ought to know that their conduct — 1. (a) is likely to cause those persons apprehension or fear of violence to them or damage or loss on that persons' property; or 2. (b) detrimentally affects that person; or 3. (c) is in whole or part, of an indecent or grossly offensive nature and affects the person.	Computer Misuse and Cybercrimes Act No 5. 2018. Part 1, Section 27
" Blockchain technology"	means a digitized, decentralized, public ledger of all crypto currency transactions;	Computer Misuse and Cybercrimes Act No 5. 2018. Part 1, Section 2

Appendix F: Findings from focus group discussions with children aged 13 to 17 to assess the National Response to Child Online Sexual Exploitation in Kenya, 7 April 2021

Overview of focus group discussions (FGDs)

Critical learning from other research[232] has consistently demonstrated that children are best placed to inform the child protection workforce and policy makers of their "lived reality" online, which differ from adults who grew up in the analogue and digital age. However, due to COVID-19, the field research that was planned with children to help shape Kenya's NPA on OCSEA was unable to take place. In February 2021, the Technical Working Group decided that the NPA requires children's views on OCSEA to help shape the NPA before it can be validated.

The main objectives of obtaining the views of children were to:

- **Better understand** the opportunities and risks that the internet gives children (anyone under 18 years old), particularly in light of being in a digital era and emerging trends in communication that increase children's use of the internet, which has been exacerbated by COVID-19;
- **Provide more in-depth and tailored actions in the NPA** for each of the stakeholder groups that respond to the challenges and strengths identified by children;
- **To understand children's online experiences** in terms of how the challenges faced on the internet affect their decision making and how their access to the internet affects their decisions and actions.

Children (aged 13 to 17) were asked to input their views on OCSEA and online safety. Two methods of engaging children were used:

- An online survey
- Focus Group Discussions in person.

Workshops with children under 13 years old did not take place due to (1) the content of the FGDs (2) the short amount of time remaining on the project to conduct these and (3) the continuing COVID-19 restrictions.

Fourteen focus group discussions were held with children aged 13 to 17 years in Garissa, Dadaab, Kisumu and Mombasa in March 2021 with a total of 112 children participating. Boys' and girls' sessions took place separately. Additional FGDs were planned in Turkana but COVID-19 restrictions prevented them from taking place. With thanks to UNICEF, Department of Children's Services, KAARC, SOS Children's Villages, Danish Refugee Council, Save the Children, Garissa Primary, Girls High and Boys High schools for their support in enabling these vital discussions to take place.

Location	FGDs	Survey 7-17 years	Children 13-17 yrs	F	M
National		10			
Garissa			48	24	24

[232] UNICEF (2017), Children's participation in local governance, https://www.unicef.org/sites/default/files/2019-12/UNICEF-Child-Participation-in-Local-Governance.pdf

Kisumu			32	16	16
Mombasa			32	16	16
Total			**126**	**62**	**64**

The report covers a summary of findings from the focus group discussions and a separate summary of findings from the online survey for children.

It is worth noting that the responses of boys and girls have not been separated because their responses are very similar. The primary reason for holding separate sessions was to enable each gender to speak more freely on the topic; facilitators reported that all participants engaged fully and were communicative in the focus group discussions. However, one facilitator said participants were scared to disclose concerns in detail.

Summary of focus group discussion findings

Most children who participated in the focus group discussions said they mainly use the internet in cyber cafes, though some buy bundles of data for smart phones (theirs, their friends' or their parents'), use a computer or laptop at home and at school. They access the internet during their free time: "after school, holidays, weekends, any time"; "We use it all day during the weekends". In one focus group discussion, most participants owned smart phones and in another, 3 out of 8 participants had access to, but didn't own a smart phone; in all discussions, many children said they had a computer at home. It is worth noting that children said COVID-19 has greatly increased children's access to the internet as they now have computers and/or smartphones in order to engage in online learning - "Most of the children had access to smart phones because online learning required them to have smart phones". Many participants said that they and their friends have webcams.

Most children said they regularly use YouTube, Facebook, Messanger and Instagram. SnapChat and TikTok are also popular; other named apps include Omegle, Likee, Phoenix, Twitter, Telegram, Opera Mini, IMO and online games. The importance of online platforms for showcasing talents and making money through getting subscribers or followers was cited by several participants. One groups said they rarely watch TV any more other than Premier League football games with friends – instead they watch short videos on social media. Many said they have YouTube accounts. "I have a youtube account and upload funny videos".

Participants said that COVID-19 has heavily impacted on their use of the internet - "there was a lot of use during Corona and not before". "It [the internet] keeps us connected during lockdown"; "It kept us busy". Children noted problems including lack of sleep, weight loss, eye problems and addiction were cited. Some felt they 'waste time' online but noted they have had much more time alone during the pandemic. The internet has provided the opportunity for online learning and revision - "If a teacher gives you a hard question you can research online", keeping in contact with friends and making new ones, keeping them entertained including online gaming and skills development, enabling them to showcase and develop talents such as comedy and dance, and earn money through having subscribers, followers, likes and comments. One participant said that COVID-19 has changed their lifestyle – the internet is now how they stay close to friends. "COVID-19 confined children to the internet as there were no other commitments apart from school".

Children discussed the positives of the online world, with online learning being the most cited reason - “One of the advantages of the internet is that it has a lot of information on certain topics”. Platforms such as Yali, Viusasa and Zeraki were cited as useful for studying. Meeting new friends and socialising was also important, as was keeping in touch with family who don’t live nearby – “I talk to my mother on WhatsApp who lives in Somalia. Even my brother is reachable on WhatsApp calls”. Access to job opportunities, developing talents and having earning potential was seen as key - “One of the positive things about social media and the internet is job opportunities online”; “It helps to expose and empower talents hence the platforms can create employment and scholarships to the universities”; Research was also a key positive factor of the internet, particularly on non-curricula topics such as lifestyle, food, clothing, beauty, news, new songs and nature - “It keeps people informed and learn new skills and knowledge to equip them with new ideas”. One participant noted the importance of getting regular updates on COVID-19 online. Additionally, participants said the internet gives fast access to information” and is low-cost especially as it negates the need for travel to see friends and family, buying books and paying for tutors. Another positive of the internet given was it encourages diversity and inclusion - “It helps us to be connected with the rest of the world”; “It has given a voice to the voiceless”; “One of the advantages of the internet is that it is a platform where we can express our feelings about different matters online”.

Participants outlined a variety of perceived risks of being online, including addiction to the internet, keeping children away from their studies, wasting time and affecting sleep. Online bullying was highlighted as a key risk - “If you upload something onto a platform and get negative comments it gives emotional disturbance and can lead to suicide and mental health problems” and linked to this, having reputation damaged online – “It ruins your reputation if you make friends who eventually turn their backs on you”. One participant particularly cited boys verbally abusing girls on online chats. One participant said they felt the internet can lead to an erosion of culture as it encourages children to copy ‘foreign ways of life’, another said “bad company spoils good morals”.

All groups discussed online child sexual abuse and exploitation risks, including from popular sites including Facebook and Instagram, as well as wider online risks such as early exposure to relationships, hacking, cybercrime, involvement in drugs, joining cults and blackmail - “Some ladies trap you by use of messages and photos and even photo-shop as evidence of you being responsible for their pregnancy”. Whilst some children referred more broadly to OCSEA as “exposure to negative information” and “bad things”, many named specific OCSEA risks including online ‘predators’ – “the possibility of someone taking naked pictures and putting them on Facebook and WhatsApp”; “[children are] told to text personal information then they ask you to meet with them then they kidnap you”. Participants also cited pop-up pornography and sexual videos, ‘bad companies and ISPs’, account hacking to groom and blackmail, child sexual abuse material (CSAM) - “You may make friends online, share your pictures with them and they use those pictures for bad intentions”, ‘defilement’ and meeting sponsors online - “It may cause early pregnancy: you meet sponsors online, they entice you with money and meet and sleep with you”. One participant said that there was a risk of children watching pornography online and then practicing what they have seen. One participant noted, “It makes children know more things than adults” whilst another said “Most of the parents don’t have control of their children online”.

Most participants would report online concerns to a teacher; some said they would talk to the police, parents, the child rights officer in the community, relatives, a neighbour, the village elder, church elder, friends - "I will tell my best friend because they understand me"; "We find it easy to deal with our peer groups or friends instead of reporting to any authority", or someone else they trust - "I will tell a psychiatrist because he will be open to me and give me advice since he's older than me". One participant said, "Most youths tend to confine and confide with friends and peers. They are not ready to share with friends and guardians, teachers, sheiks, preachers. This is because older people perceive us as criminals whilst using the net." Another noted, "When parents or teachers realise the problem is when kids share".

Participants noted several barriers to reporting abuse and/or exploitation, with fear of parents' responses being the highest and threats/blackmail from the perpetrator as second highest. Fear of parents' responses included harsh parenting - "When the parents are strict, instead of helping you they decide to punish you. This may prevent reporting"- including blaming the child - "Fear that when they tell parents they will be thoroughly beaten and get accused of watching pornography", thinking 'ill' of them - "Parents should mind the way they talk to their children and call them 'malaya'", beating them, stopping them using the internet and/or taking away their phone - "If I tell my mother she will take away the phone". Someone else said that the "harshness and strictness of parents, police and public" prevented them from reporting; someone else said "Friends tell you not to report". Another issue was the fear of losing a sponsor who the child perceives will change their life for the better.

Several children noted the potential implications of reporting – embarrassment and 'loss of dignity', "fear my reputation might be ruined", and "In the event you report the problem, it creates another bigger problem". Another participant said "many parents are illiterate and outdated so they are incapable of problem-solving online issues". One participant said that often children have a 'don't care' attitude that prevents reporting.

Many children were unaware of the safety measures in place to protect children online. Some of the measures outlined included reporting to a responsible adult including the police, changing settings to be the most secure they can be and setting passwords, and parental control of what children look at online. Children were also aware they can access support numbers, counselling and guidance. Not going to 'bad sites' was also discussed as a safety measure.

Children had many safety measures they thought should be in place, including better filtering of inappropriate and illegal content, monitoring children's online activity, having better prosecution of those who perpetrate OCSEA, having a basic online safety course for all children before they can own phones and using fingerprints to access the internet. Some participants said they would like to know current statistics on OCSEA in Kenya.

When asked what they would tell the government, they focused both on prevention and response, including blocking certain websites and apps (Phoenix was named) - "Ban apps that mislead and entice children online" and content (such as inappropriate content on YouTube) – "Take action on the production of immoral music videos", advertising the risks of specific sites, having more restrictions on apps such as age, locking accounts of those who perpetrate

OCSEA, having more apps that are educational for children and providing forums to educate parents, caregivers and other stakeholders – "Sensitise parents and children on proper use of internet"; "Teach online safety in the school syllabus". Regulating where children access the internet, especially cybercafes, was seen as important.

Children also outlined the need for better enforcement of legislation - "Enforce law on online content and how to handle it"; "Arrest and charge those who abuse children online", and specific policies that enable children to stay safe online - "Come up with policies that limit children's access to so much information". Children outlined the importance of government taking more direct responsibility - "The government should talk to parents regarding their children, especially those with social media accounts". And the need for improved victim/survivor support throughout the judicial procedure was highlighted: "Offer free legal support to children who are abused by the perpetrators"; "guidance and counselling".

Several participants highlighted personal fears of being restricted from using the sites and apps that they enjoy - "Please spare YouTube and TikTok; you can close the rest"; "I have an account on YouTube and I wouldn't want it blocked".

The majority of children do not feel comfortable sharing what they come across on the internet with a parent or caregiver. "We share only if we feel our lives are threatened". Participants clarified, "Some share the light content with parents and the heavy content with friends mostly"; "In the event you share, you can only share what parents can approve e.g. online shopping, online classes, lectures, preaching etc". Participants again referred to fear of their parents' responses - "Parents can cane you so you don't report to them". One participant said, "most of the time we use the internet without their [parents'] knowledge."

In general, facilitators noted that participants had a wide knowledge of internet use and raised many overarching concerns during the focus group discussions. There was active participation from everyone, which two facilitators outlined was specifically because boys' and girls' sessions were separate – "Separating boys and girls was important – more freedom to talk". One group was scared to disclose.

Whilst no safeguarding cases relating to participants was raised, two cases that are publicly known of were discussed: (1) a girl who disappeared and was found a few days later in a dumpsite having been sexually abused; the case is currently under police investigation, (2) a girl who was verbally abused by her mother who regularly called her names – she met someone online (Facebook), was abducted and is still missing. The case was reported but there has been no feedback so far.

Overview of findings from the online survey

Ten children aged 7 to 17 years old completed the survey; one girl and nine boys. 70% lived in a city and 30% in a town or village. None had a disability. All had permission from their parent/caregiver to complete the survey. 90% answered the survey with their parent/caregiver present, which may have affected their responses, particularly in light of the large number of children in FGDs who discussed not sharing concerns online with their parent/caregiver due to fear of punishment.

80% of participants said they think children should be aged 14+ to use the internet; the other 20% thought aged 7+. All participants thought there should be a minimum age requirement for using the internet. As with the FGDs, most children use the internet for online learning, watching videos and listening to music. All participants use the internet.

As with the FGDs, the most popular apps are Facebook (50%), YouTube (40%), WhatsApp (40%) and Instagram (30%). 90% said they use the internet more for online learning due to COVID-19; 20% to connect more with friends. When asked to rate how safe they feel (out of 100) when using the internet, the average rating was 57.

50% said they have engaged with a stranger online and another 10% said their friend had. Two said they mainly do so through online gaming. Whilst 50% have never seen anything that upset or worried them on the internet, the other 50% have seen inappropriate images of adults, 40% have also seen inappropriate images of children and 30% have been bullied online. One participant said they have been asked for inappropriate images of themselves and had sent them.

70% said they would tell a parent or caregiver if they experienced something that worried them online, 50% said they would tell a friend and 30% ChildLine. 20% said they wouldn't tell anyone and 10% said they were not sure what they would do. 20% said they would stop using the internet. 70% wanted their parent or caregiver to talk to them about staying safe online, 60% wanted to know more about the risks online themselves, 60% wanted better blocks on inappropriate websites and apps and 20% wanted more restrictions on internet access. 40% said their parent/caregiver already helps them to stay safe online. 80% felt that the community and religious leaders could do more to educate children on internet safety, 60% felt community and religious leaders could help them set up blocks and learn about the risks themselves and 50% said they wanted leaders to teach parents about internet safety, monitor public computers and support children to teach their parents about online safety. There were similar responses for the role teachers can play, though 90% felt that teachers need to learn more about internet safety so they can better protect children. 90% felt that if they know more about internet safety themselves, they can better support their friends to stay safe online. 70% also felt this will help them to set up blocks, educate their friends and know how to report concerns.

Informed consent form

For participation in the focus group discussion for children aged 13 to 17 on online child sexual exploitation (OCSEA) and abuse to inform Kenya's National Plan of Action on OCSEA.

The researcher has explained to me that *The Department of Children's Services, Maestral International and UNICEF* are doing research on child abuse that takes place, or is viewed online and what is and can be done about it. Someone has explained to me **why** the researchers would like to speak to me and may include my views, including what I say, in reports. I understand my name will **not** be used.

☐ I give consent for what I say, including quotes, to be used in this project including published reports and presentations that may be seen by people in this country and other countries. I understand they will not include my name and that no-one will be told where I live, or any other information that might identify me

I know *Maestral International* will keep a record of the focus group discussion safely in case I want to refer to what I said at a later date.

Name:…… Age (if under 18)……..

Signed:..... Date:.....

For children under 18 years old, the parent/caregiver is also required to give consent.

Relationship to the child: (parent/caregiver/other): _____

☐ I agree to the consent requirements outlined above by *[name of child]*

OR

☐ I do not agree to *[insert what you do not agree to]* of the consent requirements outlined above by *[name of child]*

Name:……

Signed:..... Date:.....

Name of researcher:……

Signed:..... Date:.....

Appendix – guidance on conducting FGDs with children for Kenya's action plan on OCSEA

Preparing for the FGDs

Selecting who to be present in the FGD: Ideally, participants should know the facilitators well. This enables a more open, honest discussion to take place and for the facilitators to identify if a child becomes upset during the discussion. However, if they do not know participants well, a trusted adult who does must be present (such as a staff member from the NGO who works with the children). Parents and caregivers should not be present as this may prevent children from talking openly.

Choosing a suitable venue: it is important to use a safe space for the FGD where participants can speak openly without being heard by anyone outside of the space.

Choosing who to participate: Between 6 to 8 children between 13 to 17 years old should participate. There should be a minimum of two FGDs – one for boys and one for girls. We strongly recommend that boys are in a separate FGD to girls to enable more open discussions.

NGOs may choose to ask children to nominate themselves to participate and select the first eight participants, or have another process they use for selecting participants. It is recommended that any child who is known to have experienced OCSEA does not participate unless they have counselling and other support services in place. If someone chooses to who is known to have experienced OCSEA, show them the questions prior to the FGD and discuss with them about only sharing what they feel comfortable sharing and getting support during the FGD if they need it.

Obtaining informed consent (see below and appendix A). Informed consent from all participants and their parent/caregiver must be obtained before the FGD takes place.

COVID-19-safe practices: a maximum of eight participants is recommended. Everyone eligible should wear masks; hand sanitizer and/or hand washing stations with soap should be available. Social distancing measures should be in place. All current COVID-safe recommendations and requirements must be adhered to.

Step 1. Verbally clarify informed consent

Informed consent is required for all participants before the FGD begins. Use the informed consent form in appendix A.

It is important to clarify verbally at the start of the FGD:

Purpose of the FGD:

- The purpose of this FGD is to gather your views on the opportunities and risks of the internet
- It will be used to develop ideas for putting Kenya's National Plan of Action on tackling OCSEA into action
- The project is being led by UNICEF and DCS, supported by Maestral International.

FGD structure:

- This FGD will take approximately one hour
- Notes will be taken to record your views. No names will be written down so that all views are anonymous. No information that might identify you (such as your school) will be recorded
- You are welcome to stop participating in the FGD at any time.

Answering questions:

- You have the right not to answer any question posed by the facilitator for any reason
- If a question is unclear, please ask for it to be repeated or re-worded
- When you give your views, you can speak about your own experiences and opinions, or you can speak on behalf of children you know, or who are in your community
- There is no right or wrong answer
- Please be as open and honest as you feel you are comfortable with
- If you tell us about abuse that is taking place or has taken place, we have a duty to report it. We will talk to you after the FGD about next steps and give you support.

Confidentiality:

- All FGD notes will be shared with the Maestral team afterwards; they will not be shared with any other organisations.
- Maestral will write a short report summarising all the views of participants in the four counties; names will be omitted from the report
- Interview notes will be stored securely at Maestral HQ in case you wish to view them in the future
- Non-identifiable data (such as gender, age bracket) may be shared with UNICEF and used in the report.

Safeguarding/child protection:

- Any safeguarding/child protection concern or disclosure (person under 18 years) may require Maestral, the Department of Children's Services and/or the NGO to take action that prioritizes the safety and well-being of the child in line with national laws.

Do you have any questions?

Participants then complete the informed consent form *(see Appendix A).*

Step 2. Introductions

The facilitator introduces themselves and ask participants to introduce themselves using first names only.

Step 3. Overview of the project

The field research team give an overview of the project and definition of OCSEA using age-appropriate language:

- Your participation is to help us to better understand the opportunities and risks of the internet for under 18s, particularly in light of being in a digital era and emerging trends in communication that increase children's use of the internet, which has been exacerbated by COVID-19
- Your views will help shape the development of actions in the national action plan that addresses OCSEA
- The project is led by UNICEF and DCS, supported by Maestral International
- So far, we have spoken to law enforcement, DCS, NGOs and the tech industry, but due to COVID-19 restrictions we were unable to speak to under 18s. Given the NPA is to help keep you safe online, it's really important you help shape the next steps.

Step 4. Overview of OCSEA

It is important to provide participants with a brief overview of OCSEA so that everyone has a clear, shared understanding of the topic before discussions take place. The overview should be tailored to participants, taking into account their ages, existing level of knowledge of OCSEA and other factors such as learning disabilities.

- By OCSEA we include (note – the language should be tailored to the level of understanding of participants):
    - **CSAM** – child sexual abuse material on the internet. It is imagery or videos which show a child engaged in or is depicted as being engaged in sexual activity, including their genitals or anus being touched; a child being told to touch their own genitals or anus; a sexual act being performed on a child or in the presence of a child
    - **Possession, production and sharing of indecent images of children and Prohibited Images**
    - **Online Grooming** - The act of developing a relationship with a child to enable their abuse and exploitation both online and offline
    - **Live Streaming** – Live streaming services can be used by Child Sex Offenders (CSOs) to incite victims to commit or watch sexual acts via webcam. CSOs also stream or watch live contact sexual abuse or indecent images of children with other offenders.
    - **Online coercion and blackmail** – The coercion or blackmail of a child by technological means, using sexual images and/or videos depicting that child, for the purposes of sexual, financial or other personal gain.

Children can also face other risks online, including bullying, coercion into other criminal activity such as trafficking or selling drugs.

Simplified language version:

- Sometimes people use the internet because they want to harm children. We will be looking today at OCSEA - online child sexual exploitation. By this we mean:
    - Sexual abuse images or videos of children **(CSAM)**
    - Someone older than you who pretends to be your friend but instead wants to harm you either online or offline **(online grooming)**
    - Someone who gets you to watch or participate in sexual acts using a webcam **(Live Streaming)**
    - Someone who blackmails you because they have personal information or images of you that you don't want to be shared with other people **(Online coercion and blackmail)**
    - Someone that has, or gets inappropriate images such as photos or video of children, including sexual images **(possession, production and sharing of indecent images of children and prohibited Images).**

Step 5: Ground rules

The facilitator reads out draft ground rules with participants. This is particularly important for FGDs and workshops. Ask participants if there are any ground rules they would like to change or add.

Participants agree to:

- Respect each others' views and opinions
- Not interrupt each other or cross-talk
- Not share anything personal said by others outside of the session
- Turn off mobile phones or turn them to silent
- Ask the facilitator if you would like them to repeat, rephrase or skip a question.

The facilitator will:

- Listen objectively to what you have to say
- Repeat, clarify or skip a question if asked

- Report any new concerns or disclosures about serious harm to a child or adult to ensure their safety and well-being is prioritized
- Keep your identity confidential in written notes.

If someone finds the FGD upsetting, participants are asked that they speak to the facilitator or the organization they are affiliated with. This enables the team to check individuals' well-being and get support for someone if they require it.

Step 6: Icebreaker

An icebreaker helps participants get to know each other and feel more comfortable giving their views during the discussion. See Appendix B for some icebreaker ideas.

Step 7: Questions for FGDs

1. How do children mostly access the internet? When and where (cinemas /movie theatres/cyber cafes)? Do many children you know have a webcam? Smartphone? Computer?
2. What apps are children using most?
3. Has how and how often you use the internet changed during COVID-19? If so, how?
4. What are some of the positive things about the internet and social media?
5. What do you think are some of the risks of being online? Are you aware of some risks of being online? If yes, mention them.
6. If you were worried about yourself or someone else online, who would you talk to about it? Do you know how and where you could report it?
7. What might hinder children from reporting their concerns?
8. Are you aware of some safety measures towards protecting children from online exploitation and would you like to know more about keeping children safe online and how to respond to concerns?
9. If you could tell the government one thing you would like changed to help keep children safe online, what would it be?
10. How often do you share what you come across on the internet with your parents/caregivers/guardians?

Note: if participants are mainly 13 to 14 years old and/or have learning disabilities, your organisation may instead choose to use activities to engage participants in the discussion.

Step 8: Ending the FGD

The facilitator:

- Thanks participants
- Checks if anyone has any questions
- Outlines where participants can access further information and support if they choose to
- Remains in the room for at least fifteen minutes to enable individuals who wish to make comments or ask questions outside of the FGD to do so.

Alternative FGD activities (where participants are mainly 13 to 14 years old)

Activity 1: Me and the internet (time: 25 minutes)

Materials: flipchart paper and pens; green and red paper (or two different colours of post-it notes); pens; scissors; glue

Instructions:

1. The facilitator brainstorms with the group:
    a. What do you use the internet for?
    b. What apps do you use most often?
2. The facilitator draws a tree with branches (no leaves) on the flipchart paper and a vertical line down the middle of the tree
3. Each participant is given a red and a green piece of paper. Ask participants to draw leaves on each piece of paper and in each green leaf, write or draw one positive of the internet and on each red leaf, one negative or risk
4. Participants cut out their leaves and stick them on the tree
5. Give participants time to look at each others' answers
6. Brainstorm together:
    a. What are the three biggest positives?
    b. What are the three biggest risks/challenges?

Activity 2: Reporting a concern (time: 15 minutes)

Materials: flipchart paper and pens (for facilitator only)

Instructions:

- The facilitator tells participants: "a friend of yours on an online game *[name a popular online game they play, such as Fornite]* asks you for a photo of you with your top off in exchange for some money so you can buy additional features in the game. What do you do?"
- Ask participants to talk to the person next to them for two minutes for ideas
- Brainstorm as a group. Then ask the whole group:
    - You report the concern to the police and child protection services. What should they do?
    - What support should you get?

Activity 3: Making the internet safer for me (time: 20 minutes)

Materials: flipchart paper and pens

Instructions:

1. The facilitator divides participants into smaller groups
2. Each group is given one stakeholder group to focus on (parents/caregivers; social workers; community and faith leaders; police; NGOs, CBOs and helplines; teachers)
3. Each group is given a piece of flipchart paper and pens. Ask each group:
    a. Make a poster showing what your group should do to address the risks/challenges you face on the internet. You can use drawings and/or write a message/messages
4. At the end of the activity, each group shows their poster to the other groups.
5.

Example icebreakers

1. There is a bowl of fruit or sweets (i.e. tropical mints, eclairs, ksl fruits). Each participant takes one but doesn't eat it (yet). Children with the same colour get into the same group (or with the same type of sweet). They have to introduce themselves and tell the others what their favourite food is.

2. Racing from one side of the room to the other e.g. bunny hopping; hopping; wheelbarrow racing (one child holds another child's ankles); pigeon steps (one foot touching the other when moving forward).

3. Problem-solving how to get a balloon from one side of the room to the other without it touching the ground (it cannot be carried). Props in the room can be used.

4. Internet-related: participants choose and mime an app for others in the group to guess. This can be done in small groups.