2022

A System for reporting online child abuse and offenders.

Maingi, Eunice M.
School of Computing and Engineering Sciences
Strathmore University

A System for Reporting Online Child Abuse and Offenders

By

Eunice M. Maingi

122719

Master of Science in Information Systems Security

October 2022

A System for Reporting Online Child Abuse and Offenders

By

Eunice M. Maingi

122719

Submitted in Partial Fulfilment of the Requirements for the Degree of Master of Science in Information Systems Security at Strathmore University

School of Computing and Engineering Sciences

Strathmore University

Nairobi, Kenya

October 2022

Declaration and Approval

Declaration

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the dissertation contains no material previously published or written by another person except where due reference is made in the dissertation itself.

Student's Name: Eunice M. Maingi

Sign: _____ _____ Date: ___24th Aug 2022_____

Approval

This dissertation of Maingi, Eunice M. was reviewed and approved by the following:

Dr. Joseph Sevilla,
School of Computing & Engineering Sciences,
Strathmore University

Dr. Julius Butime,
Dean, School of Computing & Engineering Sciences,
Strathmore University

Dr. Bernard Shibwabo,
Director of Graduate Studies,
Strathmore University

ABSTRACT

Online Child Abuse is a major public health concern that requires the combined efforts of all citizens to combat. The government, through legislation and the judiciary have the responsibility of setting up structures to protect children and stop online abuse, for instance, by curbing the production and distribution of Online Child Sexual Abuse Content. Those involved in the perpetration of these crimes should be appropriately prosecuted. In addition, measures should be set up to make reporting easy for the victims or anyone interested in giving a tip to the law enforcers. As knowledge is the first line of defence, a platform where citizens can access information on the variety of online child offenses prevalent in the country, legal implications of committing such offenses and prosecuted offenders is required. This information would inform and forewarn citizens. Kenya does not have such a system in place and relies on international databases for intelligence on harmful online activities directed to children in Kenya.

This project sought to tackle this lack of easily accessible information and reporting channels for online child abuse, especially online child sexual abuse, in Kenya. The general objective was to develop a national online system for reporting online child abuse and maintain a record of these abuses. This was achieved by obtaining an understanding of how online child abuse is currently dealt with in Kenya, highlighting and understanding any weaknesses noted. A review of online crime reporting systems in other countries was done to use them as benchmarks for the development of a reporting system for online child abuse in Kenya. A system to report online child abuse and maintain a record of these abuses was designed, developed, tested, and validated for adequacy in addressing the problem of reporting and maintaining a record of online child abuse.

Agile software development methodology was used to design, develop, and test the system. Agile development methodology focuses on the system features, while maintaining rapid iterations. As part of data collection, interviews were conducted. Respondents were obtained from child centric institutions and potential system users drawn from among the students, staff, and parents of Strathmore University. The System validation was done by creating some Law Enforcement agency users at different roles to confirm the systems effectiveness in receiving reports of Online Child Abuse and providing useful information and material for investigations.

Keywords: Child Online Protection, Online Child Abuse, Online Crime Reporting, Online Safety.

TABLE OF CONTENTS

List of Figures

List of Tables

List of Abbreviations

AHTCPU	-	Anti-Human Trafficking & Child Protection Unit
CA	-	Communications Authority of Kenya
COP	-	Child Online Protection
CSA	-	Child Sexual Abuse
CSAM	-	Child Sexual Abuse Material
DCI	-	Directorate of Criminal Investigation
GDPR	-	General Data Protection Regulation
INTERPOL	-	The International Criminal Police Organisation
KE-CIRT	-	Kenya Computer Incidence Response Team
NCMEC	-	National Centre for Missing and Exploited Children
OCSEA	-	Online Child Sexual Exploitation and Abuse
PII	-	Personal Identifiable information
SEC	-	Sexual Exploitation of Children
SECTT	-	Sexual Exploitation of Children in the Travel and Tourism Context

Definition of Terms

Child Online Protection: Child Online Protection (COP) refers to safeguarding a child from any form of exploitation and abuse propagated in and through the cyberspace (Kenya Law, n.d.-c).

Child Sexual Abuse (CSA): According to the World Health Organization (WHO) Child Sexual Abuse is the involvement of a child in sexual activity that he or she does not fully comprehend, is unable to give informed consent to, or for which the child is not developmentally prepared and cannot give consent, or that violates the laws or social taboos of society (World Health Organization et al., 2003).

Cyber Bullying: An aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself (Livingstone & Smith, 2014). There are many types of 'electronic' or cyber-aggression, including flaming, online harassment, cyberstalking, denigration (put-downs), masquerade, outing, exclusion, putting up false profiles and distributing personal material against someone's wishes (Pyżalski, 2012).

Cybercrime: Refers to criminal offenses committed on the Internet or aided using computer technology (NIST, 2019).

Cyber Grooming: Grooming refers to encouraging and preparing children for sexual abuse, violence and illegal acts through the sexual, religious, ideological or other impactful conversations (Andrews et al., 2020). It entails building an emotional connection with future intentions of sexual abuse, sexual exploitation, or trafficking.

Cyberspace: The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form (ISO/IEC JTC 1, Information technology, SC 27, IT Security techniques., 2012).

Digital Footprint: Digital footprints are the records and traces we leave behind us as we use the Internet, every time we use the Internet (Internet Society, 2021). It is a unique data trace of a user's activities, actions, communications, or transactions in digital media. This data trace can be left on the Internet, computers, mobile devices, or other mediums. A user can leave a digital footprint

either actively or passively, but once shared, a digital footprint is almost permanent in nature. A digital footprint can be used to track the user's activities and devices.

Online safety: It is the appropriate approach to personal safety when using digital technologies. It entails being aware of the nature of the possible threats that you could encounter whilst engaging in activity through the Internet. E.g., security threats, protecting and managing your personal data, online reputation management, and avoiding harmful or illegal content. While cybersecurity protects devices and networks from harm by third parties, Online Safety protects the people using them from harm by the devices and networks (and therefore third parties) through awareness, education, information, and technology (South West Grid for Learning, 2020).

Sexting: The sending or posting of sexually suggestive text messages and images, including nude or semi-nude photographs, via mobiles or over the Internet (Cooper et al., 2016).

Sextortion: It is old-fashioned extortion or blackmail, carried out over a computer network, involving some threat—generally but not always a threat to release sexually-explicit images of the victim—if the victim does not engage in some form of further sexual activity (Wittes et al., 2016). When carried out against children, sextortion involves a continuous process of children producing sexual material to avoid the blackmail.

Acknowledgements

This research project would not have been possible without the support of many people. Sincere gratitude to my supervisor, Dr. Joseph Sevilla, for his assistance, insightful comments and suggestions at every stage of the research project.

Also thanks to Strathmore University faculty and my colleagues in @iLabAfrica for the support they offered during the course of my Master's degree.

Thanks to my beloved family and numerous friends who endured this long process with me, always offering support and love. And Finally, thanks to God almighty for the opportunity and grace.

CHAPTER 1: INTRODUCTION

1.1 Background

The Internet offers a world of possibilities for us today in terms of education, communication, exchange of ideas on different matters of interest, nurturing creativity etc. The growing access to the Internet in Africa and specifically Kenya, occasioned by the Fourth Industrial Revolution which is driven by technology, has not only allowed the proliferation of good content but also of exploitation and abuse, more so of the most vulnerable in the society, that is, children, youth, and the poor (KAACR & ECPAT International, 2019). The Internet can expose children and young people to potential dangers like illegal content, harassment (e.g., in chat rooms), the misuse of personal data or grooming for sexual purposes.

Online child sexual abuse and exploitation refers to the production, dissemination, and possession of child sexual abuse materials; online grooming; 'sexting'; 'sextortion'; revenge pornography; commercial sexual exploitation of children; exploitation through online prostitution; and live streaming of sexual abuse using voice over Internet protocols, such as Skype (Quayle, 2016). A report by the International Society for the Prevention Against Child Abuse and Neglect observes that child sexual exploitation is one of the major public health concerns throughout the world (ISPCAN, 2016). Wangamati, Yegon, Sundby and Prince confirm the same (Wangamati et al., 2019).

Although child sexual abuse (CSA) is not contingent on and predates the Internet, forms of child abuse and their global reach are shaped by technology (Quayle & Koukopoulos, 2019). Protecting children and youth online is therefore a global problem that requires the effort of parents, teachers, guardians, governments, child centric organisations and the society at large. The contexts and manifestations of CSA are becoming increasingly complex and interlinked because of drivers like greater mobility of people, evolving digital technology and rapidly expanding access to communications (ECPAT, 2021).

As a signatory of the United Nations Convention on the Rights of the Child (UN Human rights, Office of the High Commissioner, 2021) and the African Charter on the Rights and Welfare of the Child (African Union, 2019), the Kenyan government is mandated to ensure that children are protected from sexual abuse through sound laws and policies. The government, through legislation

and the judiciary, has the responsibility of setting up structures to ensure that those involved in the production and distribution of harmful content are appropriately dealt with. Working together with the international community, several agreements, and laws to protect children and the youth from online harm have recently been signed into effect. However, the hurdle of their implementation needs to be addressed.

Child protection issues in Kenya are coordinated by the National Council for Children Services (NCCS) and the Department of Children Services. The two work together with other line ministries, the community and civil society in responding to child abuse and maltreatment. The role of NCCS includes being custodian of the Child Helpline (116), a role which includes the provision of premises, budgetary support, and the necessary personnel, and using data generated from the helpline to influence policy formulation in the child's best interest. NCCS also acts as a link between various government department and coordinates emergency responses, defines the criteria and standards for services for all children, investigates cases, undertakes rescue missions for children in distress, assists children access justice or any other service they may need and mobilizes resources to undertake publicity and awareness creation on these services (NCCS, 2017).

Kenya is concerned about the protection of children in general as seen in some government sources. However, information on forms of online child abuse is not provided, giving other forms of child abuse more visibility and publicity. This is seen, for instance, from the statistics maintained on the Kenya Child protection data website (https://data.childprotection.go.ke/archive/#000/AAAA/2018/ALL) where statistics on online child abuse do not appear, even though it is listed among the available categories of child abuse. Figure 1.1 and Figure 1.2 show child abuse statistics for the periods 2018/2019 and 2019/2020 respectively.

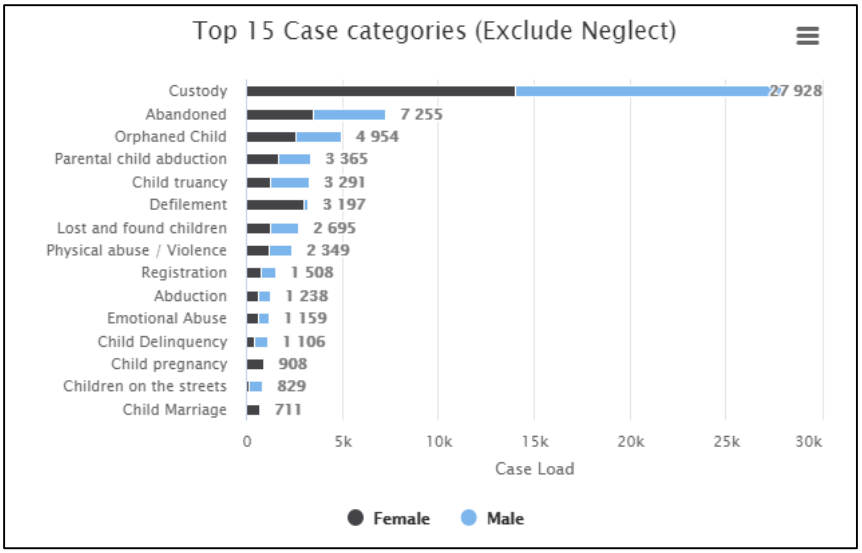


Figure 1.1: Top 15 Child Abuse Categories Excluding Neglect 2018/2019

Source: Kenya child protection website (https://data.childprotection.go.ke)

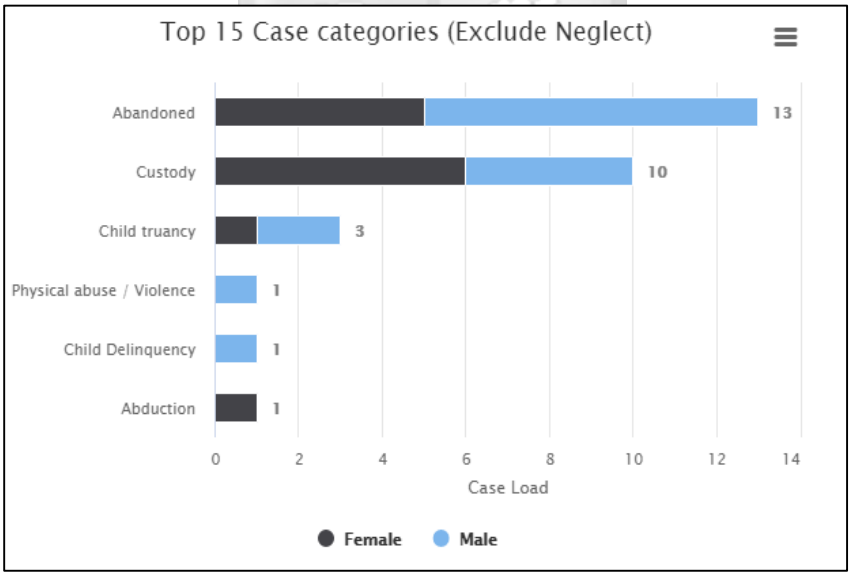


Figure 1.2: Top 15 Child Abuse Categories Excluding Neglect 2019/2020

Source: Kenya child protection website (https://data.childprotection.go.ke)

Even as the existing Child Helpline (116) deals with urgent child abuse cases reported by phone calls, there is need for a platform that can be used to submit online reports of child abuse. Such a platform could also act as an information bank containing images, videos and other helpful information for the investigation and prosecution of child abuse offenses. Other countries have

implemented such platforms to complement the call hotlines. Examples include the United Kingdom (Child Exploitation and Online Protection Command -CEOP), different states in the United Stated e.g. Illinois - Online Child Abuse Neglect Reporting (Governor, 2021), Missouri - Online System for Child Abuse & Neglect Reporting (Missouri Department of Social Services, 2021), Texas, Australia (Centre to Counter Child Exploitation, 2018), Luxenberg - The Luxembourg website for reporting child sexual exploitation (The Public Prosecutor's Office et al., 2021) etc. Some of these platforms allow anyone to report a case. However, on others, only mandated reporters are allowed to report cases of child abuse. Mandated reporters are designated persons who, because of their job role or position, have the obligation to report any child abuse that comes to their attention. Mandated reporters create accounts on the platform for reporting any cases.

1.2 Problem Statement

There is a scarcity of information and reports about online child abuse, especially online child sexual abuse e.g. possession and distribution of child sexual abuse images, grooming, sexting, soliciting sexual images, live streaming of child sexual abuse etc. in Kenya. This could be attributed to the lack of diversity in easily accessible reporting platforms available to a wide range of citizens. Currently, cases of online child abuse can only be reported by physically visiting a police station or calling the child helpline (116). A call must be answered for communication to happen. Further, a caller must be in an environment that is safe to speak for them to report. Assured storage of the reported information for subsequent reference and, where appropriate, sharing the same with other parties becomes difficult. Kenya does not have an online platform for reporting cases of online child abuse that can be used by the public to complement the Child Helpline. In other countries like Australia (Centre to Counter Child Exploitation, 2018), some states of the United States of America and Luxemburg (The Public Prosecutor's Office et al., 2021), an online reporting platform is used to complement the emergency helpline.

1.3 Research Objectives

1.3.1 General Objective

The aim of this research is to develop a national system for reporting online child abuse and maintaining a record of these abuses.

1.3.2 Specific Objectives

1. To review the current online child abuse handling process in Kenya, analyse and understand its weaknesses.
2. To review the online child abuse handling process in use in other countries.
3. To design, develop and test a national system for reporting online child abuse and maintaining a record of past online child abuse.
4. To validate the adequacy of the developed national system in addressing the problem of reporting and maintaining a record of online child abuse.

1.4 Research Questions

1. What is the current process for handling online child abuse in Kenya and its weaknesses?
2. What processes are in place in other countries to handle child online abuse?
3. How do we design, develop, and test a system for reporting and maintaining a record of online child abuse?
4. Is the developed system effective in reporting and maintaining a record of online child abuse?

1.5 Research Justification

According to the latest national census in 2019, the country's population was 47.5 million, of which around 21 million (46%) are children (Kenya National Bureau of Statistics, 2019a). Of the total population, 20.7 million own mobile phones, while 9.9 million use the Internet. Approximately 36% of the Internet users are children and young adults (Kenya National Bureau of Statistics, 2019b). These numbers depict the significant number of people with Internet connectivity, among them being children and young adults. The growing number of Internet users has led to a commensurate growth in online misconduct. Over the last two decades, online child exploitation, especially sexual exploitation has been on the rise (Wolak et al., 2012). In the United

States alone, the law enforcement agencies made an estimated 8,144 arrests in 2009 for technology-facilitated child sexual exploitation crimes, more than three times as many as in 2000 (Wolak et al., 2012). In September 2019 the New York Times noted that in the previous year technology companies reported to the US National Center for Missing and Exploited Children (NCMEC) over 45 million photographs and videos of children being sexually abused (Quayle, 2020). This was more than twice the number reported in the previous year. This could be attributed to factors like rural-urban migration, the breakdown of social morals and norms, increased national and international travel and tourism, and to a large extent globalisation, occasioned by the expansion of information and communication technologies and the Internet. The recent connection of Kenya to INTERPOL's International Child Sexual Exploitation (ICSE) database points to this increase (Interpol, 2019). To protect children from abuse, Kenya has ratified relevant international and regional conventions and treaties, enacted laws and developed policies with safeguards to protect children from abuse, especially sexual exploitation (Ministry of Labour and Social Protection, 2018).

Currently, Kenya does not have an online system for reporting online child abuse other than the National KE-CIRT (Computer Incidence Response Team), which is a general computer incidence reporting platform developed and managed by the Communications Authority of Kenya (Communications Authority of Kenya, 2021). The Directorate of Criminal Investigation (DCI) relies on international databases like National Centre for Missing and Exploited Children (NCMEC) and International Criminal Police Organisation's (INTERPOL) International Child Sexual Exploitation database (ICSE) to track online content and activities against children.

An online reporting database will be very useful in facilitating reporting, information storage and sharing, investigations, access to justice and rescue of victims. It will also act as a national repository for child abuse media which can be analysed for action on INTERPOL's International Child Sexual Exploitation (ICSE) database and a source of information for the citizens on the online risks children are facing in the country.

1.6 Scope and Limitations

This research focusses on the current reporting practice for child abuse in Kenya. The system developed will rely on the use of computers and other mobile enabled gadgets by all citizens in the country at large. Users who have smartphones will be able to report any incidences with more ease. However, users with lower models of phones will be unable to use this reporting platform.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

In the last decade, Kenya has seen remarkable improvements in Internet access because of increased urbanization, development of Internet infrastructure, and wide access to low-cost smartphones and tablets. According to the broadband connections as reported by CA in the Sector-Statistics report for 2020-2021 quarter IV, there are approximately 27.5 million Internet users in Kenya (Communications Authority of Kenya, 2021). This is about 55% of the country's population. Figure 2.1 gives a comparison of the two quarters and the percentage variation.

Table 19: Broadband Subscriptions

Indicator/Period	*Apr-Jun 21*	*Jan-Mar 21*	*Quarterly Variation (%)*	*Apr-Jun 20*
Total Broadband Subscriptions	**27,481,827**	**25,760,072**	6.7	**22,693,715**
Total Mobile Broadband Subscriptions	**26,757,648**	**25,070,158**	6.7	**22,084,104**
3G Broadband Subscriptions	13,841,463	13,326,007	3.9	14,074,018
4G Broadband Subscriptions	12,916,185	11,744,151	10.0	8,010,086
Fixed Broadband Subscriptions	**724,179**	**689,914**	**5.0**	**609,611**
Consumed Mobile Data Volumes (GB)	192,999,458	163,556,151	18.0	132,397,651

Source: CA, Operators' Returns.

Figure 2.1: Sector Statistics, Q4 2020/2021

Source: Communications Authority of Kenya – Industry Research and Statistics

Among these Internet users, the youth (15-24 years) is the most connected age group, as 71% are online in comparison to their being approximately 48% of the total population (UNICEF, 2017). Children and adolescents under 18 years old account for an estimated one in three Internet users around the world (UNICEF, 2017). Further, a growing body of evidence is showing that children are accessing the Internet at increasingly younger ages (UNICEF, 2017).

In the wake of the COVID pandemic, work and school activities were transferred to the digital setting leading to further growth in the number of Internet users in Kenya and globally. Consequently, a rise in online offences against children has been recorded, as notorious offenders are taking advantage of the situation. A recent alert by the DCI's Anti-Human Trafficking and Child Protection Unit (AHTCPU), encouraging citizens to report online crime attests to this. Though indirectly, the recent connection of Kenya to the INTERPOL's International Child Sexual Exploitation (ICSE) database also points to the existence of a need (Interpol, 2019).

2.2 Online Child Abuse: Definition and Categories

The boundaries between cybercrime and traditional forms of crime are not clear cut and are becoming increasingly blurred due to the level of hyper-connectivity in today's highly digitised and networked world (Sarre et al., 2018). The ubiquitous use of the Internet and smart mobile devices in people's everyday lives and the wide adoption of cloud-based services by industry and government have led to the widely accepted belief that almost all criminal activities include some cyber elements (Miraz et al., 2018). Child abuse predates digital technologies and the Internet. However, there are features of digital technology that have the capability to facilitate and increase the ease and scale of these activities. Research in these area has referred to these features as affordances. Affordances refer to the possibilities that an object offers for action, where the properties of the object emerge through the interaction between actors and the objects (Ben-Ze'ev, 1981). Strictly speaking, affordances are not merely static features, but relationships that ensue once a user perceives the feature and perceives the potential actions associated with it (Norman, 1988). Affordances of digital technologies which include persistence, replicability, scalability and searchability, in conjunction with the capabilities of online and networked technology such as social media, allow digital information to be easily copied (replicability), easily shared with large audiences (scalability), easily recorded and archived (persistence), and easily accessed by others and found in the future (searchability) (Quayle, 2020).

Online child abuse is a kind of cybercrime in which technology plays a role across a broad spectrum of activities (Quayle, 2020). Cybercrime can either be 'cyber-dependent', 'cyber-enabled' or 'cyber assisted'. 'Cyber-dependent' crime can only be committed using a computer, computer networks or other forms of information communications technology. On the other hand, 'cyber-assisted' crime, uses the Internet in its organisation and implementation, even though the crime would still happen without the Internet. (ICT) (McGuire & Dowling, 2013). As regards to the definition of cybercrime, the United Nations Office on Drugs and Crime acknowledging the lack of an international definition to cybercrime, uses the cyber-enabled-cyber-dependent dichotomy and adds a further specific-crime type: online child sexual exploitation and abuse, which includes abuse on the clear Internet, dark-net forums and, increasingly, the exploitation of self-created imagery via extortion, known as "sextortion" (UNODC, 2022).

Online abuse can either be cyberbullying and online sexual abuse.

2.2.1 Cyberbullying

Cyberbullying or online bullying is an intentional and recurring violence (rough and threatening behaviour) done through computers, cell phones, and any other devices that can be connected to the Internet according to Rosen et al. (Akbar et al., 2020). This definition brings these important elements: Intentional: the behaviour is not incidental but intentional, recurring: the behaviour is not merely one event of an occurrence but something that happens repeatedly, endanger: the target of bullies must feel the danger resulting from such behaviour, electronic devices e.g. computers, cell phones etc., which makes cyberbullying differ from traditional bullying. It is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself (Livingstone & Smith, 2014). There are many types of 'electronic' or cyber-aggression, including flaming (online contention), online harassment (repetitive actions, sending offensive messages to the target/victim), cyberstalking (using any electronic devices to stalk others by sending repetitive threatening messages), denigration (put-downs), masquerade (adopting an online persona to bully a known person while hiding ones identity), exclusion (exclusion of someone from an online activity, group chat or a game with the intent that the person sees they are being excluded), impersonation (imitating others' identities and uploading any material to harm the reputations of whom the identities were imitated) and outing (sharing a person's personal information without his consent) (Pyżalski, 2012).

2.2.2 Online Child Sexual Exploitation and Abuse (OCSEA)

Child sexual abuse refers to the involvement of a child in sexual activity that he or she does not fully comprehend, is unable to give informed consent, is not developmentally prepared and cannot give consent, or that violates the laws or social taboos of society (World Health Organization et al., 2003).

Online Child Sexual exploitation and abuse (OCSEA) is the abuse of children by force or through enticement to take part in sexual activities where the online environment is involved at any stage of the offence (May-Chahal et al., 2018). Forms of online child sexual abuse include the production, dissemination and possession of child sexual abuse images (known in many jurisdictions as child pornography), online grooming of children for sexual purposes, 'sexting',

sexual extortion of children ('sextortion'), revenge pornography, commercial sexual exploitation of children, exploitation of children through online prostitution, and live streaming of sexual abuse (Quayle, 2016).

2.2.3 Effects of Online Child Abuse

The effects of online child abuse experienced in short term and long term range from anxiety, which is the result of chronic stress on the child, which in turn causes the child to be on edge always or constantly afraid that they will get hurt again (Allan, 2022) to clinical depression manifested by increased sadness, anger and irritability when exposed to gadgets that brought about abuse. Other effects include low self-esteem, post-traumatic stress, self-harm and suicidal tendencies or thoughts.

Although Technology Assisted Child Sexual Abuse (TA-CSA) is sometimes viewed as less serious than offline CSA, studies show the emotional, psychological and behavioural outcomes to be the same (Hamilton-Giachritsis et al., 2020). Moreover, online and image dimensions, such as increased victim participation, deception in images and image dissemination, may worsen the impact and recovery of the victim (Hanson, 2017).

2.3 Legal Instruments for handling online child abuse: Global Landscape

As outlined in the ITU Guidelines for Policy Makers on Child Online Protection 2020, global, a variety of legislation and other initiatives have been adopted on national and international levels to address the usage and risks associated with ICT for children (ITU, 2020). Some of these initiatives include Regional and National models like the:

1. Audio-visual Media Services Directive (AVMSD) of the European Union (2018)
2. General Data Protection Regulation (GDPR) of the European Union (2018)
3. Age-Appropriate Code Design of the UK (2019)
4. The Harmful Digital Communications Act of New Zealand (2017)
5. The eSafety Commissioner in Australia (2015)

Other international initiatives include world reports and statistics published by institutions on the frontline in the fight for children rights, awareness campaigns and elimination of exploitation. These include:

1. ITU Guidelines for Policy Makers on Child Online Protection (ITU, 2020) which are published periodically. They are a product of extensive collaborative research and are openly available for guidance by any entity.
2. The International Child Sexual Exploitation Image Database (INTERPOL, 2021). In May 2019, Kenya became the first African country to connect to this database as one of the government's initiatives to combat online exploitation of children.
3. The WeProtect Global Alliance resources (WeProtect Global Alliance, 2021).
4. The DQ Institute 2020 Child Online Safety Index (COSI) (DQ Institute, 2021).
5. ECPAT reports and resources (ECPAT International, 2021).

Most of these resources are publicly available and free for adoption and benchmarking by any nation.

2.4 Cross Border Governance

Kenya is a signatory to various international and regional instruments that protect the rights of children. These include:

2.4.1 The United Nations Convention on the Rights of the Child (UNCRC)

Kenya Ratified the UNCRC in 1990 becoming part of the 192 countries that have adopted this convention. The Convention has 54 articles on all aspects of the rights of a child in the civic, economic, social, and cultural ambits. The rights outlined here, which ought to be taken as a whole, are linked to each other. It also explains how adults and governments should work together to make sure all children can enjoy all their rights, which every child possesses, regardless of their ethnicity, gender, religion, language, or abilities (UN Human rights, Office of the High Commissioner, 2021).

2.4.2 The African Charter on the Rights and Welfare of the Child (ACRWC)

The African Charter on the Rights and Welfare of the Child (ACRWC) is an important tool for advancing children's rights. While building on the same basic principles as the UN Convention on the Rights of the Child, the AU Children's Charter highlights issues of special importance in the African context (African Union, 2019). Kenya ratified this charter in 2020.

2.5 Legal Landscape: Kenya

Legislation plays a key role in combatting any illegal activities in a society. It outlines the acceptable conduct, in addition to penalties related to non-adherence. The Kenyan government has defined different legislative measures to regulate online conduct, activities, and content. Some of them are described below:

2.5.1 The Data Protection Act - Personal Identifiable Information (PII)

In 2019, the government of Kenya passed to law the Data Protection Act. The purpose of this act is the enforcement of Article 31 of the Constitution of Kenya, which contains the right to privacy, establish the office of the data commissioner, regulate the processing of personal data, provide the right of data subjects and obligations of data controllers and data processors. It gives direction on the management of Personal Data in the information life cycle and the commitment of the Government of Kenya to protect the Personal Data including the Personal Sensitive Data (Data Protection Act, 2019).

According to this policy, personal data is defined as any information relating to an identified or identifiable natural person (Data Subject) (Data Protection Act, 2019). An identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity (Data Protection Act, 2019).

In the same act, sensitive personal data is defined as data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex, or the sexual orientation of the data subject (Data Protection Act, 2019).

In dealing with online abuse of children, the provisions of the data protection act are essential and applicable in protecting the identity of the victim and offender. Examples of rights on this act that apply to this are ‘the right of rectification and erasure’ and ‘processing of personal data relating to children’.

2.5.2 Cybercrime and Computer Misuse Act, 2018

The Computer Misuse and Cybercrimes Act of 2018 is an ACT of Parliament to provide for offences relating to computer systems; to enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes; to facilitate international co-operation in dealing with computer and cybercrime matters; and for connected purposes.

Among the offences listed in this act are unauthorized access, access with intent to commit further offence, unauthorized interference, publication of false information, child pornography, cyber harassment, identity theft and impersonation, phishing, interception of electronic messages or money transfers, cyber terrorism, and wrongful distribution of obscene or intimate images (Computer Misuse and Cybercrimes Act, 2018).

2.5.3 Victim Protection Act, 2014

The Victim Protection Act of 2014 was enacted to provide for protection of victims of crime and abuse of power by providing them with better information and support services for reparation and compensation, providing special protection for vulnerable victims, and for purposes of being connected. The provisions of this act apply also to those implicated in the Sexual Offences Act of 2006 which extends to online sexual offences.

This act established the Victim Protection Board to enforce the act by implementing the preventive, protective and rehabilitative programmes of victims of crime (Victim Protection Act, 2014).

2.5.4 Counter Trafficking in Person's Act, 2010

This act of parliament was enacted in 2020 to implement Kenya's obligations under the United Nations Convention against Transnational Organized Crime particularly its Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children; to provide for the offences relating to trafficking in persons (Counter Trafficking in Persons Act, 2010).

2.5.5 Children's Act, 2001

This is an Act of Parliament that makes provision for parental responsibility, fostering, adoption, custody, maintenance, guardianship, care and protection of children, administration of children's institutions and gives effect to the principles of the Convention on the Rights of the Child and the African Charter on the Rights and Welfare of the Child (Children Act, 2001). Part II of this act is

of particular interest as it covers the 'Safeguards for the rights and welfare of the child', including matters like protection from abuse, harmful cultural rites, and sexual exploitation among others.

2.5.6 Sexual Offences Act, 2006

This Act of Parliament makes provision about sexual offences, their definition, prevention, and the protection of all persons from harm through unlawful sexual acts, and for connected purposes (Sexual Offenses Act, 2006). It was passed in 2006.

2.5.7 Industry Guidelines for Child Online Protection and Safety in Kenya, 2022

In March 2022, the Communications Authority of Kenya drafted the above Industry Guidelines for Child Online Protection (COP) and Safety in Kenya and submitted them for public consultation. These guidelines fall under Section 4, 9 and 21 of the Kenya Information and Communications (Consumer Protection), Regulations 2010. They form a basis for the design, development, deployment, commissioning, use, management, sale, marketing and publicity of communication products and services in Kenya that may be accessed and/or targeted for use by children so as to provide safeguards for children's access to and use of ICT services in Kenya.

2.5.8 Discussion on Policies and Laws

From the policies discussed in the above section, both cross border and local instruments, Kenya is aware of its legal responsibilities for the protection of its citizens and especially children. Further, appropriate legislation has been adopted locally and ratified from the regional instruments to ensure that the citizens are well guided and guarded by the existing laws. Appropriate guidelines governing the operation of the communication industry, content developers and providers is also in the process of development.

In liaison with the citizens and the legal bodies, most of these laws have also been revised to address some omissions and changing landscapes in the legislated ambit. This is evident in the fact that most of them have had revisions and amendments effected after their being passed. For instance, the counter trafficking in persons act of 2010 was revised in 2012, the children act of 2010 was also revised in 2012, and an amendment bill was passed in 2016 for the sexual offenses act of 2006.

2.6 Government Institutions Dealing with Online Child Offences in Kenya

2.6.1 Child Welfare Society of Kenya (CWSK)

The Child Welfare Society of Kenya is a State Corporation for the care, protection, welfare, and adoption of children through the Legal Notice No. 58 of 23/05/2014. It is the National Adoption Society for Kenya and the National Emergency Response, Welfare and Rescue Organization for children. The government agency was established and gazetted in 1955.

CWSK has a statutory responsibility to provide services to all marginalized children across all social sectors in line with Section 56 of the constitution. Its programmes are tailored to meet the affirmative action necessary for the children to access welfare services across the country. Its programmes include emergency preparedness, rapid response and rescue of separated children, advocacy; HIV/AIDS, child adoption, foster care for orphans and other vulnerable children, child labour, street children, rescue shelters, vocational skills training, child rights and community empowerment, early childhood education, education sponsorship, and other such opportunities.

The organization carries out its programs throughout the 47 counties in the country. CWSK is also a member of the international social services and the global professional body of social workers, which has a membership of 150 countries. (Child Welfare Society of Kenya, 2021)

2.6.2 National Council for Children Services (NCCS)

Established under section 30 (1) of The Children Act of 2001, the National Council for Children's Services (NCCS) is a corporate body with the mandate to supervise and control the planning, financing, and coordination of child rights activities. It is the government's advisor on all aspects related to children, coordinating and guiding children's activities in their areas of operation (National Council for Children's Services, 2017).

In line with their mantra "Our Children Our Responsibility", NSSC formulates policies, develops plans, monitors, coordinates, and mobilizes resources for the implementation, realization and safeguarding of the rights and welfare of the child (National Council for Children's Services, 2017).

2.6.2.1 The Child Help Line (116)

The NSSC is also the custodian of the child help line (116) which became operational in March 2008. It was established to provide a 24-hour free emergency public line for reporting any cases

of children in danger and thus in need of care and protection. Among other information, the child help line together with the DCI maintains a national data base (CPMIS) of calls made on child issues, acts as a referral center for abused children in need of therapy referrals, offers a networking avenue linking those in need with support systems for the rehabilitation of abused children and advices, counsels and assists parents experiencing difficulties with children (National Council for Children's Services, 2017).

2.6.3 Ministry of Labour and Social Protection - Department of Children Services

Under the Ministry of Labour and Social Protection, the Department of Children Services (DCS) is the government function charged with safeguarding and protecting the rights and welfare of children for national prosperity as per the Children Act (2001). It does this by leading, overseeing, planning, and coordinating child protection programs and services in Kenya.

In discharging its functions, DCS refers to international Instruments (UNCRC), Regional Instruments (ACRWC), the Kenyan Constitution, other relevant statutes, the Children's Act, Policies, Manuals, guidelines, regulations, and National Plan of Actions.

2.6.4 DCI Anti– Human Trafficking & Child Protection Unit

Under the DCI is the *Anti-Human Trafficking & Child Protection Unit* (AHTCPU) which has the following core functions:

- Carrying out investigations on cases of child sexual exploitation and abuse.
- Undertake investigations on cases of child trafficking.
- Rendering advice to police officers and other stakeholders' country wide on reported child sexual exploitation and abuse.
- Taking over cases of child sexual exploitation and abuse from other police stations country wide that have been poorly investigated.
- Coordinating with Interpol office, National and International law enforcement agencies on cases of child sexual exploitation and abuse.
- Liaising with the department of children services and non-state actors in identifying, rescuing sexually abused children.

Guided by the principles of the child's best interest, child participation, do no harm and non-discrimination, AHTCPU ensures the enforcement of children's rights and punishes offences committed against children (Directorate of Criminal Investigations, 2020).

An important resource provided by the AHTCPU is the Children Protection Information Management System (CPIMS). This is a public dashboard that contains statistics of a variety of reported issues of concern that are facing the children in Kenya. The offenses against children as listed on the DCI page e.g., neglect/ abandonment, child trafficking, abduction and kidnapping, child labour, emotional abuse, female genital mutilation, physical abuse, sexual abuse (defilement, sexual assault, and indecent acts), forced marriage, child stealing, child online sexual exploitation, etc. are maintained on CPMIS and the statistics of the same available for public viewing.

2.6.5 Communications Authority of Kenya and the KE-CIRT

In 2014, the Communications Authority of Kenya (CA) in a bid to localise this initiative conducted child online protection campaigns. In 2018, they produced a COP booklet with content to train children on online child safety and a brochure on 'Children and the Use of Internet' accessible on their website (Communications Authority of Kenya, 2018). The campaign seeks to provide consumers, especially children and youth, with information and skills to practice safe Internet use and minimize exposure to risks and vulnerabilities. To ensure that the campaign is effective, CA has partnered with various organisations including Department of Children Services, The Cradle, Kenya Girl Guides Association, Kenya Scouts Association, Kenya Association of Professional Counsellors, UNICEF, Google, Plan International, Terre de Hommes, Childline Kenya, GSMA and mobile service providers Orange, Airtel and Safaricom (Communications Authority of Kenya, 2018).

Another important role that the CA does is in line with the national KE-CIRT (Computer Incidence Response Team), a general computer incidence reporting platform which the Communications Authority of Kenya has developed and manages (Communications Authority of Kenya, 2020). Recently, the KE-CIRT has been updated with a page for reporting online child abuse, which can be complemented by the system being developed. Further, CA has been organising events to mark the global 'Safer Internet Day' annually in February.

2.6.6 Kenya Film Classification Board (KFCB)

The Kenya Film Classification Board (KFCB) is a State Corporation established under the Films and Stage Plays Act Cap 222 of the Laws of Kenya to regulate the creation, broadcasting, possession, distribution and exhibition of film and broadcast content with the aim of promoting our culture, National values and aspirations as well as protecting children against exposure to harmful content. The Kenya Information and Communications Act (KICA) empowers the Board to impose age restrictions to ensure that content which depicts or contains scenes that are rated as adult or are of the language intended for adult audiences are not aired during the watershed period (between 5 am –10 pm). KICA also mandates the Board to enforce the programming Code for the free-to-air radio and TV services by ensuring that all programme and non-programme matter, namely: commercials, infomercials, documentaries, programme promotions, programme listings, community service announcements and station identifications are classified before they air (Kenya Film Classification Board (KFCB), 2021).

2.7 Online Child Abuse Reporting in Other Countries

2.7.1 Australia

Australian government though the department of child protection has availed an online platform for child abuse reporting to be used by the citizens. On this website, visitors are given guidelines on the Child Abuse Reporting Line (CARL) number to call for cases where a child is in immediate danger. Further guidelines on what to look out for as indicators of abuse in a child, what to report and what not to report as child abuse are given. A section on mandated notifiers is included where their roles are outlined and a guide on preparing a child abuse report given. A snapshot of this page is given on Figure 2.2.

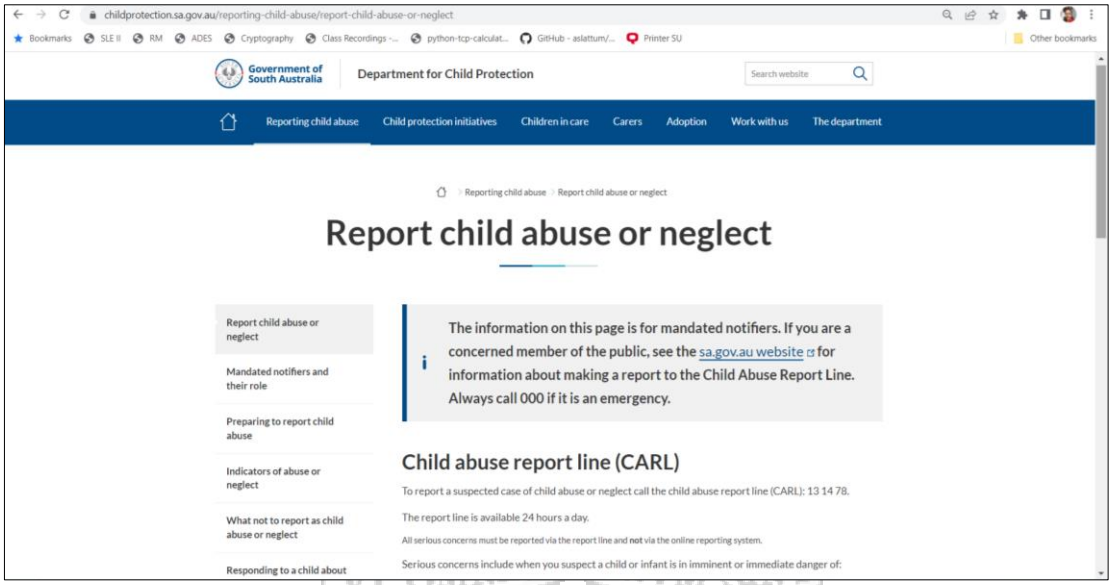


Figure 2.2: Australian Government Platform for Reporting Child Abuse

Source: Government of South Australia – Department of Child Protection

An option for reporting online is given too. For one to file a report, they have to be a registered user with an account. Only mandated notifiers are allowed to report on this platform. A snapshot of the page is given on Figure 2.3.

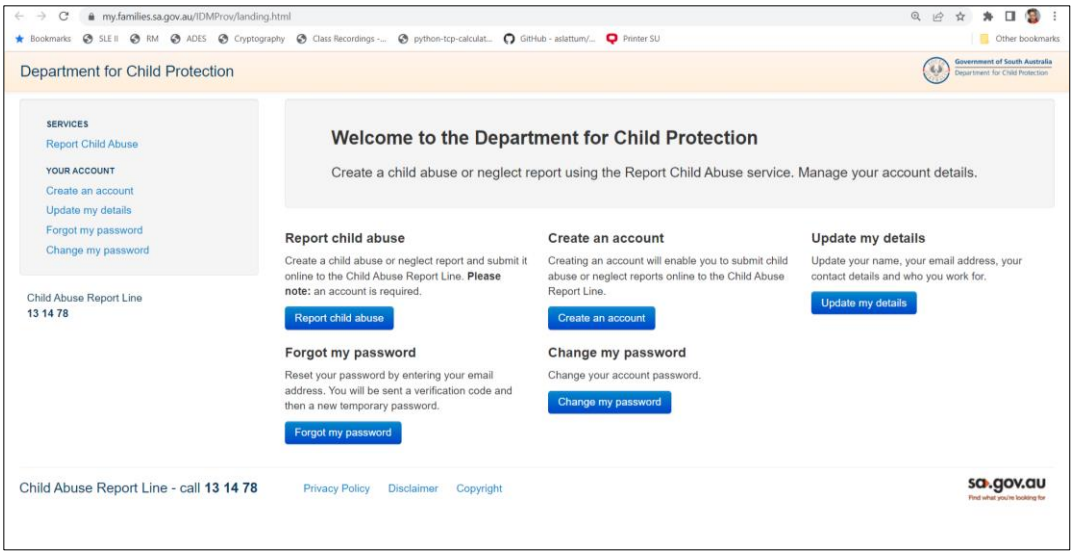


Figure 2.3: Australian Government Platform for Reporting Child Abuse – Account Creation

Source: Government of South Australia – Department of Child Protection

Further, the Australian centre to counter child exploitation (ACCCE) offers another platform where anyone can report inappropriate behaviour towards children online. A link to this page is also provided on the federal police website in case anyone needs to file a report. The option to call the helpline, report on a private call or even to report online are given. Anyone can report any category of online child abuse. On the side, there is a 'quick exit' button to allow the reporter a quick exit from the page in case of need. See a snapshot on Figure 2.4.

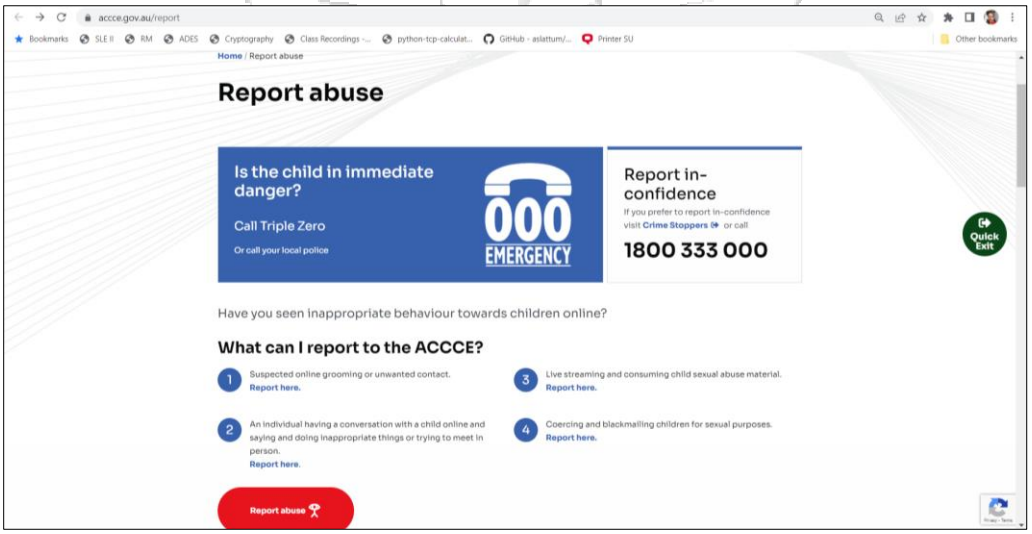


Figure 2.4: ACCCE – Report Abuse Platform 1

Source: Australian Centre to Counter Child Exploitation (ACCCE)

Other forms of online abuse that can be reported on this page are image-based abuse, illegal and harmful content, cyber bullying as shown in Figure 2.5 and Figure 2.6.

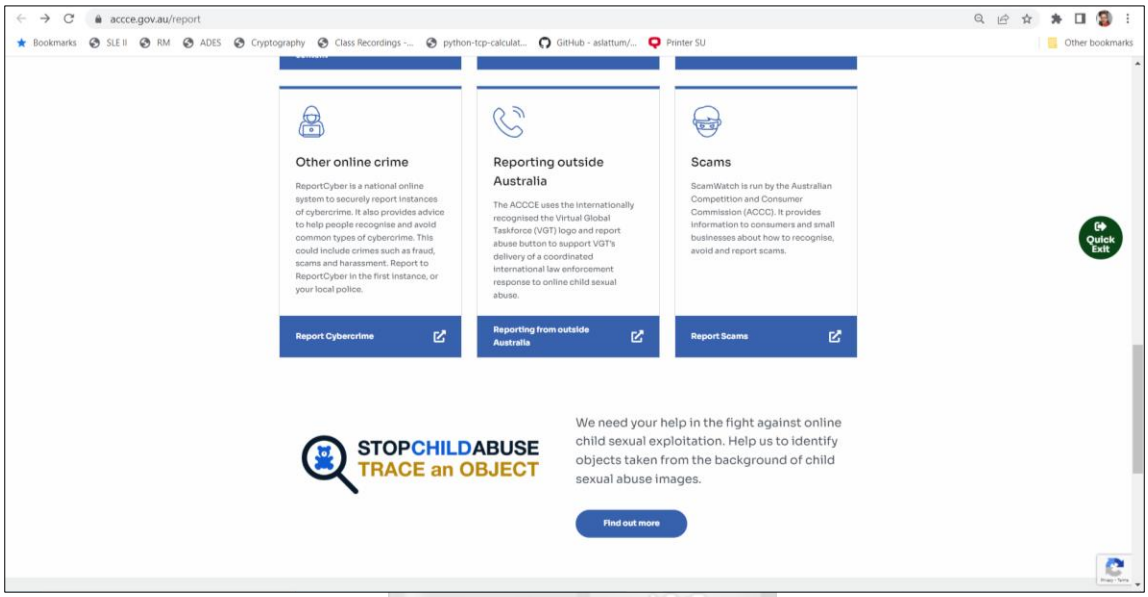


Figure 2.5: ACCCE – Report Abuse Platform 2

Source: Australian Centre to Counter Child Exploitation (ACCCE)

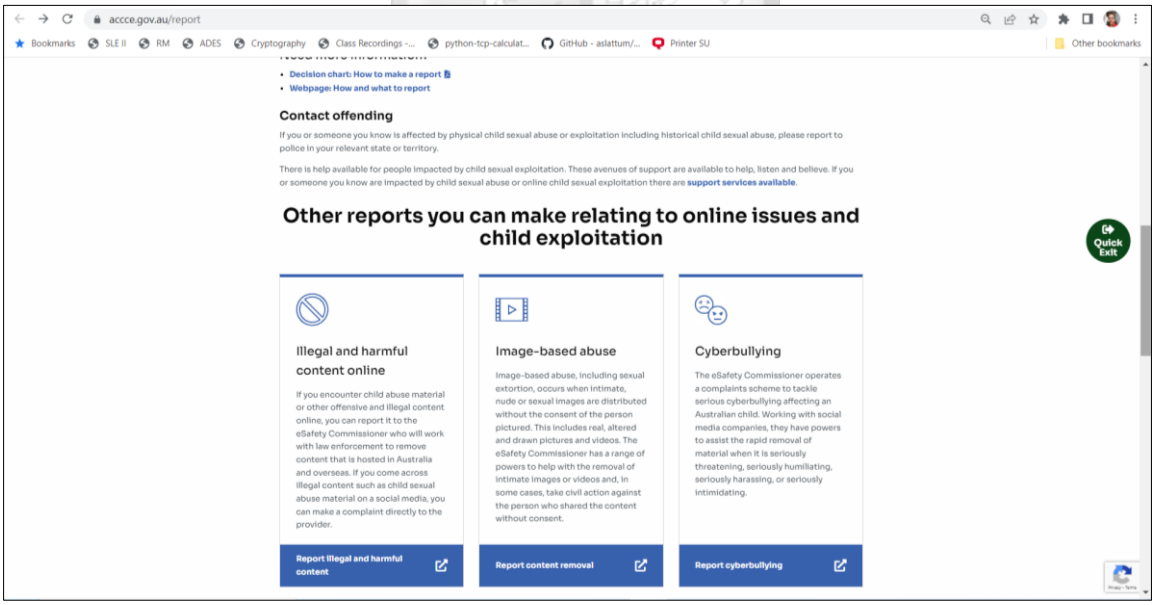


Figure 2.6: ACCCE – Report Abuse Platform 3

Source: Australian Centre to Counter Child Exploitation (ACCCE)

Further, the platform is also used to help the law enforcement get useful information for ongoing investigations in online child abuse. By helping trace an object obtained from a child abuse image, members of the public can help accelerate the process of identifying a victim or perpetrator. See Figure 2.7 and Figure 2.8.

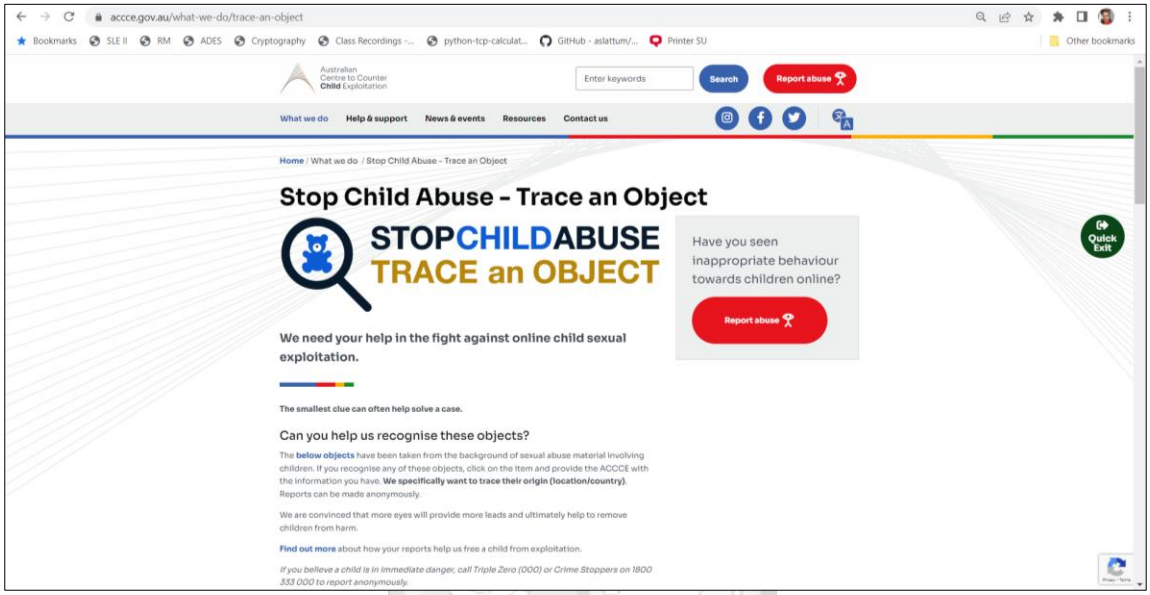


Figure 2.7: ACCCE – Trace an Object 1

Source: Australian Centre to Counter Child Exploitation (ACCCE)

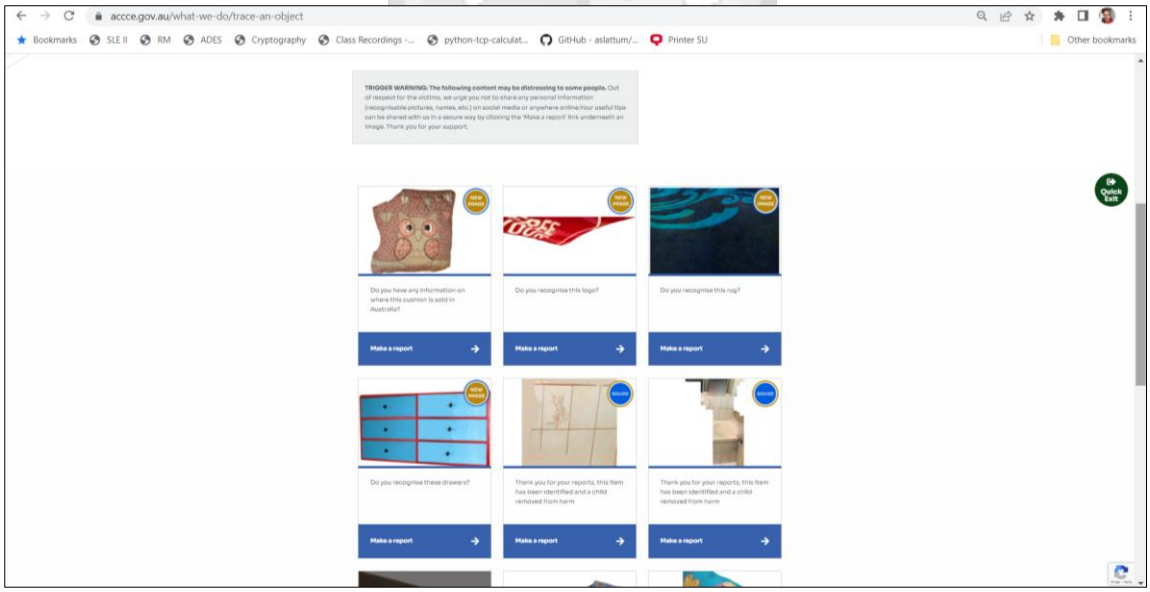


Figure 2.8: ACCCE – Trace an Object 2

Source: Australian Centre to Counter Child Exploitation (ACCCE)

2.7.2 United Kingdom (UK)

The government of the UK also provides a platform to report child abuse online where the free call lines and the online reporting link are given for cases that are not emergencies. See Figure 2.9.

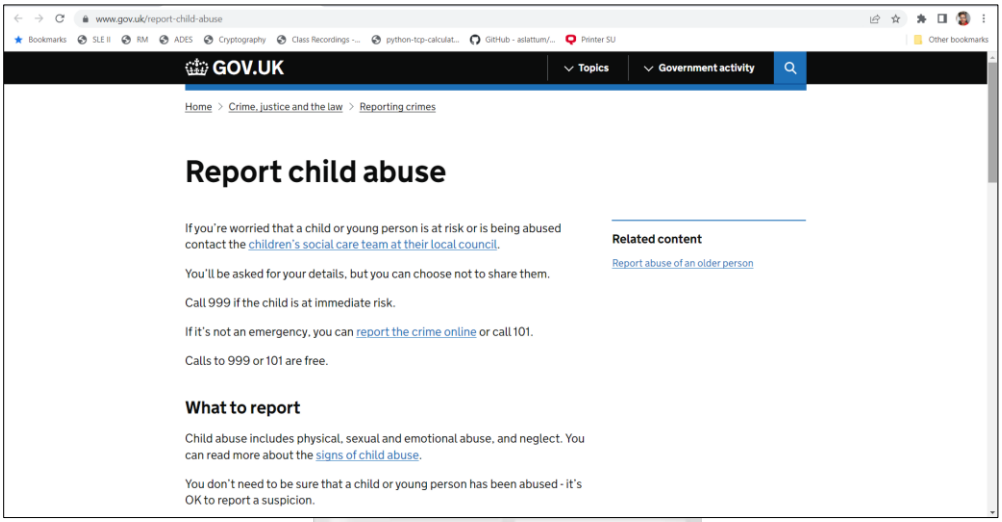


Figure 2.9: Government of UK - Report crimes

Source: Government of UK Services (www.gov.uk)

Further, through the national crime agency command, a platform for Child Exploitation and Online Protection command is available and accessible to any member of the public for reporting. See Figure 2.10.

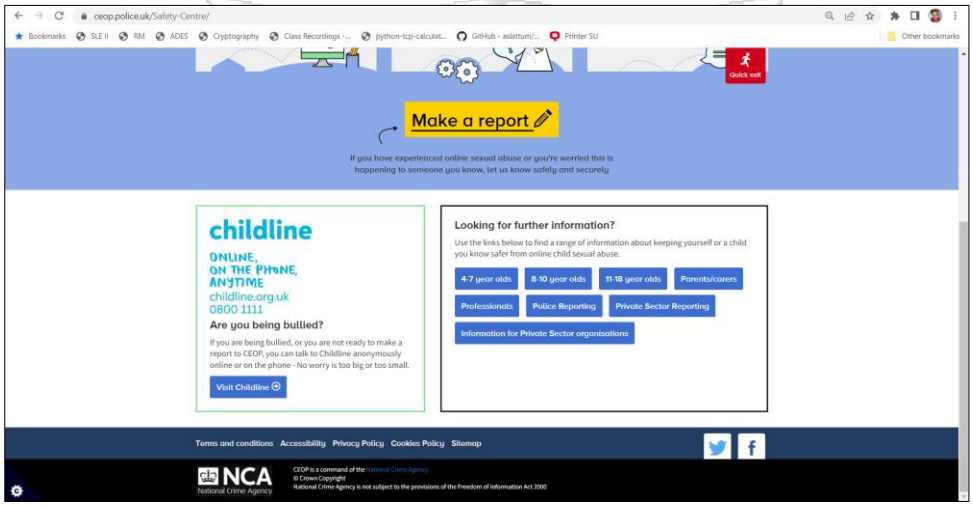


Figure 2.10: Child Exploitation and Online Protection – Reporting Website

Source: Child Exploitation and Online Protection Command

2.7.3 USA and Luxemburg

Different states of the USA and Luxemburg also offer its citizens a platform to report child abuse online with basic information on what and how to report. See Figure 2.11 and Figure 2.12 for the Luxemburg page.

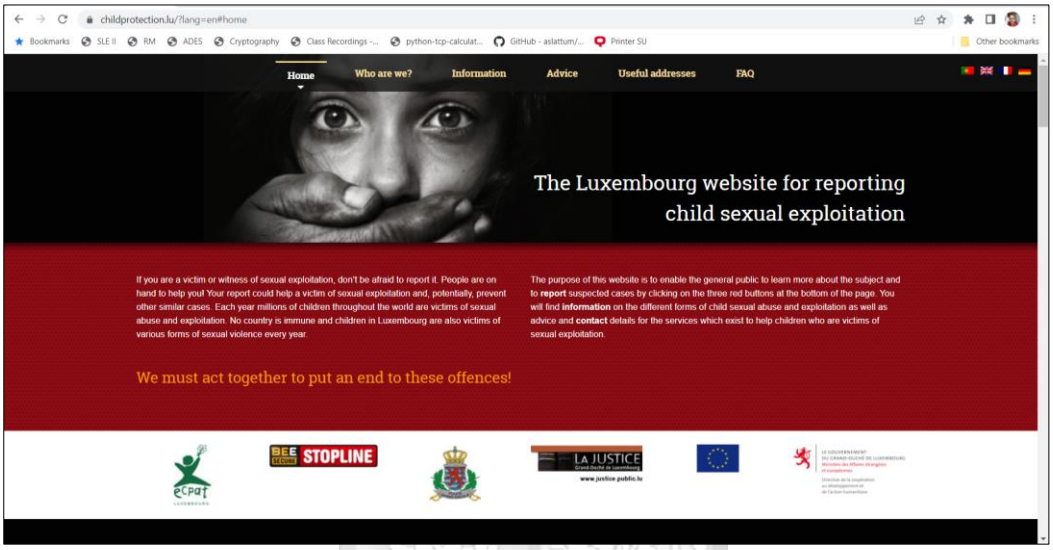


Figure 2.11: The Luxembourg Website for Reporting Child Sexual Exploitation

Source: Child Protection Luxembourg

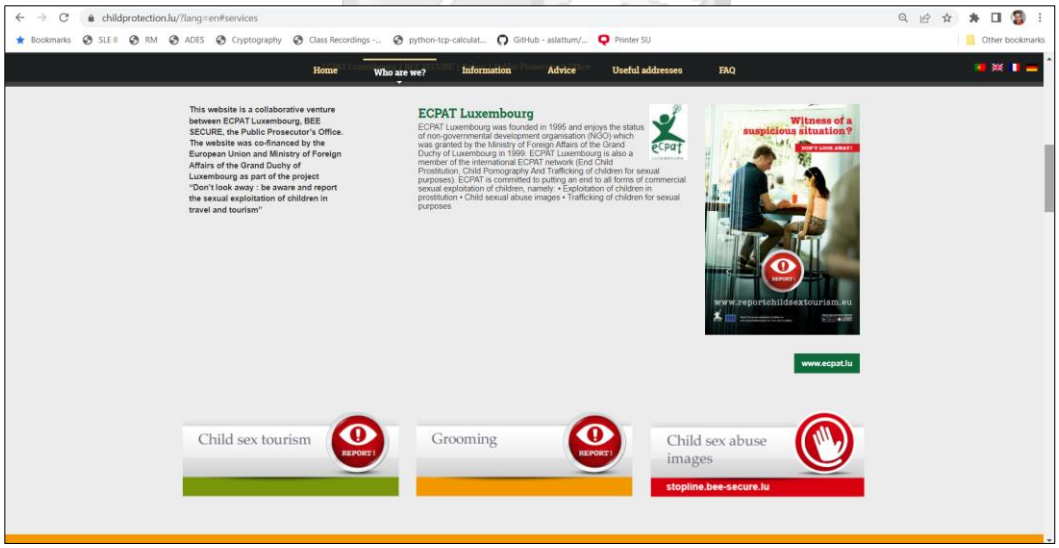


Figure 2.12: The Luxembourg Website for Reporting Child Sexual Exploitation

Source: Child Protection Luxembourg

A snapshots of the reporting page of the USA government is shown in Figure 1.1Figure 2.13.

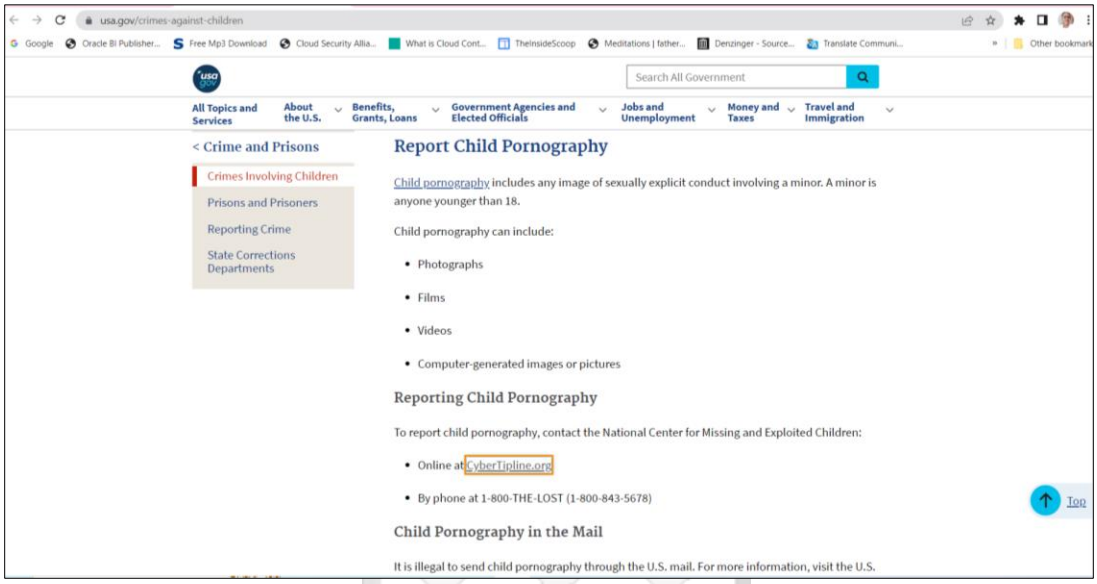


Figure 2.13: USA Government Online Reporting Page for Crimes Against Children

Source: Crimes Involving Children - USA Government

Child online abuse, referred to here as 'Child Pornography' is reported through a link given to the CyberTipline.org. See Figure 2.14, Figure 2.15 and Figure 2.16 for the landing page and some of the information provided and required when one is using this page to report online child abuse.

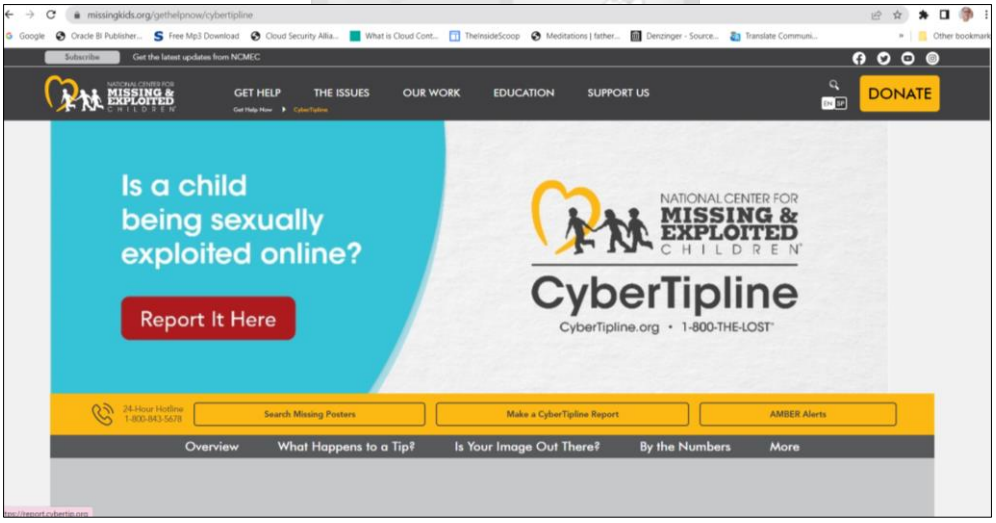


Figure 2.14: On clicking the Link to CyberTipline (To report online child abuse)

Source: Crimes Involving Children - USA Government

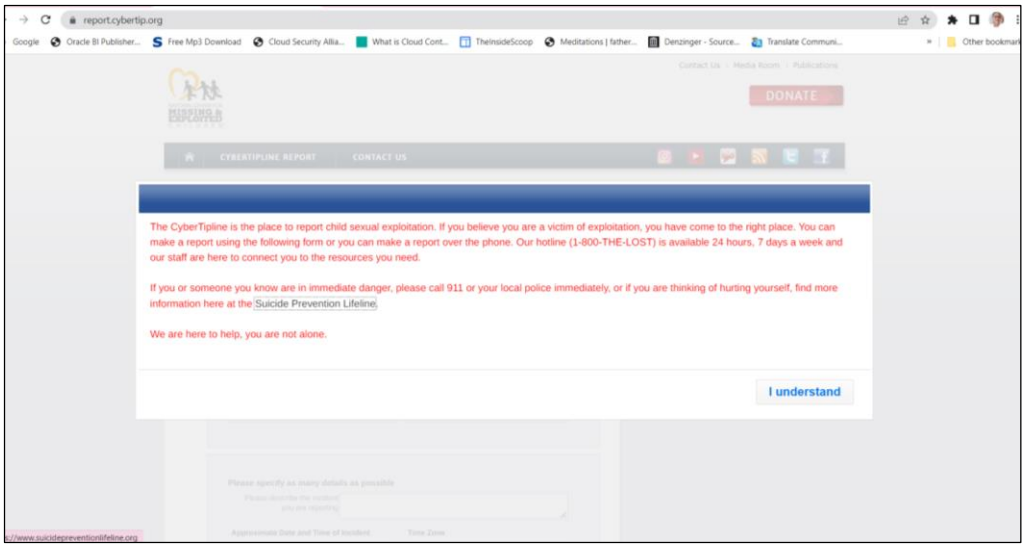


Figure 2.15: CyberTipline - On Clicking Report here

Source: Crimes Involving Children - USA Government

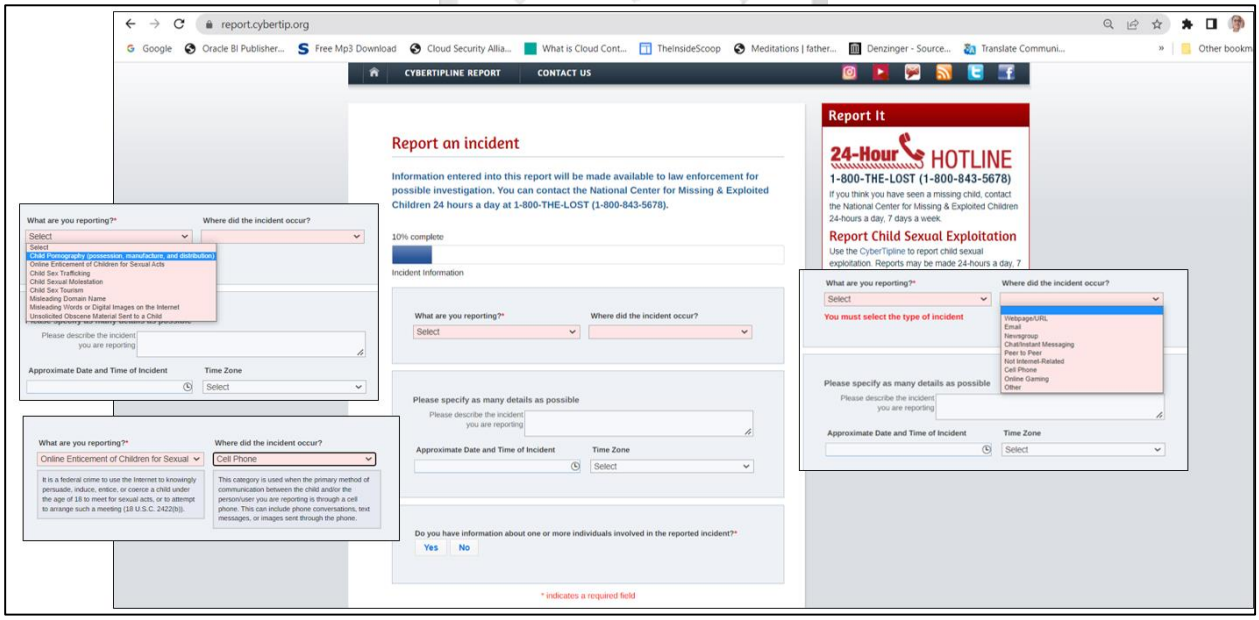


Figure 2.16: CyberTipline - Some Fields When Reporting and Incident

Source: Crimes Involving Children - USA Government

2.8 International Databases for Reporting Child Online Exploitation

2.8.1 National Centre for Missing and Exploited Children (NCMEC)

The National Centre for Missing and Exploited Children (NCMEC) is a private, non-profit organization established in 1984 by the United States Congress. It serves as an information clearing house and national resource centre on issues related to victims, missing and exploited children and operates a national toll-free hotline (National Centre for Missing and Exploited Children, 2020). It serves not only the United States population, but liaises with cyber intelligence departments in other regions, sharing any information related to activity in their countries identified on their system.

The CyberTipline, a national mechanism to report instances of Child Sexual Exploitation for the public and electronic service providers is also operated by NCMEC. Statistics from 2019 show that the CyberTipline received 16.9 million reports on various form of Child Sexual Abuse including "sextortion" (National Centre for Missing and Exploited Children, 2020).

2.8.2 Interpol's ICSE

The International Child Sexual Exploitation (ICSE) image and video database is an intelligence and investigative tool, which allows specialized investigators to share data on cases of child sexual abuse (INTERPOL, 2021).

Video and image comparison software are used to identify victims, abusers, and places. Duplication of effort is avoided as the database can alert the investigators on whether a series of images has been investigated elsewhere, or whether similar features have been found in previously reviewed content.

In May 2019, Kenya became the first African country to connect to INTERPOL's International Child Sexual Exploitation (ICSE) database.

2.9 Summary of the Literature Review

There is a substantial amount of legislation on the issues of Child Online abuse that is in effect. Kenya also has ratified some international instruments to aid in the protection of children online. The Child Help Line (116) managed by the National Council for Children Services (NCCS) deals with all forms of child exploitation. People can call to report any incidences and statistics are maintained on the Children Protection Information Management System (CPIMS).

There are also several government institutions dealing with issues of child protection in Kenya. Different child protection issues are dealt with like neglect/ abandonment, child trafficking, abduction and kidnapping, child labour, emotional abuse, female genital mutilation, physical abuse, sexual abuse (defilement, sexual assault, and indecent acts), forced marriage, child stealing etc. Online abuse has only become a cause for attention recently, causing the law enforcement to pay it attention. The child helpline has been in existence longest and many people use it for reporting child abuse by calling. Information on child abuse is collected though the child help line and maintained on the Children Protection Information Management System (CPIMS). On the statistics available so far, there is almost no information regarding online child abuse. This is an area that requires more attention and thus having information on the same would help in investigation, public awareness of the issues facing children online and in being a crowd sourcing platform for reporting and sharing information and transmitting evidence of crimes witnessed to law enforcement.

From the review of the practise in other countries, a dedicated online platform for reporting online abuse is required. This platform will be of great help to the law enforcement agencies in receiving tips and information that can help in their investigation activities. This platform would also offer members of the public, including children, a channel on which to report at their convenience. Furthermore, it would enhance citizens' awareness of online child abuse and their role in preventing and addressing it. Some of the features on the reviewed systems will be adopted for the system being developed.

Until now, reporting of child abuse offenses (both online and offline) has been mainly done on the helpline. The KE-CIRT was recently (during this research) updated to include a section where child online abuse can be reported. A platform solely dedicated to child online abuse would be

most appropriate as among other things, it would resolve the issues below that the online child reporting section on the KE-CIRT does not address:

a. Providing a section to upload any digital evidence, image, video, or link for any issue being reported.
b. Location picker option which will be a tip to the law enforcement on the location where the report is being filed from.
c. Reports on the types of online offenses against children and statistics on their frequency of occurrence. This will be a good informational resource for the public.

The issues mentioned above will be addressed by the system being developed.

CHAPTER 3: METHODOLOGY

3.1 Introduction

This chapter discusses the approaches taken in performing the research to address the research objectives outlined in chapter one. A defined set of methods and procedures were applied to identify, select and analyse data related to the topic in question. The software development methodology used is described together with the rationale behind its choice.

3.2 Research Approach for Objective 1 and 2

Research objective one sought to review the current online child abuse handling process in Kenya, analyse and understand its weaknesses. This was done in chapter two by conducting a review of literature on the current measures in place to regulate online activities, conduct and content in the country. These measures include policies, statutes and even the establishment of government institutions dealing with child protection and children's rights. A systematic review of the major legal instruments in place together with the current methods of reporting abuse cases was done. Government institutions dealing with children's rights were identified and their roles studied. These reviews were done through reading, analysing, evaluating the relevancy of the findings to the current question and synthesizing the findings as documented in the literature review chapter.

Research objective two sought to review the online child abuse handling process in use in other countries. Similarly, this was done in chapter two by conducting a systematic review of literature on the current measures in place to prevent and handle online child abuse in other countries. Reading and analysis of global and cross border instruments in place was done, with special emphasis on the regional instruments that have been ratified by Kenya. Further, the features and content of online crime reporting platforms in use by other countries were examined for benchmarking. A synthesis of the findings is documented in the literature review chapter.

3.3 Research Approach for Objective 3

Research objectives three was addressed by designing, developing and testing a system for reporting online child abuse and maintaining a record of past cases reported.

To design and develop the system, Agile Software Development Methodology was used. It is a customer-centric, iterative, and incremental methodology, whose goal is to deliver tangible software results often and efficiently (Lynn, 2021).

Agile Software Development Methodology consists of the following 5 basic processes as shown in Figure 3.1.

1. Planning
2. Requirements Gathering
3. Design
4. Development
5. Testing

The system is developed in small iterations per functionality until all the functionalities are achieved. See Figure 3.1.

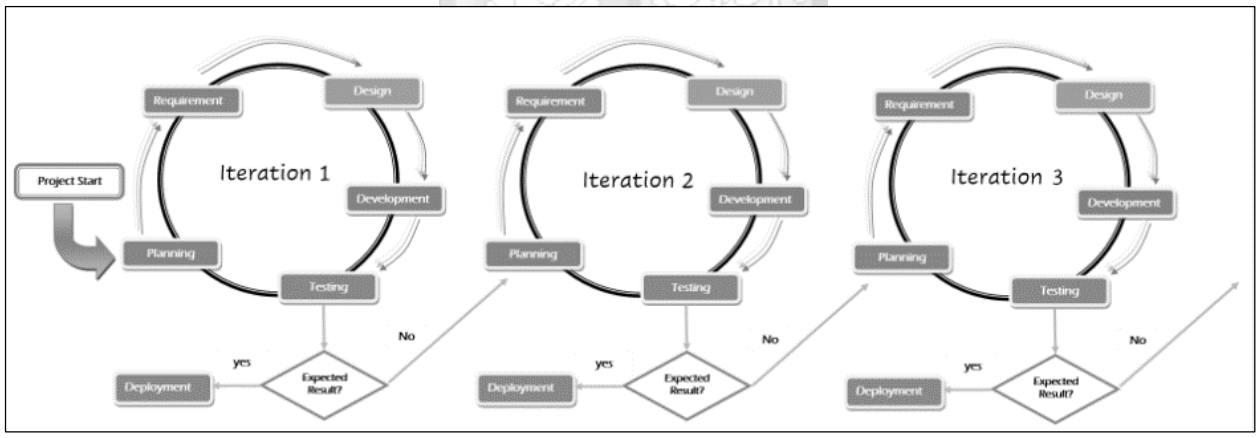


Figure 3.1: Agile Software Development Methodology

Source: A Practical Guide to Feature-Driven Development (Coad Series), Palmer & Felsing, 2002

3.3.1 Planning

Planning of the project was done throughout the project proposal development and review stage. This entails review meetings to discuss with the supervisor, colleagues and other stakeholders about the problem being addressed and how to approach it. The problem was defined accurately here and the objectives to be addressed in resolving the problem. The possible features of the system to be developed were outlined and discussed. An assessment of their complexity and dependencies was done to plan for the tasks involved and decide on the order of their

implementation. Features were grouped or broken down further depending on their complexity. Unified Modelling Language (UML) was used for the detailed modelling of system features before building each one of them. Interaction Diagrams were used to show how objects collaborate in the system. The data collection approvals were identified and duly sought. The cost implications and development environments to be used were also identified.

3.3.2 Requirements Gathering

In this phase the information necessary to design and develop the system was gathered. It entailed finding out if there was need for and if users were ready for an online system to report Online Child Offences and what capabilities (functional and non-functional requirements) they desired.

3.3.2.1 Research Design

Primary quantitative approach was adopted during data gathering. Data was collected directly from the respondents for purposes of this system development.

According to Creswell and Creswell (2018), "quantitative approach seeks to explore and understand the meaning individuals or groups ascribe to a social or human problem. The process of research involves emerging questions and procedures, data typically collected in the participant's setting, data analysis inductively building from particulars to general themes, and the researcher making interpretations of the meaning of the data. The final written report has a flexible structure. Those who engage in this form of inquiry support a way of looking at research that honours an inductive style, a focus on individual meaning, and the importance of reporting the complexity of a situation".

It is a systematic investigation of phenomena by gathering quantifiable data and performing statistical, mathematical, or computational techniques. As quantitative approach is data oriented, data collected using this method is objective, elaborate, and many times, even investigational. The results achieved from this research method are logical, statistical, and unbiased.

The three methods listed below were used for gathering the system requirements:

1. Literature review and bench marking with existing systems in other countries
2. Interviews with key stakeholders
3. Questionnaires with intended users

Literature review and bench marking with existing systems in other countries

Based on the review of literature and systems in use by other countries, key system features were identified. This was done in the literature review conducted in chapter 2.

Interviews with key stakeholders

Key institutions dealing with children's rights were identified in the literature review. Interviews were conducted with staff in these institutions as part of requirements gathering. Collected responses were recorded in MS Word and the results are discussed in chapter 4. The interview guide used is attached in Appendix I.

Interviews: Target Population

The interviews targeted members of staff working in institutions dealing with children's rights. The main aim of the interviews was to find out what types of online abuse have been encountered, how online child abuse issues are reported and handled in these institutions, establishing gaps and possible ways to bridge the gaps identified. The interview guide is attached in Appendix I.

Interviews: Sampling Method

Convenience sampling was used for the interviews. In the selection of the actual institutions to interview members of staff from, those that highly collaborate with other institutions in their role were selected to ensure the data gathered is representative of more people. Similarly, convenience sampling was used to identify who among the members of staff would be interviewed. Staff member who were available and willing to participate in the study were interviewed.

Interviews: Sample Size

Four or five participants from each of the participating institutions dealing with children were interviewed. Information gathered from the interview respondents would offer a big picture response, owing to their collaboration with many institutions.

Table 3-1 lists the main institutions that work with the government in dealing with children's rights and specifically on child exploitation.

Table 3-1: Government and Private Institutions Dealing with Children in Kenya

	Institutions Name
1.	Child welfare Society of Kenya (CWSK)
2.	National Council for Children Services (NCCS)
3.	Ministry of Labor and Social Protection - Department of Children Services
4.	DCI Anti– Human Trafficking & Child Protection Unit
5.	Communications Authority of Kenya and the KE-CIRT
6.	Kenya Film Classification Board (KFCB)
7.	UNICEF
8.	Watoto Watch
9.	Terre des homes

A sample of these institutions as shown in Table 3-2 were selected. An institutions degree of collaboration with other institutions was a major criterion for selection. 4-5 interviewees from each of the institutions were selected using convenience sampling method.

Table 3-2: The Institutions Sampled for the Interviews

	Institutions Name
1.	Child welfare Society of Kenya (CWSK)
2.	National Council for Children Services (NCCS)
3.	DCI Anti– Human Trafficking & Child Protection Unit
4.	Communications Authority of Kenya and the KE-CIRT
5.	Watoto Watch

Questionnaires with intended users

These were administered to a section of the intended users of the system to check their readiness for the system being developed and obtain their views on desirable features that the system being developed should have. The features mentioned would in turn be incorporated into the system during development.

The respondents were from Strathmore University (Students, Staff and Parents).

Participation in the survey was on a voluntary basis. Personal Identifiable Information (PII) of the respondents was not collected and the fact that the information collected was for purposes of the study and system development was made explicit to the respondents on the questionnaire.

The questionnaire was developed using google forms and disseminated via online channels like social media platforms and email. Analysis was done using charts and graphs. This questionnaire is attached in Appendix II and the results are discussed in chapter 4.

Questionnaires: Target Population

Questionnaires were administered to students and parents of Strathmore University. The aim was to find out if respondents had encountered any kind of online child abuse, which one(s), how they had dealt with it and if an online reporting platform would enhance reporting and handling of online child abuse. It also sought to know what features the respondents would want on such a system.

Questionnaires: Sampling Method

Simple random sampling was used owing to the homogenous and large population size among the students and staff in the university. Some students helped to reach out to their parents. Simple random sampling is a probabilistic sampling method where participants of a sample are chosen through a random selection process. Each member has an equal opportunity to be selected (Hamed Taherdoost, 2016).

Questionnaires: Sample Size

At least twenty-five staff, students and parents were each approached to respond to the questionnaire. This numbers were indicative to ensure that we get a representation from the different stakeholders in the university. The choice of Strathmore was done based on convenience. This brought the total respondents to about one hundred which is considered adequate for this study.

3.3.3 Design

Based on the requirements gathered, high level Conceptual Models of the system were defined, describing actors, attributes, relationships, and mappings. They were then combined to form the overall system model (See Figure 4.13). Use Case Diagrams were used to demonstrate users' interaction with the system (See Figure 4.14) while the database structure was represented using

JSON trees for the NoSQL firebase database used. See Figure 4.20, Figure 4.21 and Figure 4.22 for the database representations.

3.3.4 Development

Agile Software Development methodology entails iterative processes that are repeated until all the desired features are fully developed. In general, the following tools were used to build the features:

Web application

Dart programming language on flutter framework and Figma for the User Interface were used for the Web Application. Dart is a client-optimized language for developing fast apps on any platform. It allows for development on multiple platforms in addition to working with a flexible execution runtime platform for app frameworks (Dart Development Community, 2022). Flutter is an open source framework by Google for building beautiful, natively compiled, multi-platform applications from a single codebase (Flutter Developers Community, 2022).

Figma is a web-based design tool for the User Interface design of anything e.g. websites, applications, logos etc. It also has additional offline features enabled by desktop applications for macOS and Windows. The Figma mobile app for Android and iOS allow viewing and interacting with Figma prototypes in real-time mobile devices (Figma Development Community, 2022).

Mobile application

For the mobile application, JavaScript was used on Flutter framework and Figma for the User Interface.

Backend

Dart programming language was used on flutter framework for the backend.

Database development

The Firebase Real-time Database was used for the database design and development. Firebase Real-time Database is a cloud-hosted NoSQL database that supports real time storage and syncing of data between users (Google Developers, 2022).

3.3.5 System Testing

As part of the Build by Feature process, **feature testing** was carried out to ensure that each feature works as intended and designed. The following tests were carried out during feature testing.

i. Functionality tests: These were carried out through a re-performance of each of the systems features e.g. reporting an abuse case, recording and storing of the reported case on the backend, login and manipulation of cases by an admin, reviewing and ability to change the reported case's status etc. This was done to check if the features met the functional requirements outlined effectively. See discussion on functional testing in chapter 4.

ii. Usability tests: These were done by reviewing the adaptability of the user interface on web, mobile and different browsers, the simplicity/ ease of system navigation and use, and system response speed during abuse reporting. See discussion on usability testing in chapter 4.

iii. Security tests: These were done by ensuring data validation was right when reporting a case, reviewing user roles (for the admin users) to ensure that users access only the information within their mandates and only perform their roles.

3.4 Research Approach for Objective 4

Research objective 4 was validating the adequacy of the developed system in addressing the problem of reporting and maintaining a record of online child abuse. This was done by selecting a subset of intended systems users to evaluate how the system worked. The intended system users included the general public (who would report crimes) and law enforcement personnel (who would receive, review and act on the reported crimes). The aim was to confirm that the systems purpose of having cases of online child abuse anonymously reported on an online platform, received by Law enforcement officers, reviewed and used for investigations was achieved. 5 reporters made reports of crime and 5 law enforcement personnel were granted system access to review the reports made and update their status accordingly. A questionnaire was administered to them to evaluate the systems adequacy.

3.5 Ethical Considerations

Ethical review and approval was required for the research. The same was obtained from Strathmore university – Institutional Ethics Review Committee (SU-IERC) as data gathering would be carried out among respondents from within and outside the university. Letter of approval is attached in Appendix IV. Considering the sensitivity of the topic on child abuse, the ethical review sought to ensure that the key ethical considerations of data confidentiality and privacy, voluntary participation and informed consent from any respondents, and the appropriate research methods were employed. As a result, the interview guides and questionnaires required the respondents to give informed and free consent, gathered no personal information to ensure respondents remained anonymous. Any personal obtained was kept private and used only for purposes of the study. Dummy photos and videos were used for system testing.

CHAPTER 4: SYSTEM ANALYSIS, DESIGN AND ARCHITECTURE

4.1 Introduction

This chapter discusses process followed in establishing the need for an online system to report online child abuse. Information obtained from the survey respondents is consolidated to draw out useful feedback on the need for the system, system requirements, system design for both the front and backend done for the application development and implementation. It includes sections on requirements gathering and data analysis, functional and non-functional analysis, conceptual modelling where the different actors, attributes and relationships are defined, use case diagrams, database JSON tree and the wireframe design showing how the system will look like.

4.2 Requirements Gathering

This phase of the system development methodology was employed to gather the system requirements. Data collection was done using interviews and questionnaires. A questionnaire (Appendix II) and an interview guide (Appendix I) were used with the main aims being to ascertain:

1. Whether there is need for the system
2. The features that the users desire to have on the system

4.2.1 Data Analysis: Interview Findings

Interviews were conducted with staff working in institutions dealing with children rights as part of requirements gathering. Five institutions were selected based on their level of interaction with other institutions. From each institution, four to five people were interviewed using convenience sampling. A total of twenty-three people were interviewed.

87% of those interviewed affirmed having encountered online abuse of children as seen in Figure 4.1. The types of abuse encountered ranged from cyber bullying, grooming to sharing sexual content of children. See Figure 4.2.

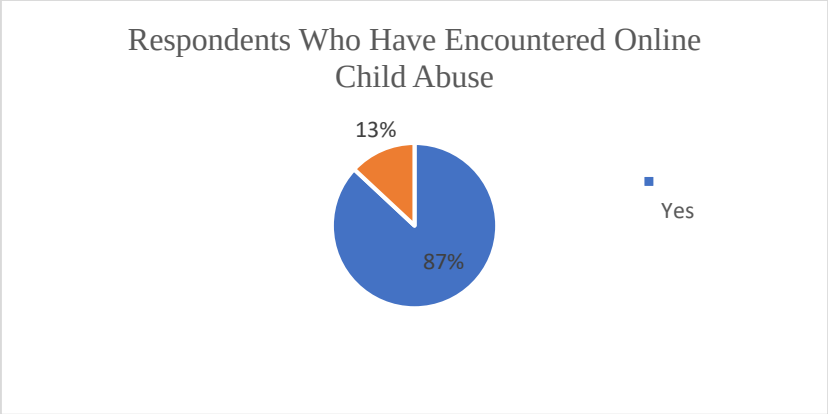


Figure 4.1: Respondents Who Have Encountered Online Child Abuse

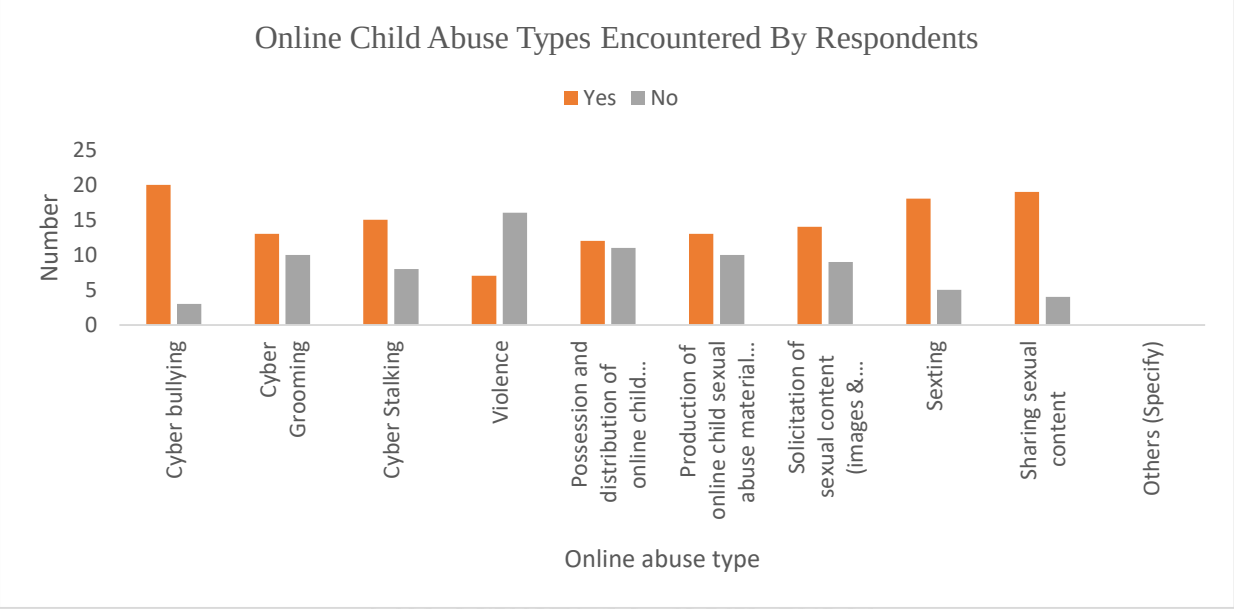


Figure 4.2: Online Abuse Types Encountered By The Respondents

The percentages of online child abuse cases encountered in a month were more than 22% as seen in Figure 4.3. Reporting of these abuse cases was done verbally or using phone calls. Some of the institutions had official phone calls they used to make or receive these reports. It was also noted that none of the institutions had an online platform where the reporting could be done.

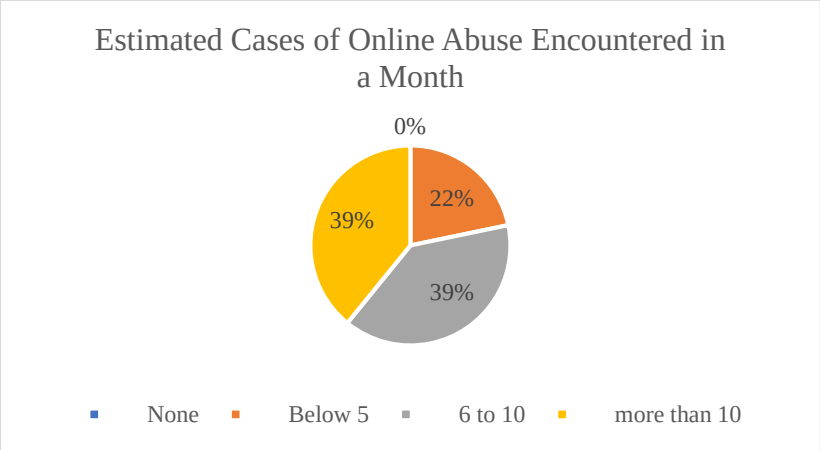


Figure 4.3: Estimated Cases of Online Child Abuse encountered in a Month

Majority of the institutions dealt with online child abuse cases either by reported to the child help line or to the nearest police station. Most of them combined this with reporting to their management and offering guidance and counselling to the victims who they could. See Figure 4.4.

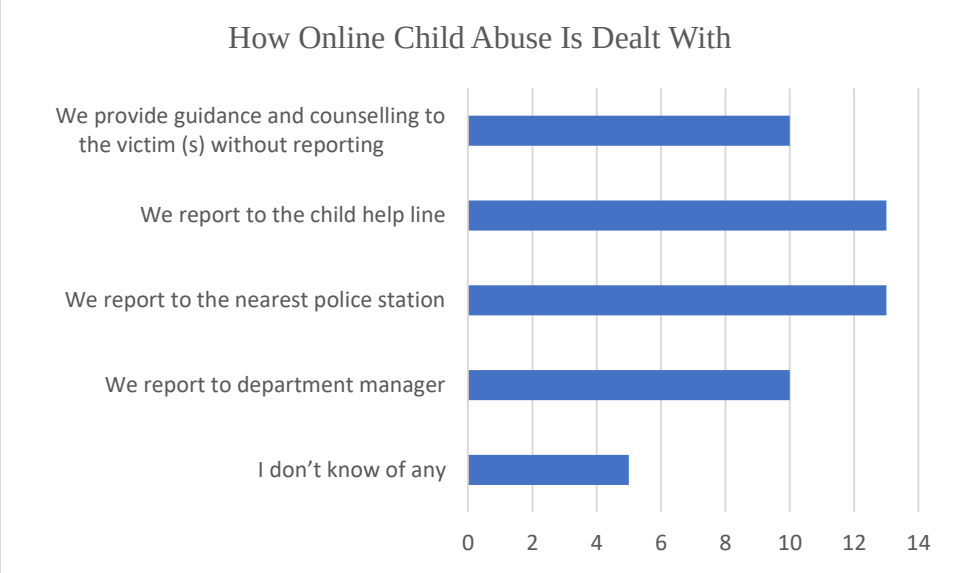


Figure 4.4: How Online Child Abuse is Dealt with

The suggestion given on what the respondents would change to make the measures taken by their institutions more effective included making the reporting process more convenient (50%), minimising the contact with the victim e.g. by not having to go to the police station (30%) and also reporting to people who understood online abuse (27%). All the respondents agreed that an online reporting platform would aid in simplifying the reporting process and even in investigations (See Figure 4.5) and gave the desirable system features as seen in Figure 4.6.

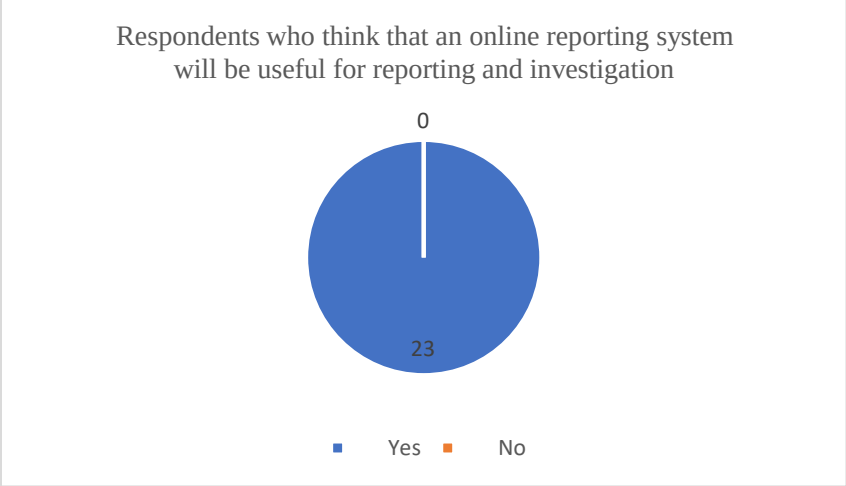


Figure 4.5: An Online Platform Would Aid Reporting and Investigation

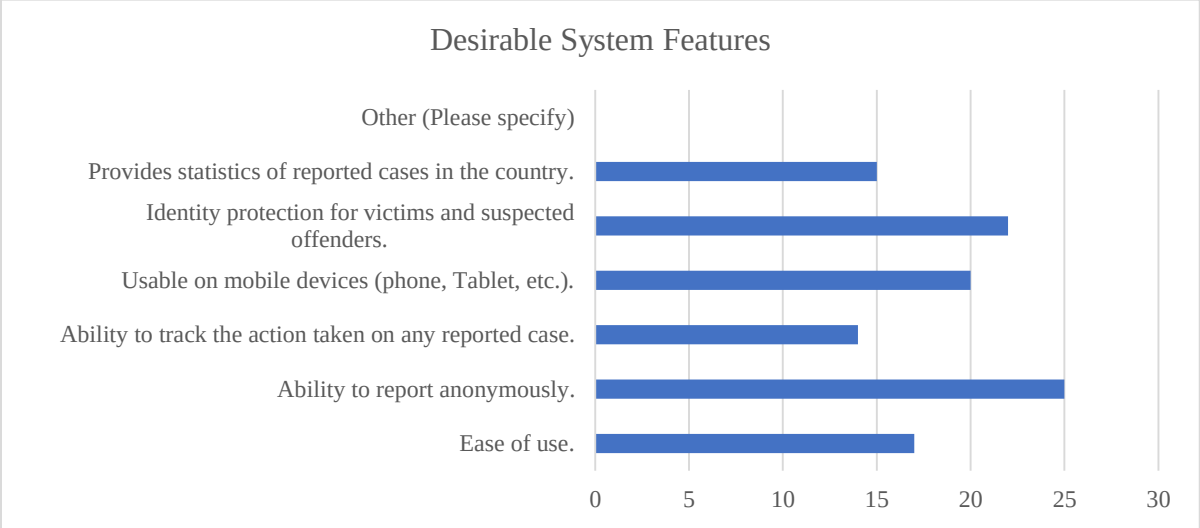


Figure 4.6: Desirable System Features

4.2.2 Data analysis: Questionnaire Findings

Questionnaire respondents were sought among the student, staff and parents in Strathmore university. Approximately 80 responses were obtained. 70 % of the respondents affirmed that they have encountered online child abuse. See Figure 4.7

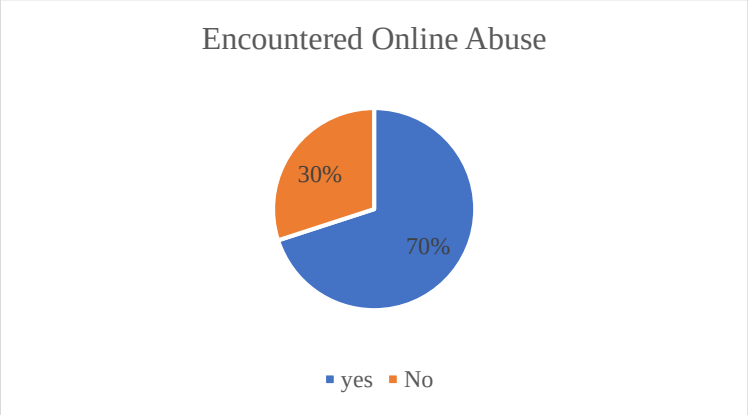


Figure 4.7: Questionnaire Respondents Who Have Encountered Online Child Abuse

The content encountered included the following abuses: Bullying, Grooming, Stalking, Violence, Possession, and distribution of Child Sexual Abuse Material (CSAM), Solicitation of sexual content (images & conversation) from children, Sexting, Sharing sexual content. See Figure 4.8

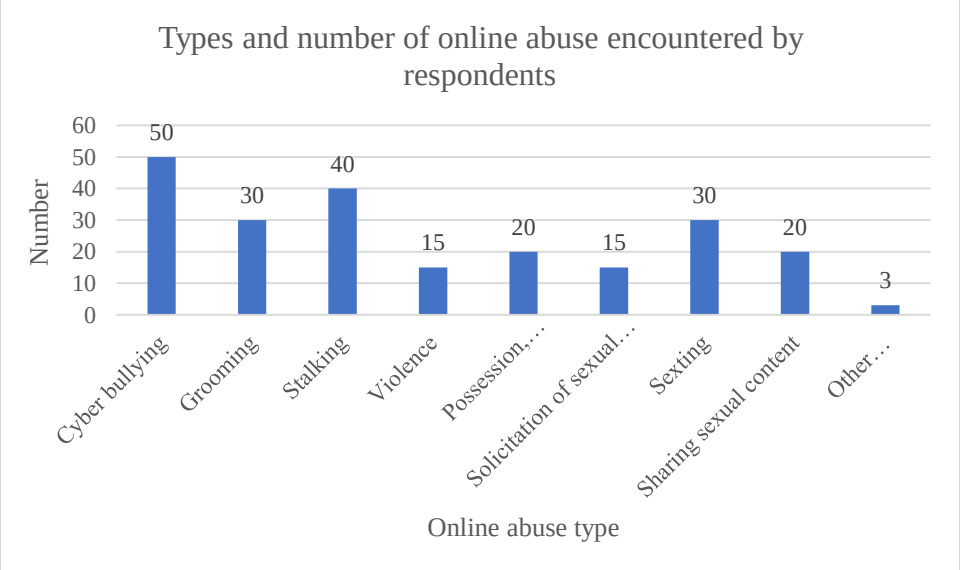


Figure 4.8: Types of Online child Abuse encountered by Questionnaire Respondents

As shown in Figure 4.9, 20 % of those who have encountered online child abuse content took the step to report.

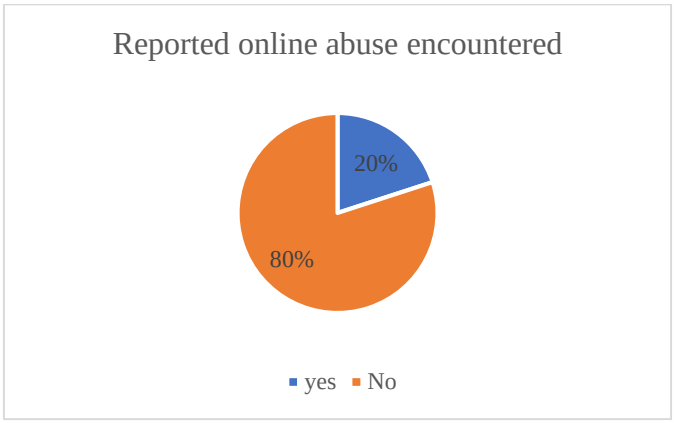


Figure 4.9: Respondents Who Reported Online Abuse Encountered

Out of all the interviewed respondents, 53 % were unaware of the existence of the child help line, where they could call to report online abuse incidences (See Figure 4.10).

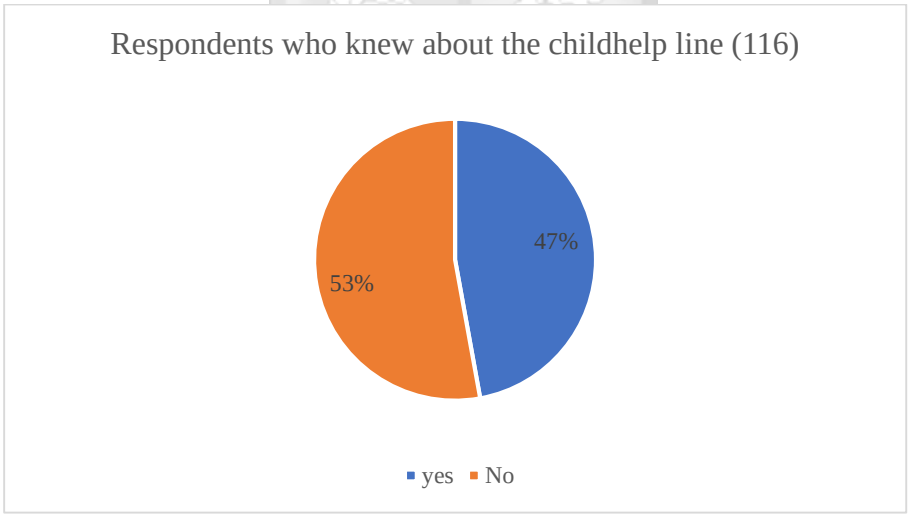


Figure 4.10: Questionnaire Respondents Who Knew About The Child Help Line

Out of the respondents who know about the child help line and have called to report an online abuse, 61% got assistance (See Figure 4.11). This leaves about 39% of the cases of online child abuse unreported.

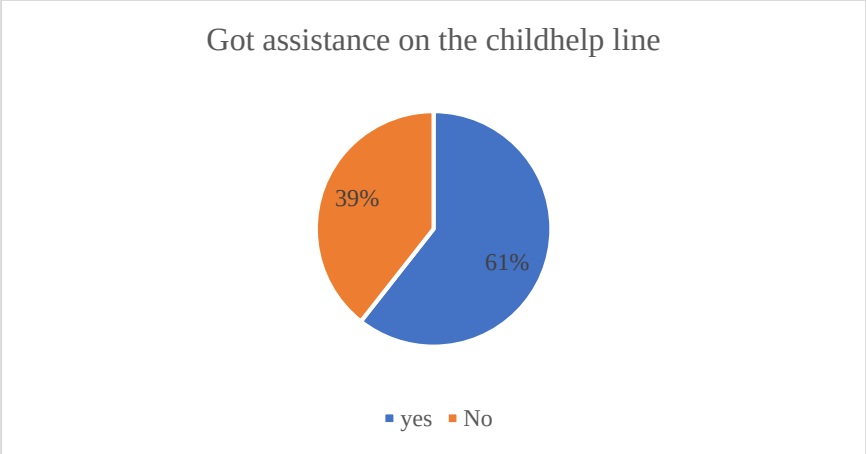


Figure 4.11: Respondents Who Were Assisted on The Child Helpline

An online reporting system is likely to cater for most of these unreported cases since:

1. It does not require an immediate response.
2. It allows for a reporter to do so at their convenience.

58% of the respondents as seen on Figure 4.12 were ready to report on an online system due to its convenience. The remaining 42% were not ready to report online child abuses on an online system. They gave the following reasons for not being ready to report on an online system:

1. Doubts about whether they could report anonymously.
2. Doubts about how identity protection for the victims and offenders would be ensured.

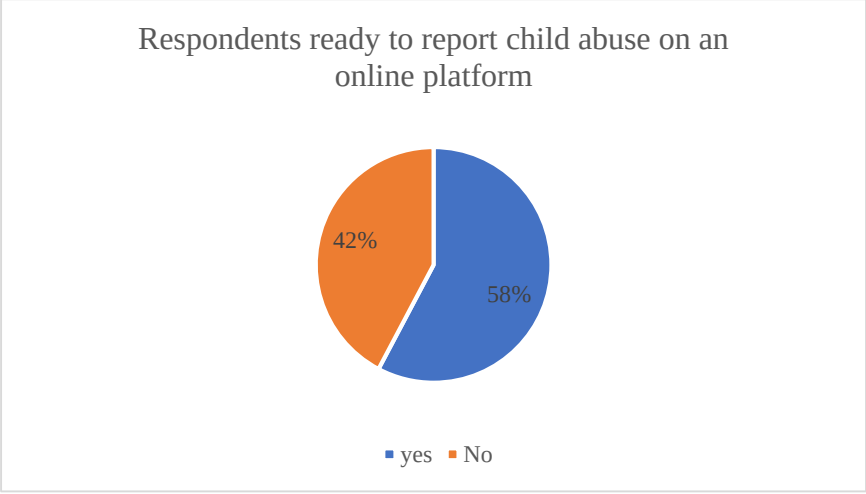


Figure 4.12: Respondents Ready to Report on an Online platform

These two issues (anonymous reporting and identity protection for the victims and offenders) have been addressed. The developed system allows for anonymous reporting of online abuse cases. Through appropriate segregation of rights, it also ensures that only the necessary parties have access to the details of the reported cases which may include identity revealing details (images, videos etc.) of the victims and offenders on reported cases.

The survey respondents ranked some system features based on priority. Table 4-1 shows the priority ranking of the system features given by the respondents.

Table 4-1: Key System Features in Order of Priority for System Users.

Feature	**Priority**
Ease of use	1
Ability to report anonymously	2
Identity protection for victims and suspected offenders	3
Usable on mobile devices (phone, tablet, etc.)	4
Ability to track the action taken on any reported case	5
Provides statistics of reported cases in the country	6

From the children rights centred organizations, 70% of the respondents acknowledged that an online reporting system would help in the reporting and investigation of crimes. Further, they confirmed that it directly improves the collection of intelligence and statistics.

Survey respondents from these organisations ranked the following system features in order of priority as shown on Table 4-2.

Table 4-2: Key System Features in Order of Priority for Practitioners Dealing with Children.

Feature	**Priority**
Ability to report anonymously	1
Identity protection for victims and suspected offenders	2
Usable on mobile devices (phone, tablet, etc.)	3
Ease of use	4
Provides statistics of reported cases in the country	5
Ability to track the action taken on any reported case	6

4.3 Design

The overall system design was done using the overall model, sequence diagrams, use case diagrams and the database structure. Use case diagrams were used to describe the interactions of the system users with the system.

The overall model of the system is depicted on Figure 4.13.

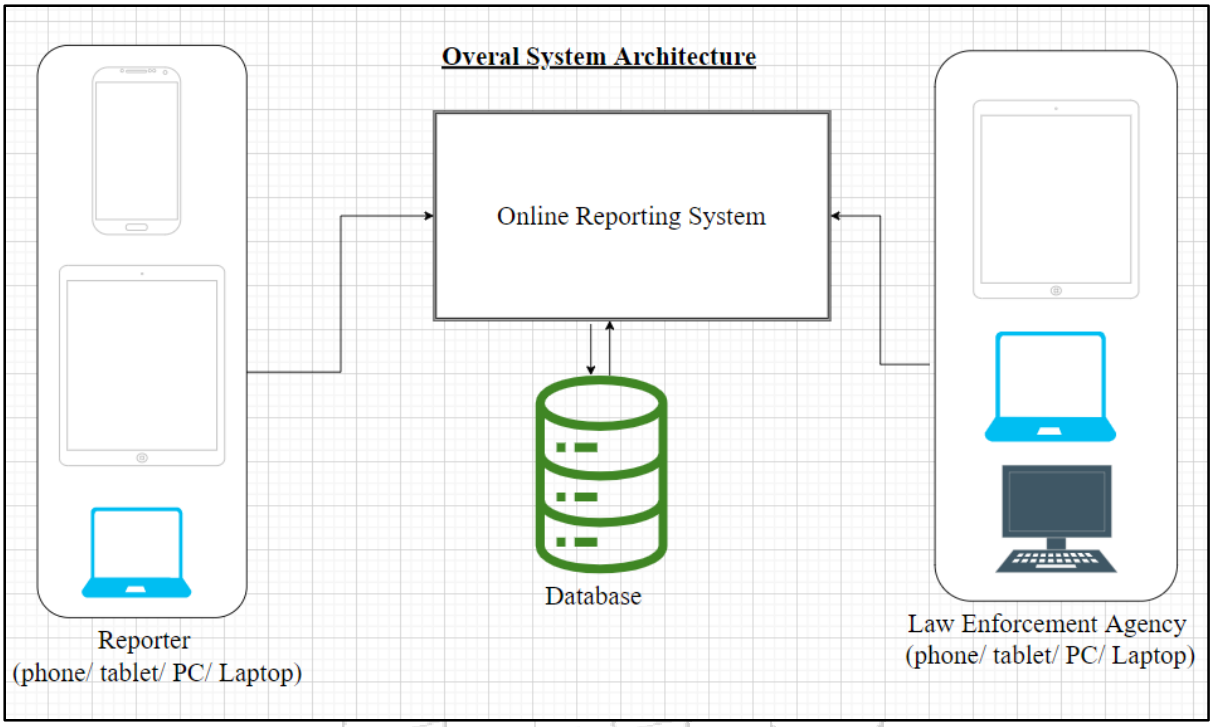


Figure 4.13: Overall System Architecture

The information obtained during data gathering was used to come up with both the functional and non-functional system features. These features show how the designed system will operate and what it will do to accomplish its role.

4.3.1 Functional Analysis/ Requirements

These are the required system features. They directly point to its essential operations, that is, what the system should do. The following were the identified functional requirements:

1. **Report a case**: The system should allow anyone to report a case. The reporter of any case will do so without need for authentication. Reporters will have the option to do so anonymously since on the form availed, personal user details are optional during reporting.
2. **Authentication**: Law enforcement users on the system will be required to use their credentials to login. The role assigned to each user will determine the level of detail one can view regarding any reported case. User roles will be of either, 'SuperAdmin', Admin and Officer. 'SuperAdmin' has rights to manage all system users and roles by creating new users and suspend existing ones. 'Admin' role will view all the reported cases and assign them to specific users to handle them. 'Officer' role will view cases assigned to them for investigation. This role can manipulate the status of a reported case as investigations proceed.
3. **Data management**: On the backend, users with 'Admin' and 'officer' roles will perform data management procedures like changing the status of a reported case to either 'Received', 'Investigation ongoing' or 'Closed'.
4. **Data accuracy**: The data collected and stored should remain accurate to facilitate investigations, prosecution, and true reporting.

4.3.2 Non-functional Analysis/ Requirements

Non-functional requirements refer to system features that aid in the achievement of the systems operations with ease, efficiency, and safety. Also known as system qualities, they include attributes such as security, reliability, performance, maintainability, scalability, and usability (Scaled Agile inc., 2021).

The following are the identified non-functional requirements:

1. **Usability**: The system should be user friendly and simple to navigate.
2. **Security**: This entails:
    a. Ensuring that access to specific modules is restricted based on roles.

b. Ensuring that users who choose to remain anonymous remain so.

c. Protecting the identity of victims and offenders on the system. This will be achieved by:

   i. Ensuring statistics published to the public are anonymised

   ii. Enforcing information access on a need to know basis through user roles.

3. **Browser independence**: The system should function well across multiple browsers.

4. **Device compatibility**: The system should be customised for both Web and mobile device interfaces.

4.3.3 Use Case Modelling

Use cases define how different actors (users) interact with a system to achieve specific goals. The key elements in use cases are the actors and the use cases. The actors on this system are reporter, Super admin, Admins (Crime monitor) and visitor.

4.3.3.1 Use Case Descriptions

The Use Cases for the reporter are:

1. Report a case

Use case	**Report a case**
Actor	Reporter
Purpose	To report a case
Overview	Any civilian can access the system and report a case of online child abuse that comes to their attention.
Cross reference	N/A
Pre-conditions	Open the reporting page.
Post conditions	A case is successfully reported.

The Use Cases for the Super Admin are:

1. Create users on the system

Use case	**Create admin user on the system**
Actor	Super Admin.
Purpose	To create new users on the system. Created users can either be Admin or Officer.
Overview	The system will have 2 types of users; Admin and Officers. Admin users are the ones who receive reported cases on the system and assign them to officers.
Cross reference	None.
Pre-conditions	The Super Admin should be logged into the system.
Post conditions	A new user is created.

2. Manage users on the system

Use case	**Manage users on the system**
Actor	Super Admin
Purpose	To update, activate or deactivate users on the system.
Overview	Users need to be created on the system and assigned a role (Admin or Officer).
Cross reference	Add user on the system.
Pre-conditions	User exists on the system.
Post conditions	User status is updated to either active or inactive on the system.

The Admin Use Cases are:

1. Login to the system and Assign reported cases

Use case	**Login to the system, Assign reported cases**
Actor	Admin
Purpose	To gain access into the system, view and assign reported cases to officers.
Overview	Admin has access to the reported cases and assigns them to officers.
Cross reference	Add Admin user on the system.
Pre-conditions	Admin exists on the system and is active.
Post conditions	Admin can see and manage reported cases or assign them to Officers.

Officer Use Cases are:

1. Login to the system and View assigned cases

Use case	**Login to system and View assigned cases**
Actor	Officer
Purpose	Officer accesses the system to view reported cases assigned to him.
Overview	Reported cases are visible by the Officer on login into the system.
Cross reference	Login to the system.
Pre-conditions	Officer exists on the system, is active and logged in.
Post conditions	Reported cases assigned to Officer are seen and can now be actioned.

2. Manage reported case (change status, close, etc.)

Use case	**Manage reported cases**
Actor	Officer
Purpose	To allow Officers update the status of cases as they are progressively being dealt with.
Overview	Reported cases can change status from reported to received, escalated, investigation ongoing and closed.
Cross reference	Report a case and case assigned to Officer
Pre-conditions	Login to the system and report a case.
Post conditions	The status of a case is updated.

3. Manage reports

Use case	**Manage reports**
Actor	Admin and Officer
Purpose	To allow for the generation of reports on reported cases.
Overview	This are reports about the cases reported on the system.
Cross reference	None.
Pre-conditions	Login to the system.
Post conditions	Visitor can view some details from the reports on the reported cases

The Use Cases for the visitor (public) are:

4. View statistics on reported cases

Use case	**View statistics on reported cases.**
Actor	Visitor.
Purpose	To view the general information (not personal and confidential information) about cases of online child abuse reported using this system.
Overview	The public will be able to see general information about cases reported here.
Cross reference	Manage reports.
Pre-conditions	Access the reporting site, Manage reports.
Post conditions	Visitor can view reports.

4.3.4 Use Case Diagram

The use case diagram shows the actors on the system and how they interact with the system. This reporting system has 5 actors: super-admin, admin, officer, reporter, and visitor. Figure 4.14 shows what they can do on the system.

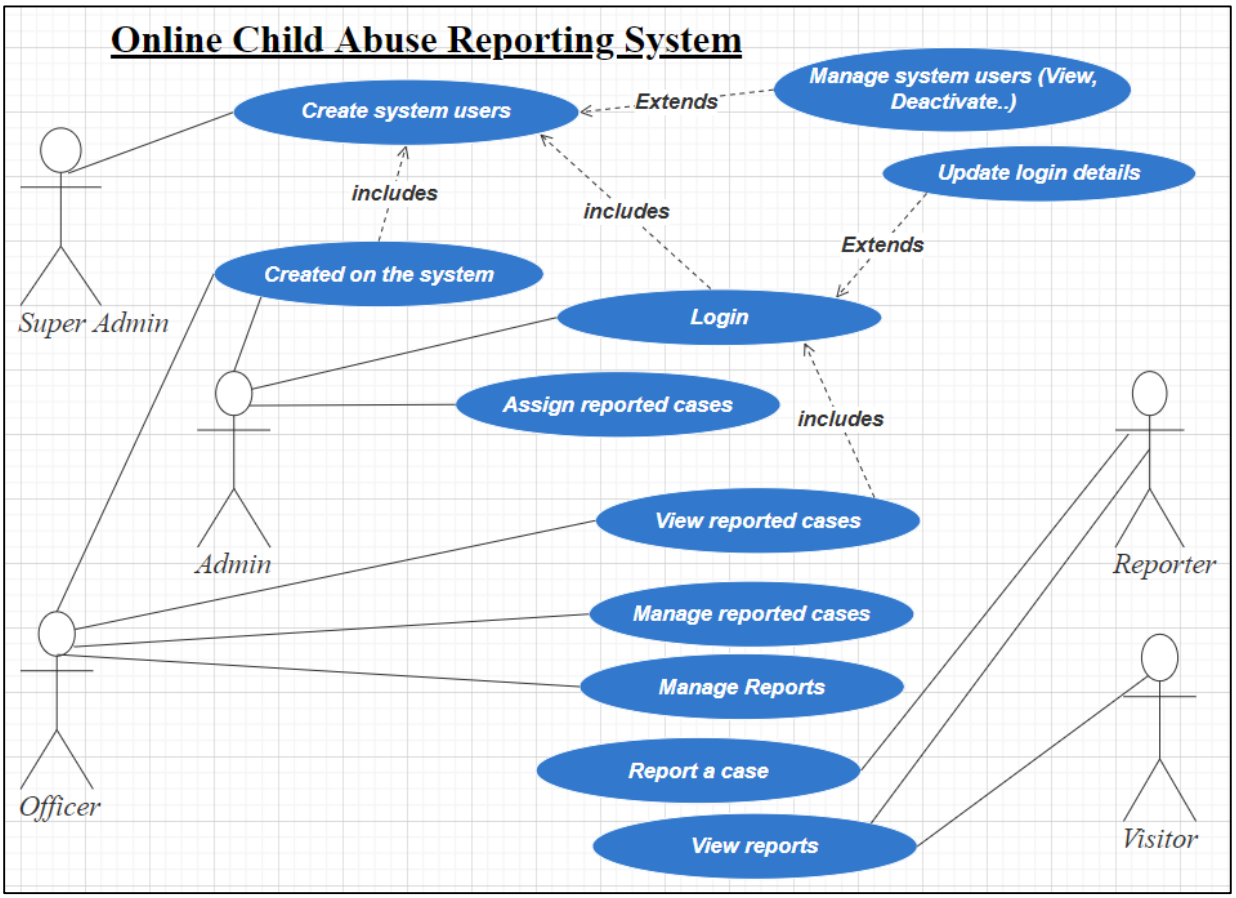


Figure 4.14: Use Case Diagram for the Reporting System

4.3.5 Sequence Diagrams

The sequence diagrams show the flow of each users' interaction with the system. Figure 4.15 shows the Super-admin's flow of actions on the system and responses.

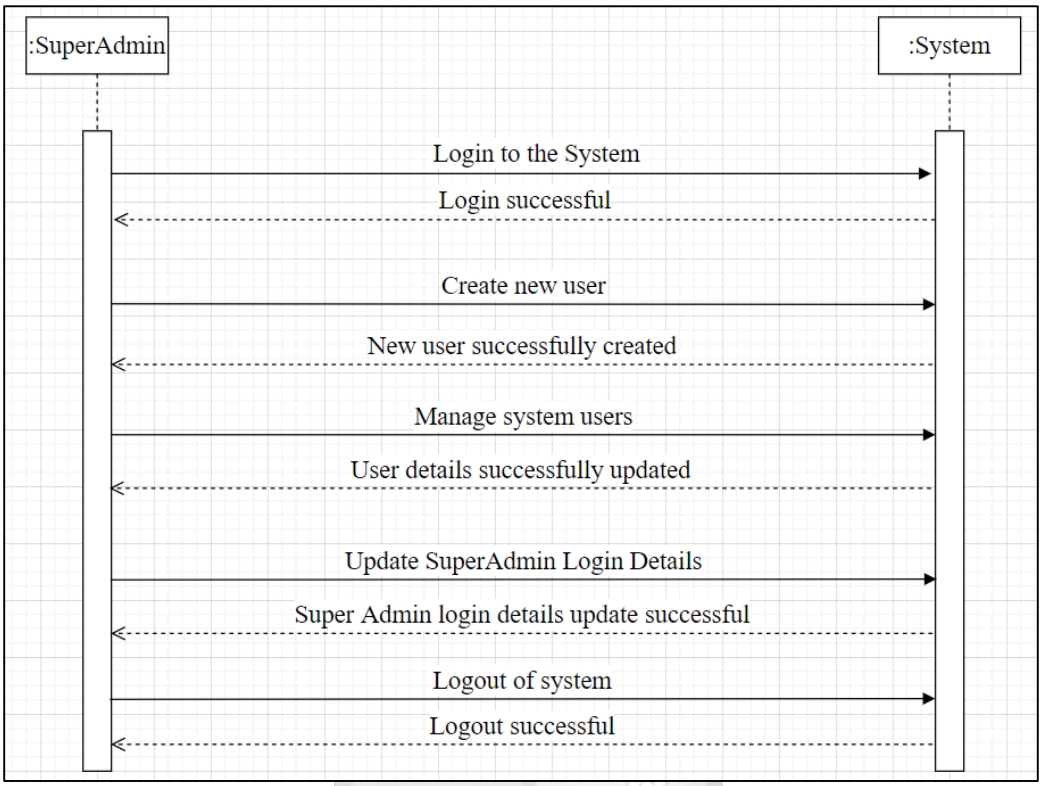


Figure 4.15: Sequence Diagram for SuperAdmin

Figure 4.16 shows the reporter's flow of actions on the system and responses.

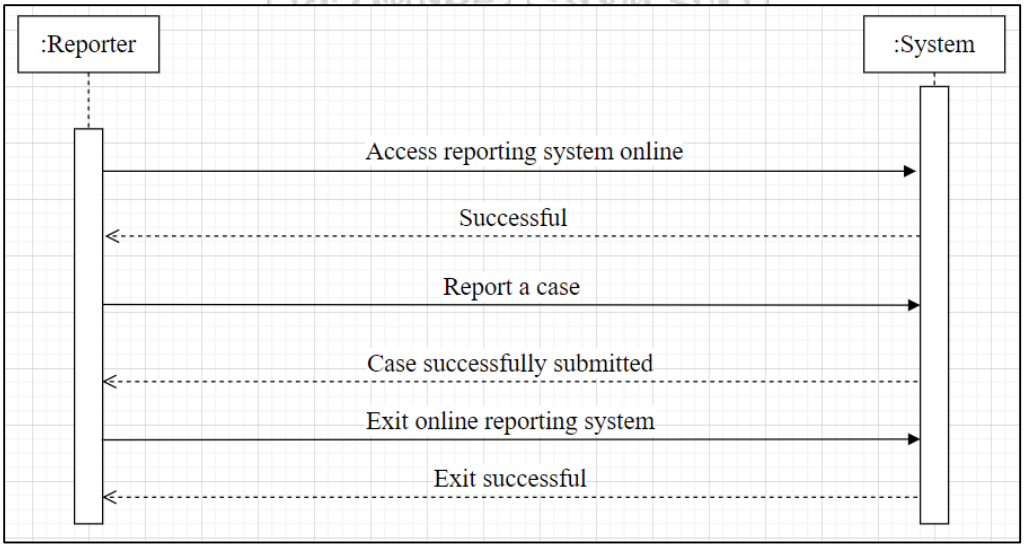


Figure 4.16: Sequence Diagram for the Reporter

Figure 4.17 shows Admin's flow of actions on the system and responses.

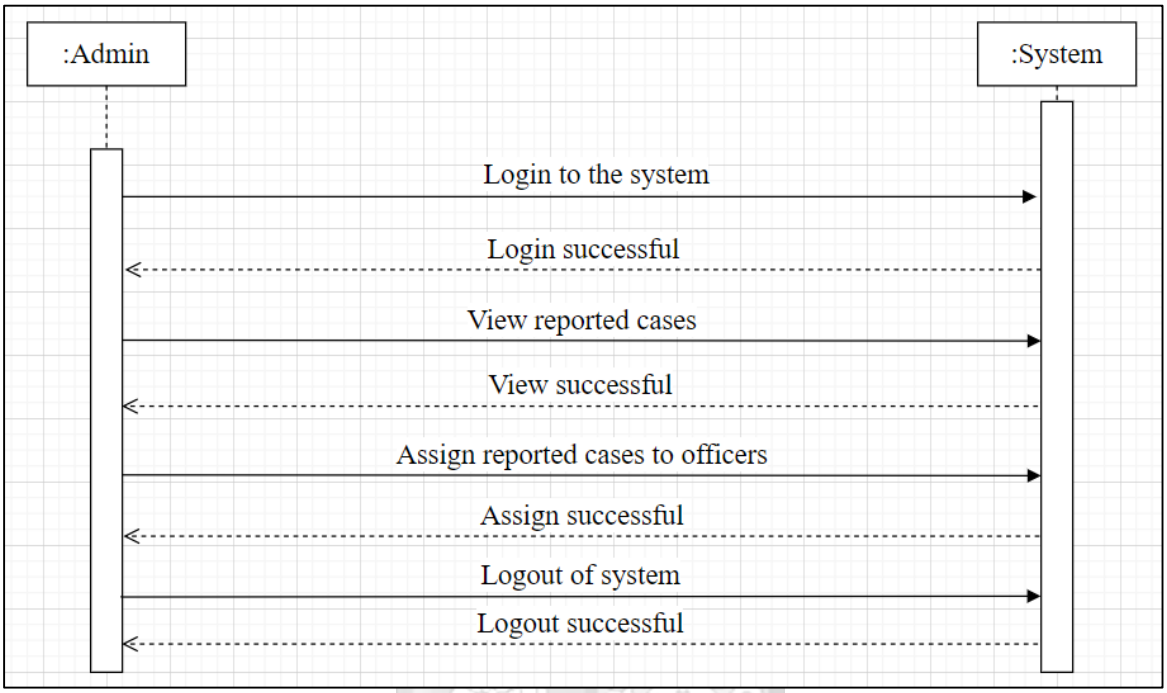


Figure 4.17: Sequence Diagram for Admin

Figure 4.18 shows Officer's flow of actions on the system and responses.

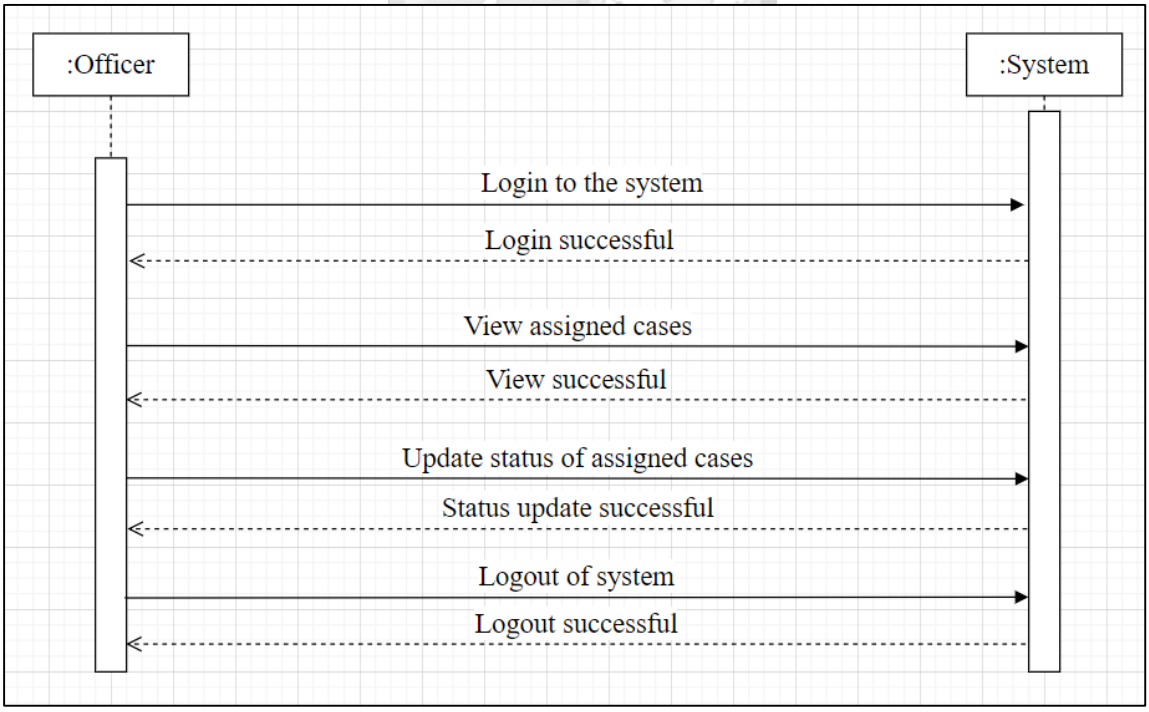


Figure 4.18: Sequence Diagram for Officer

Figure 4.19 shows the reporter's flow of actions on the system and responses.

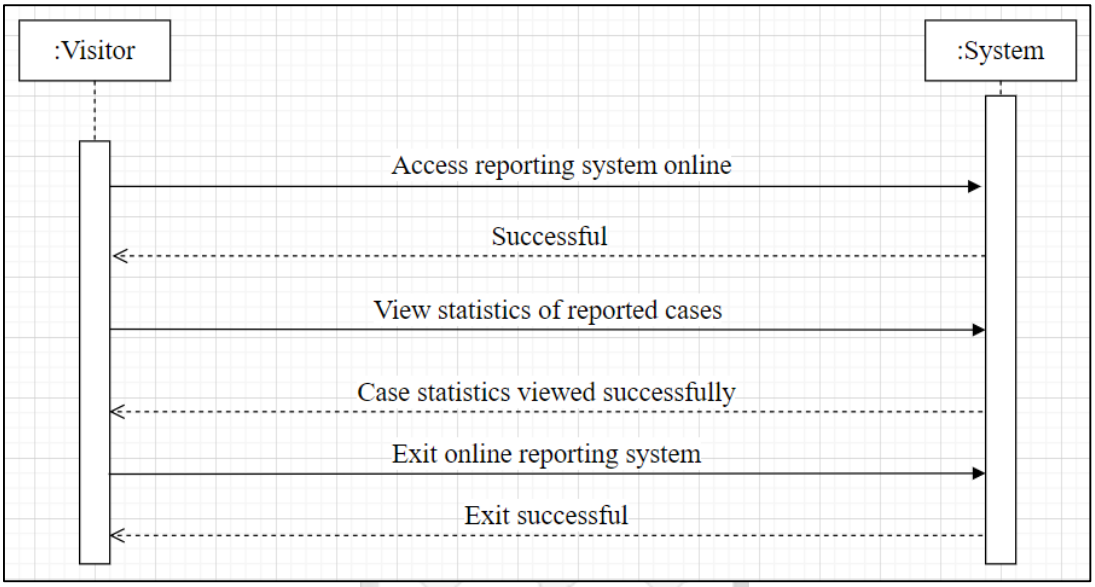


Figure 4.19: Sequence Diagram for Visitor

4.3.6 Database Structure

The database was build using Firebase Real-time Database, a cloud hosted NoSQL document database for mobile and web app development. On Firebase, storage, real-time synching and querying of app data are done at a global scale. Firebase is a product of Google (Google Developers, 2022).

The database structure is represented by a JSON tree on Figure 4.20 while Figure 4.21 and Figure 4.22 represent the objects on the database.

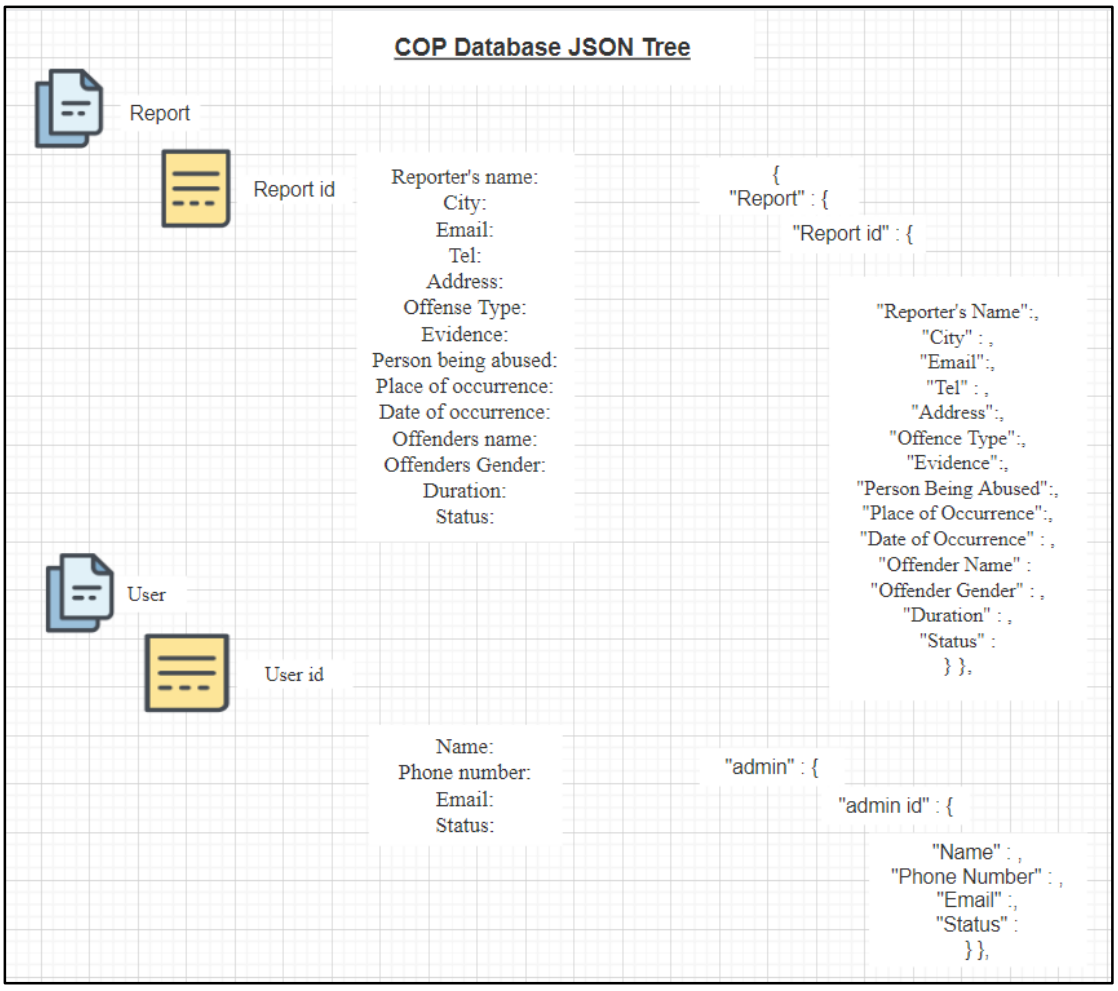


Figure 4.20: Database JSON Tree

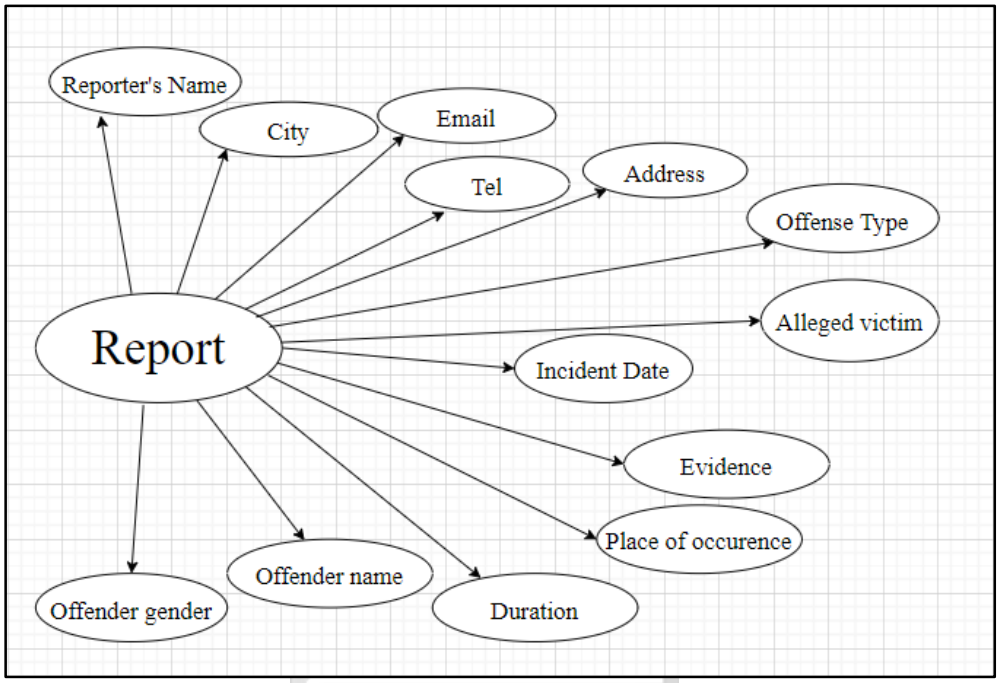


Figure 4.21: JSON Object – Report

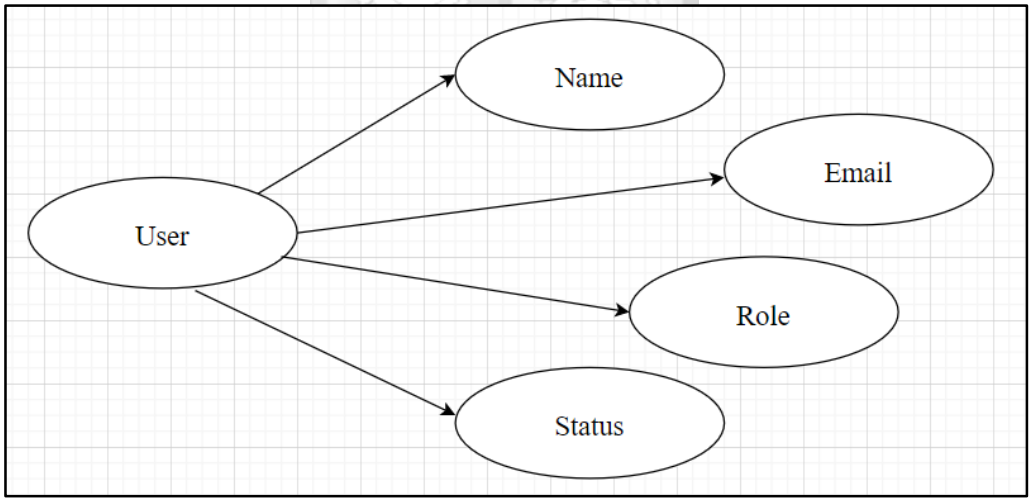


Figure 4.22: JSON Object - User

4.3.7 Wireframes – Web Application

The wireframes for the web platform are shown in Figure 4.23, Figure 4.24, Figure 4.25, Figure 4.26, Figure 4.29, Figure 4.28, Figure 4.29 and Figure 4.30.

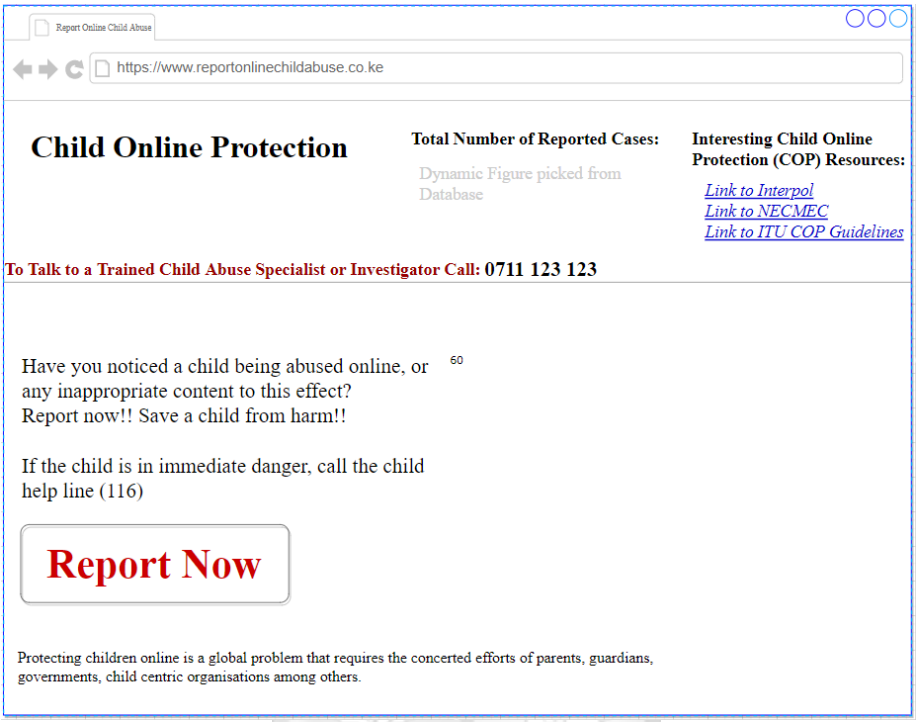


Figure 4.23: Landing Page

Figure 4.24: Reporting Page

Figure 4.25: Report Successfully Submitted

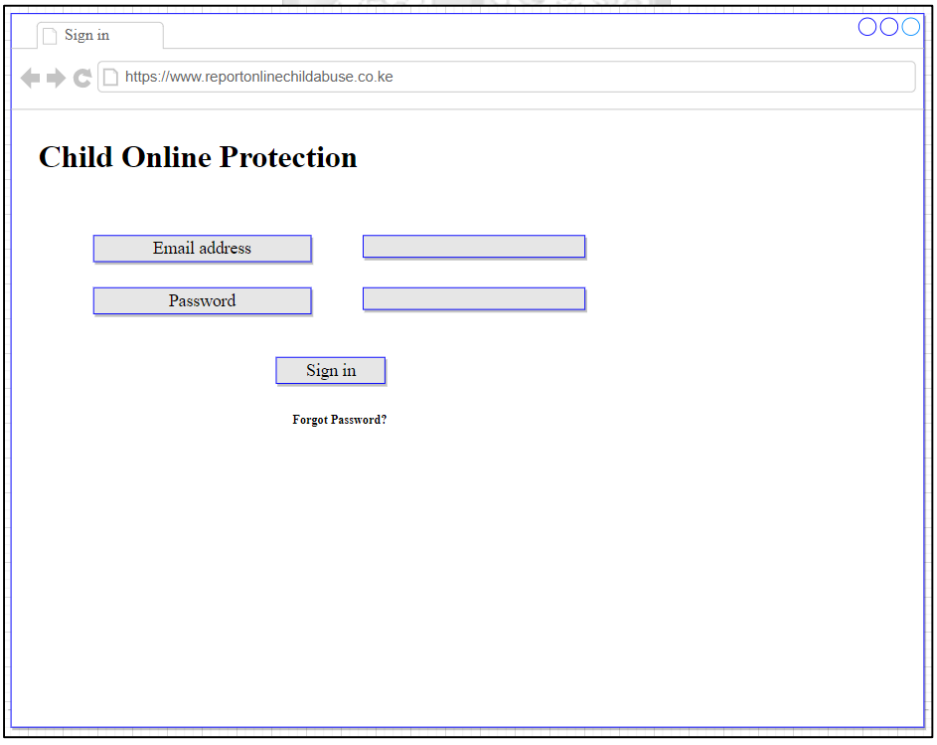


Figure 4.26: Law Enforcement Agency (LEA) Sign-in Page

Figure 4.27: SuperAdmin Landing Page

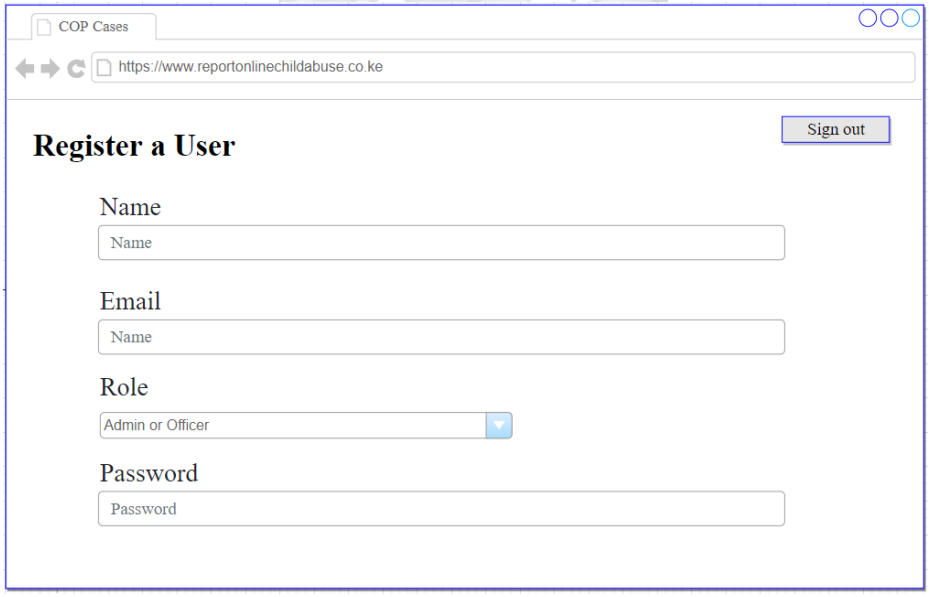


Figure 4.28: SuperAdmin on Clicking Register Users

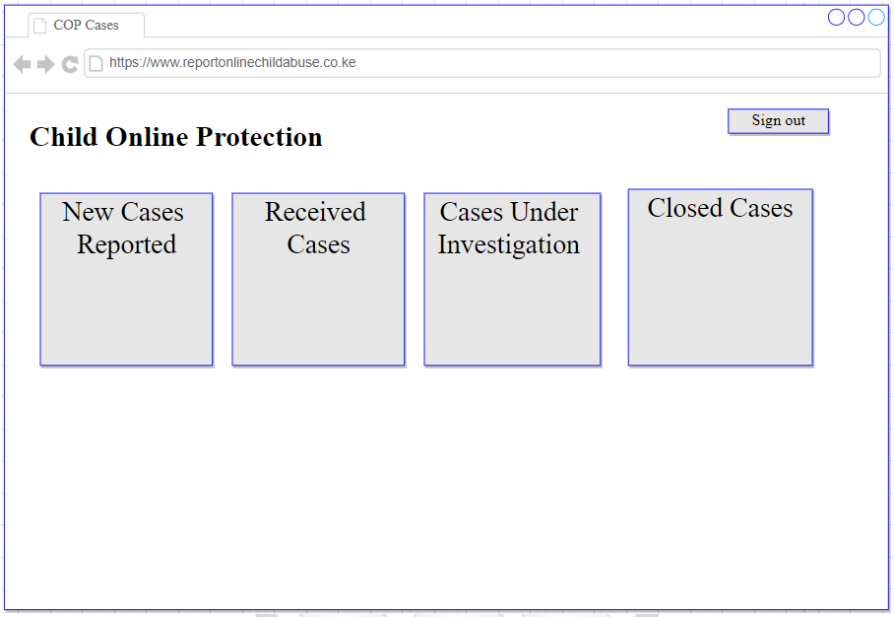


Figure 4.29: Admin on Clicking View Reports

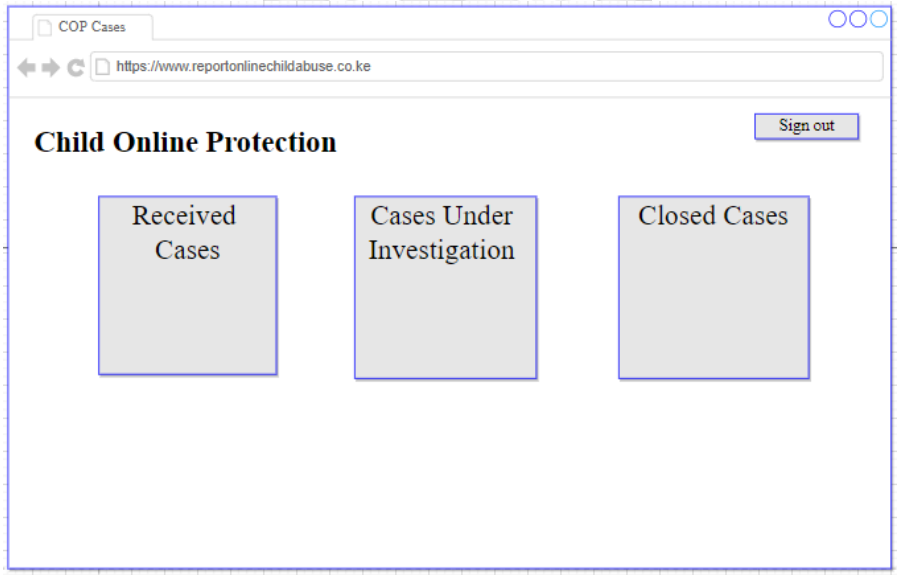


Figure 4.30: Officer Landing Page

4.3.8 Wireframes – Mobile Application

The wireframes for the mobile application are shown in Figure 4.31, Figure 4.32, and Figure 4.33.

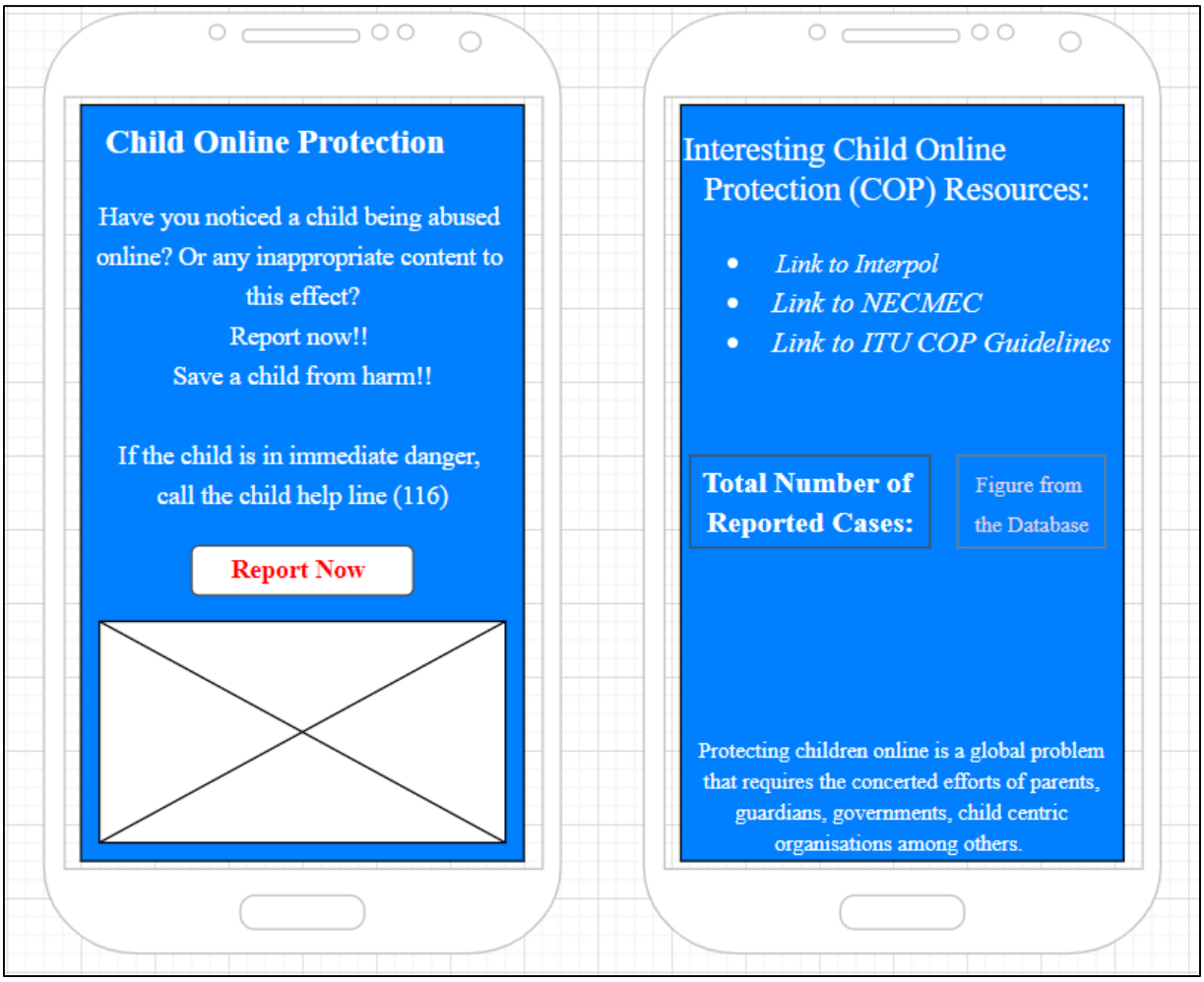


Figure 4.31: Mobile Device - Home Page

Figure 4.32: Mobile app - Report a Case

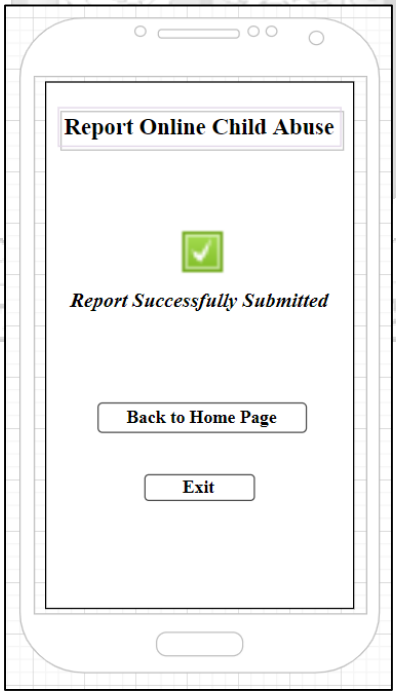


Figure 4.33: Mobile App - Report Successfully Submitted

4.4 Chapter Summary

The focus of this chapter was the system design beginning from requirements gathering from key stakeholders and intended system users. The data collected was used to define the system's functional and non-functional features. The overall model was used to depict the overall systems components. Use case modelling was done to come up with the use case descriptions and diagrams for the system. Sequence diagrams were used to represent interactions of different users with the system. The database structure was designed using a JSON tree and the respective objects shown. Finally, the Web and Mobile application wireframes were designed.

CHAPTER 5: SYSTEM IMPLEMENTATION AND TESTING

5.1 Introduction

System implantation and testing is dealt with on this chapter. The hardware and software tools and techniques employed during the implementation process are described.

5.2 System Implementation

5.2.1 Hardware and Software Requirements

The system implementation was done using Dart Programming Language (Dart Development Community, 2022) on flutter, an open source framework by Google for building of natively compiled applications for mobile, web, desktop, and embedded devices from a single codebase (Flutter Developers Community, 2022). This hastens the development process enabling the developer to focus on delivering system functionality. The user interfaces were designed using Figma, a web based UI design tool (Figma Development Community, 2022).

The database was build using Firebase Real-time Database, a cloud hosted NoSQL database which accelerates development by managing the backend and authentication. (Google Developers, 2022)

The system specifications for development and proper running of the tools mentioned above were at least Core i5 processor with a 2.4 GHz speed, 8 GB RAM, and 500 GB Hard Drive. Since the system is web based, accessing and using it requires only internet access from any internet enabled device.

5.2.2 Web Application Screenshots

Screenshots of the system showing different functionalities are given. Figure 5.1 shows the landing page of the system. On this page, a reporter can click on the report button make a report. One can view statistics of the reported cases and also access some useful links on Child Online Protection. The law enforcement agencies can also make use of the sign in to access and review the reports made.

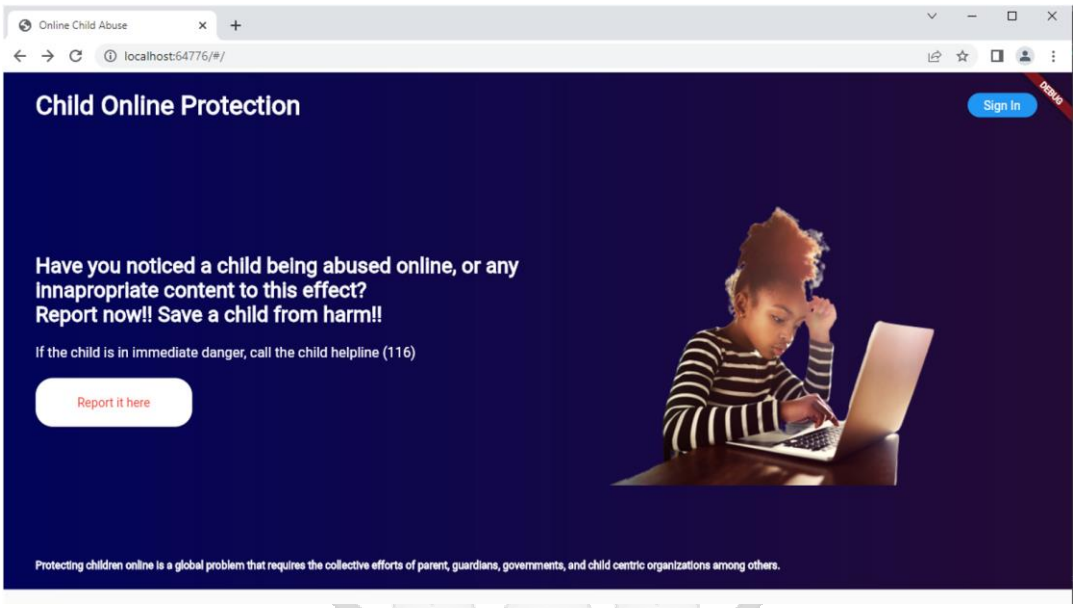


Figure 5.1: Landing Page for the Reporter and general public

On clicking report, the user gets a form to fill in with details of the abuse being reported (See Figure 5.2, Figure 5.3 and Figure 5.4). Among all the fields given, the only mandatory field is the evidence that needs to be attached since this alone can be used by Law Enforcement Agencies to kick off investigations.

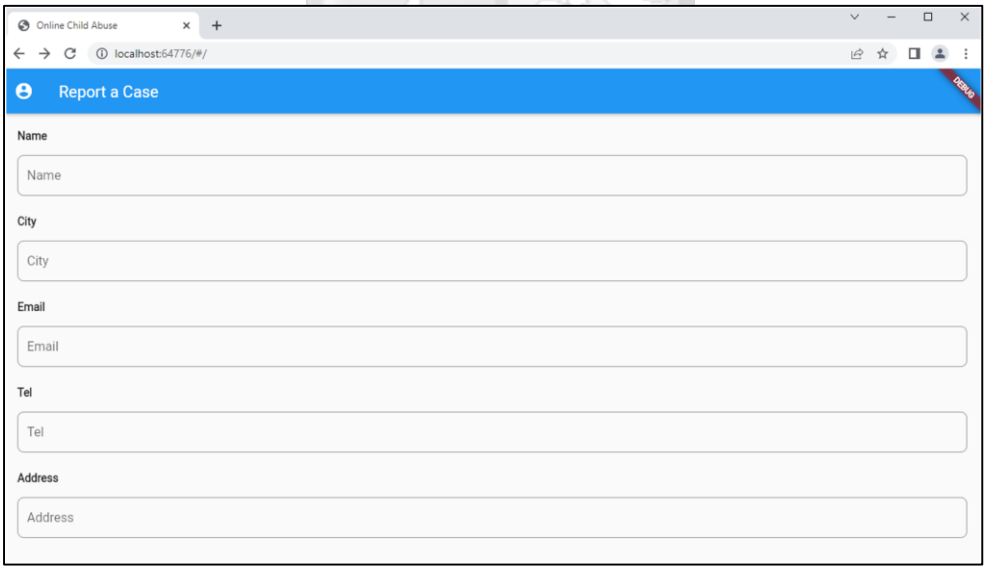


Figure 5.2: Fields That a Reporter Fills-in When Reporting a Case

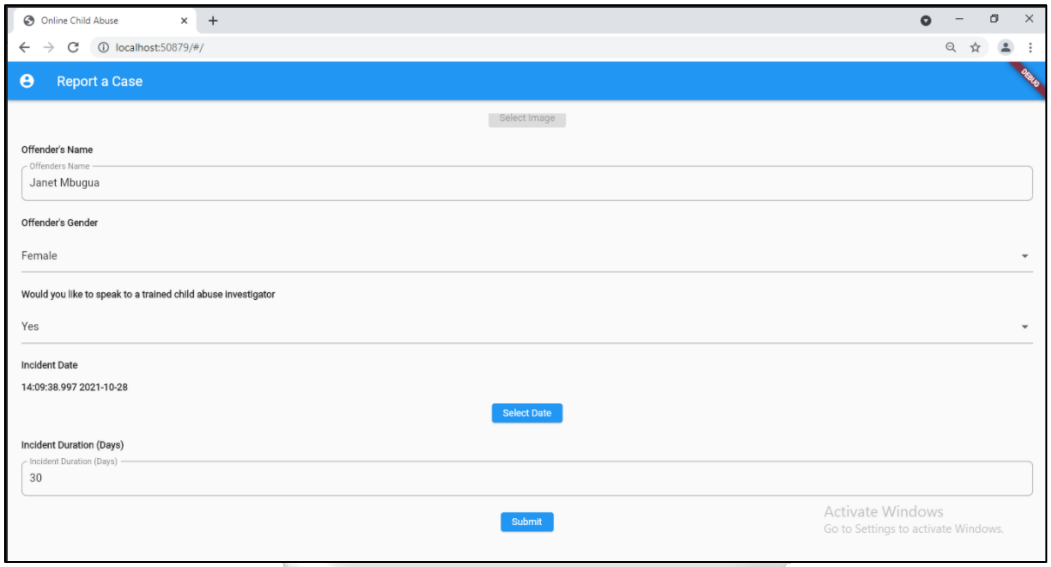


Figure 5.3: Fields That a Reporter Fills-in When Reporting a Case

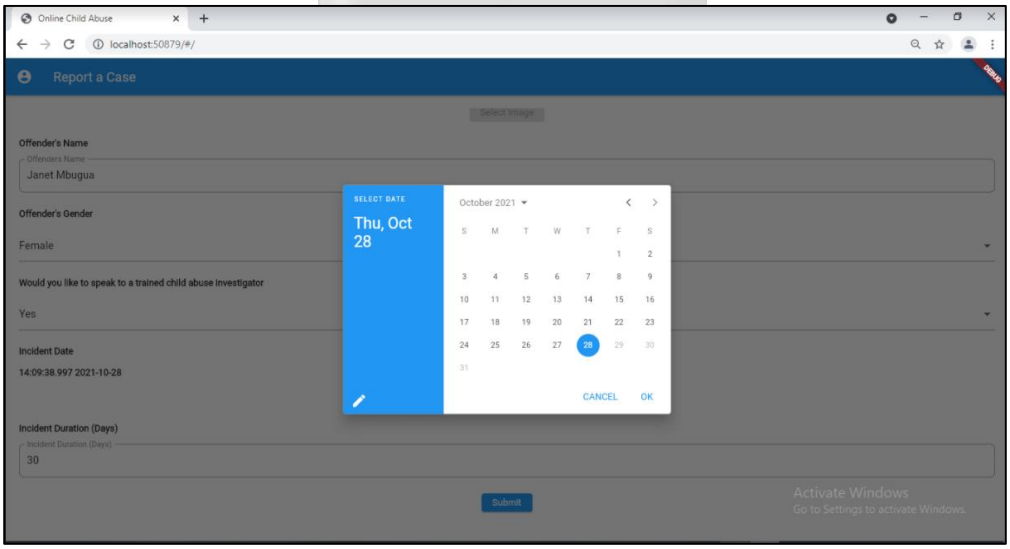


Figure 5.4: Fields That a Reporter Fills-in When Reporting a Case - Date Entry

On pressing the submit button, a reporter gets a notification of success if the mandatory entry has been made. See snapshot on Figure 5.5.

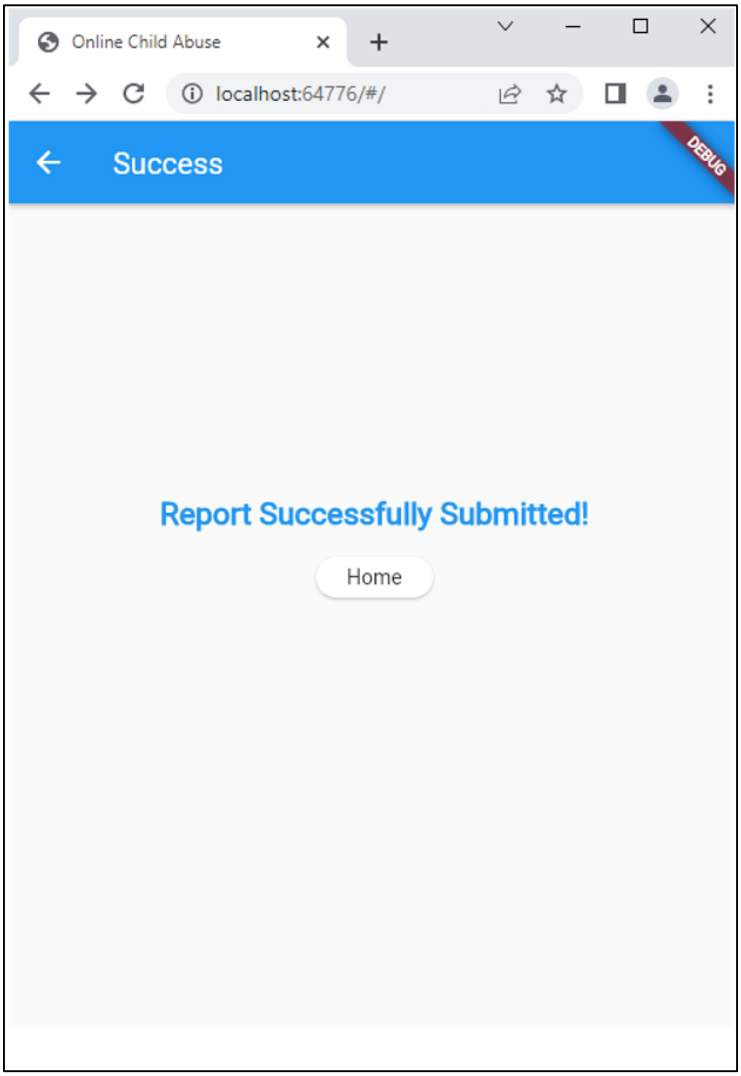


Figure 5.5: On Successfully submitting a report

The Law Enforcement Agency can gain access to the reported cases by signing into the system on the backend using their email and password as seen on

Figure 5.6. Users are created on the system by the 'SuperAdmin'. Management of the authentication process is handled by firebase authentication.

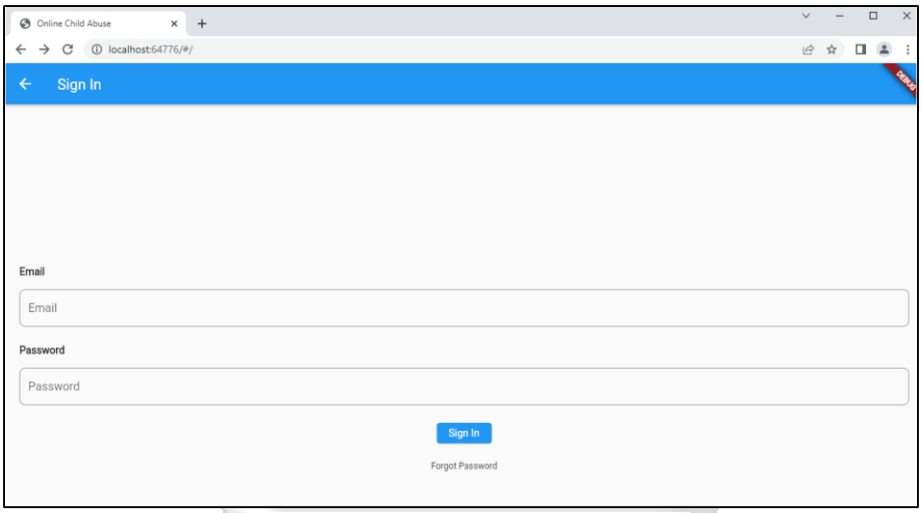


Figure 5.6: User Sign-in

On successfully signing in, the admin can Register users or view the reported cases on the system. The admins role is to assign the reported cases to officers for follow-up. See Figure 5.7, Figure 5.8 and Figure 5.9.

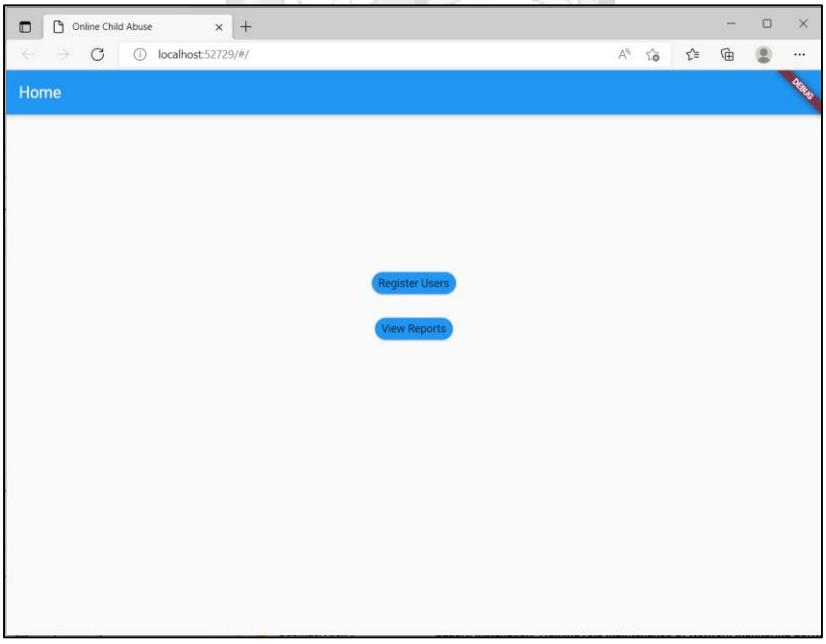


Figure 5.7: SuperAdmin Landing Page

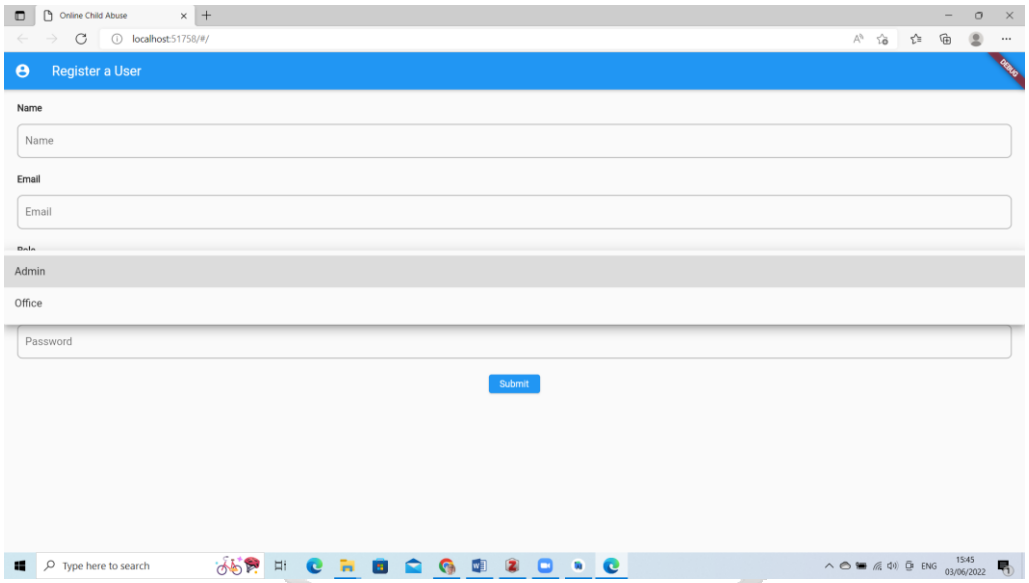


Figure 5.8: SuperAdmin On Clicking Register Users

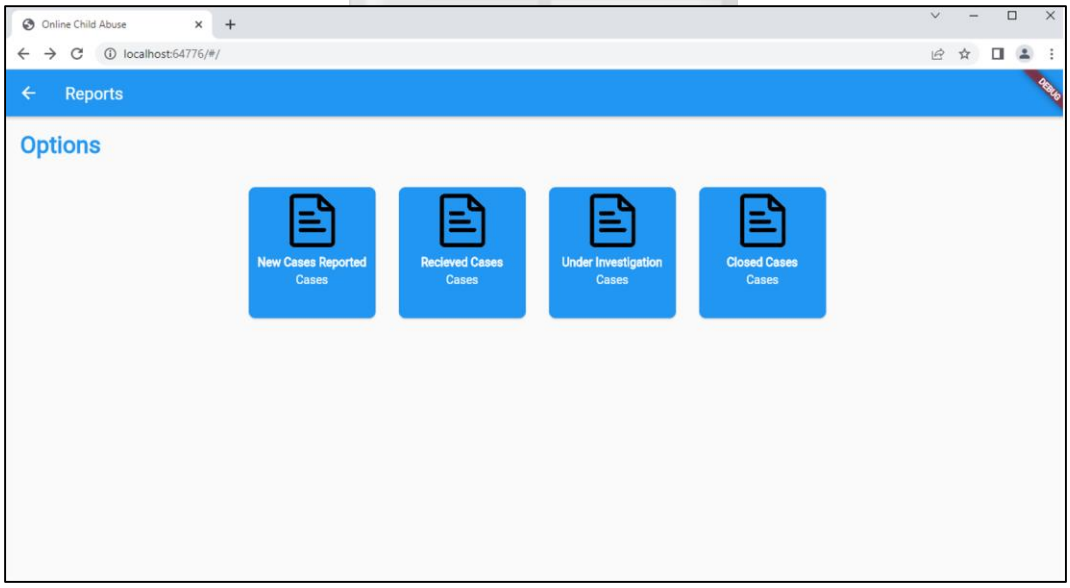


Figure 5.9: Admin On Clicking View Reported Cases

5.2.3 Mobile Application Screenshots

Screenshots of the mobile UI showing different functionalities are given. Figure 5.10 shows the landing page of the system. On this page, a reporter can click on the report button to make a report. The details that a user can give are shown in Figure 5.11, Figure 5.12, Figure 5.13, and Figure 5.14.

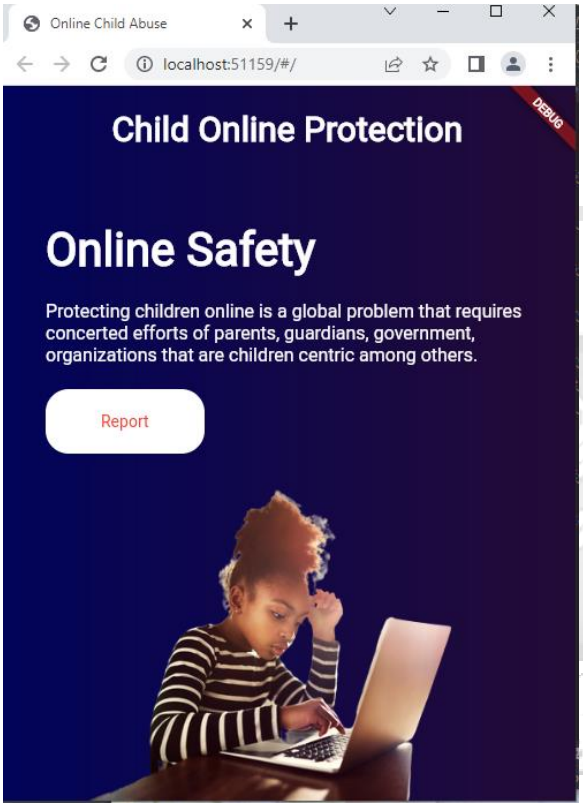


Figure 5.10: Mobile Landing Page

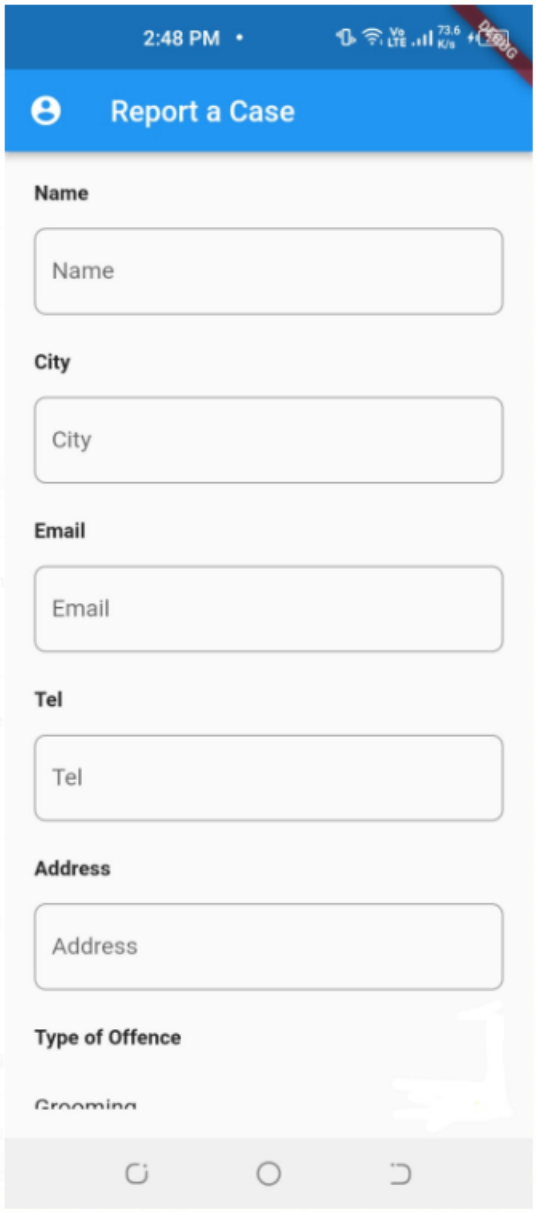


Figure 5.11: Reporting Page on the Mobile

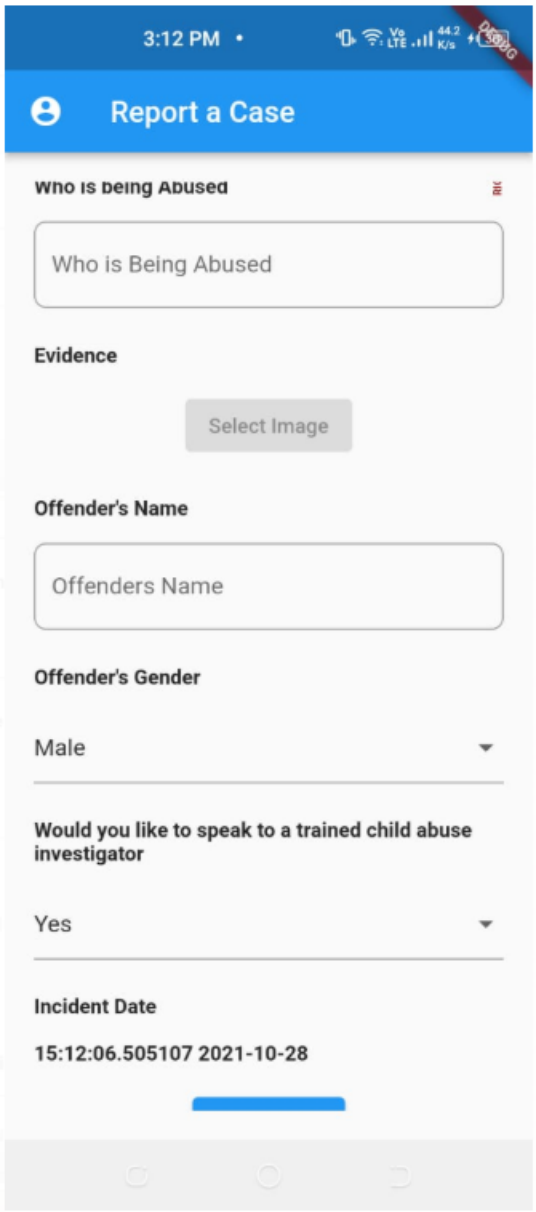


Figure 5.12: Mobile Reporting Page with Details Entered by the Reporter

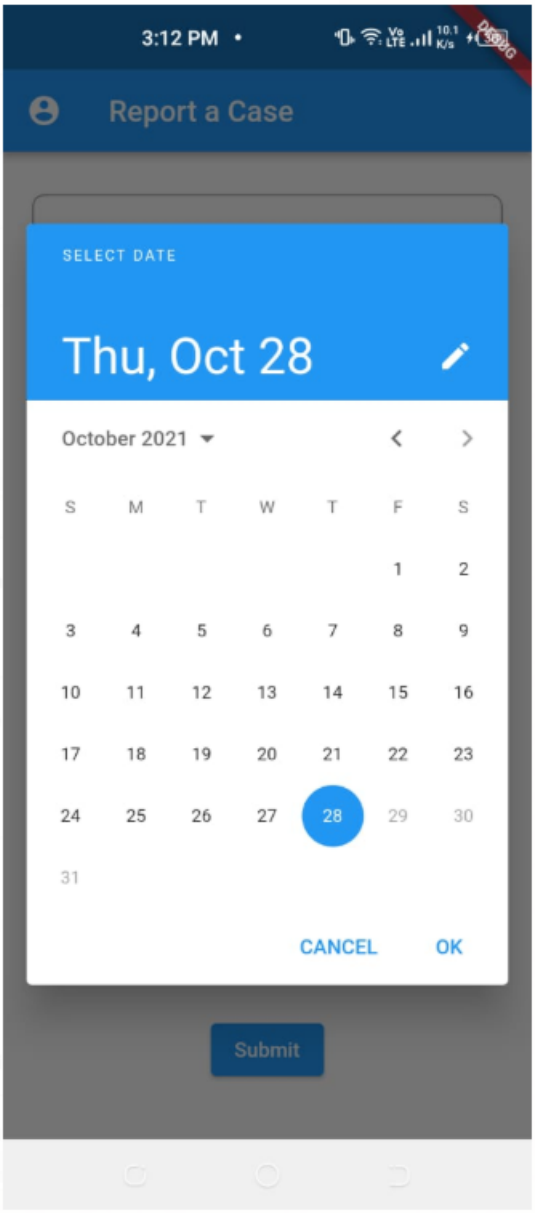


Figure 5.13: Mobile Reporting Page with Date Entry Ongoing

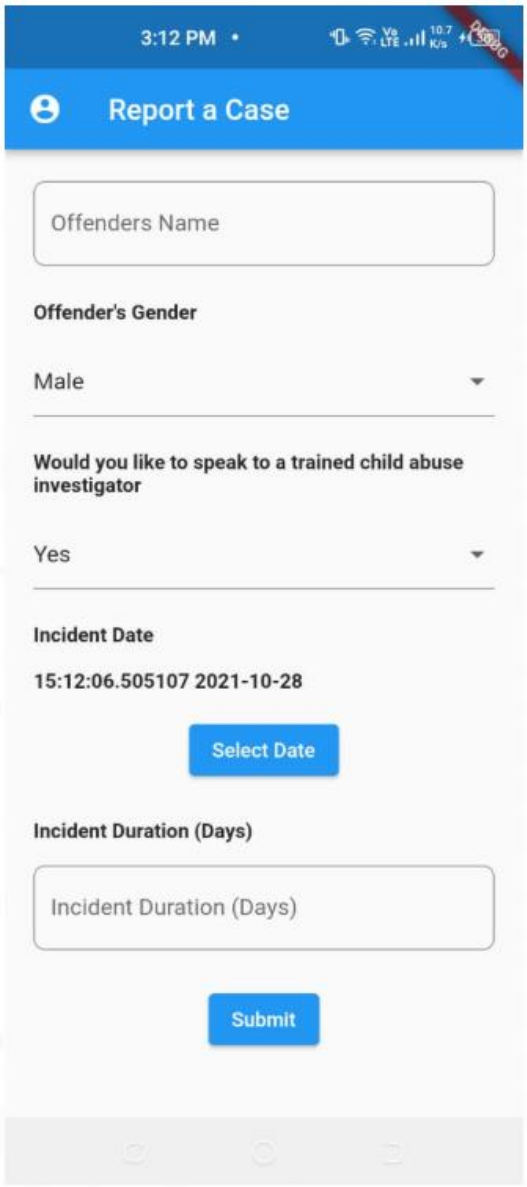


Figure 5.14: Reporting Page - More Details on the Incidence

5.2.4 Firebase Database Screenshots

Screenshots of the firebase database are given below showing the database structure, how reported cases are stored on the database system users and the folder with attached evidence. Figure 5.15 shows the 2 objects, report and users that are on the database. Details of one of the users highlighted are seen. Figure 5.16 shows the list of reported cases with the highlighted case showing more details. Figure 5.17 shows the folder containing attached evidence for a reported case.

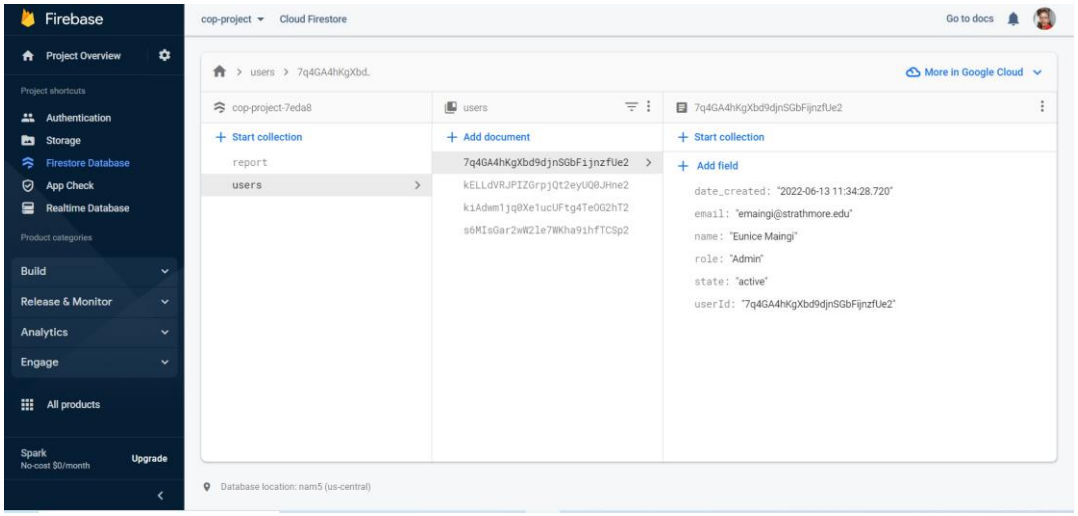


Figure 5.15: Database view showing the 2 objects (report and users) and the users

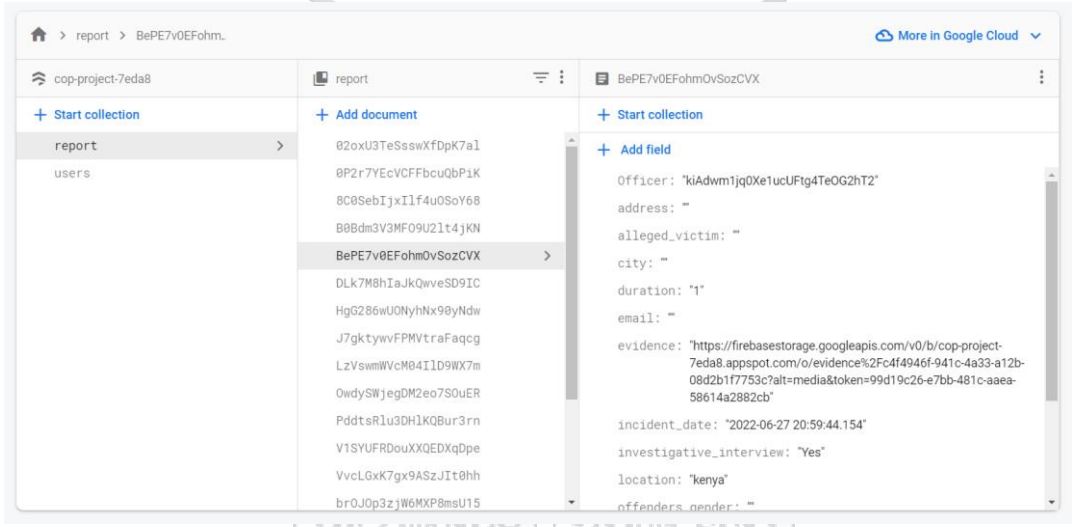


Figure 5.16: Database - List of reported cases and the details of the highlighted one

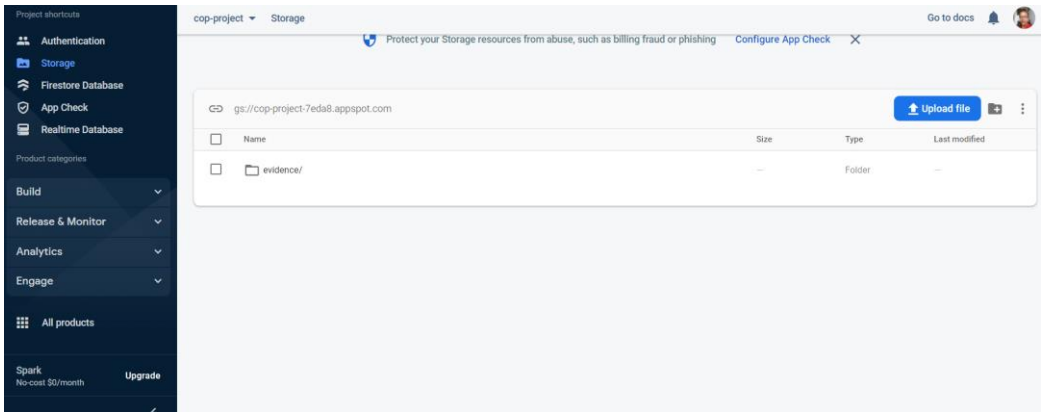


Figure 5.17: Database - Folder containing the evidence attached when reporting

5.3 System Testing

System testing was done by conducting a re-performance of the system functions required during the design. 5 random end users (reporters) and 5 random stakeholder users (from Law Enforcement Agency) tested the system based on the parameters given in Table 5-1 which form part of the system functionality requirements.

Table 5-1: System Testing Checks - Reporter

Feature	Tested		Successful
Ease of use	√		√
Ability to report anonymously	√		√
Ease of attaching evidence	√		√
Identity protection for victims and suspected offenders	√		√
Usable on mobile devices (phone, tablet, etc.)	√		√
Provides statistics of reported cases in the country	√		√

The 'SuperAdmin' role was used to create Law Enforcement Agency users at different roles, in addition to manipulating the status of created users from active to suspended and vice versa. The created users were required to manipulate the reported cases by assigning them to different users (Admin) and changing their status on review (Officer). User creation was successful and all the users performed their roles successfully and found the system easy to use as shown on Table 5-2.

Table 5-2: System Testing Checks – Law Enforcement Agency Users

Feature	SuperAdmin	Admin	Officer	Officer	Officer
Create users on the system	√				
Change created users status	√				
View reported cases on the system		√			
Assign reported cases to Admin2		√			
View assigned cases			√	√	√
Review & change status of assigned cases			√	√	√
Ease of system use	√	√	√	√	√

5.4 System Validation

Validation was done by creating Law Enforcement Agency (LEA) users from a close collaborator at different user levels on the system. After performing their different tasks on the system as defined by the assigned roles, the users from the Law Enforcement Agency (LEA) were required to evaluate based on their view of whether it solves the problem of reporting online child abuse cases and helps in investigation. All the sampled users agreed that the system solves the problem of not having an online platform for reporting online child abuse and that it will be facilitate investigations. See Table 5-3.

Table 5-3: System Validation Checks

Feature	**SuperAdmin**	**Admin**	**Officer**	**Officer**	**Officer**
Does the system resolve the problem of reporting online child abuse cases and help in investigation	√	√	√	√	√

CHAPTER 6: DISCUSSION

6.1 Introduction

This section outlines how the project objectives were fulfilled by referring to the work done in the research and development of the reporting system.

6.2 The Current Process of Handling Online Child Abuse in Kenya and Its Weaknesses

Through the review of literature conducted in Chapter 2, it was noted that the Kenyan government has defined various legislative measures to regulate online conduct, activities, and content. These measures include policies, statutes and even the establishment of government institutions dealing with children's rights and protection. Kenya also has ratified some international instruments to aid in the protection of children online.

The Child Help Line 116 telephone line managed by the National Council for Children Services (NCCS) deals will all forms of child exploitation. People can call to report any incidences and statistics are maintained on the Children Protection Information Management System (CPIMS). It was however noted that the statistics given do not include any information about online child abuse but only covers other forms of child abuse. Having a platform giving this information would help in the investigation and public awareness about online child abuse.

Until recently, reporting of child online abuse offenses (both online and offline) has been mainly done on the helpline. The National Computer Incidence Response Team (KE-CIRT) was recently (during this research) updated to include a section where child online abuse can be reported. This section is not so direct for the citizens as it is a small section of the KE-CIRT. Further, users don't have a way of giving any evidence of the case they are reporting. A platform solely dedicated to child online abuse is more appropriate as it is more straight forward during the process of reporting, allows the attachment of a digital evidence and a location picker which are further tips to the crime investigation processes. This system will also be in direct use by Law Enforcement Agencies.

6.3 The Processes in Place in Other Countries to Handle Online Child Abuse

In the literature review (Chapter 2), the measures in place in other countries were reviewed. This review was done from the global perspective, down to the regional (East Africa) and finally Kenya. The United Nations Convention on the Rights of the Child (UNCRC) ratified by Kenya in 1990

and The African Charter on the Rights and Welfare of the Child (ACRWC) are some of the cross-border policies in place and that have been ratified by Kenya.

Various ways of dealing with child abuse by other countries were also reviewed. It was noted that there are many countries with more advanced processes of dealing with online child abuse, which include national child online protection guidelines (ITU etc.), varied reporting and public awareness platforms, sections on police websites and the establishment of mandated notifiers among the citizens of different professions, especially those in close contact with children etc. A review of online abuse reporting platforms in other countries was done to get design ideas for the platform.

As the internet blurs the existing geographical boundaries and online crimes pervade these, corporation among nations is key in combating these offenses. A key step by the Kenyan government in the area of combatting online child abuse is connection to INTERPOL's International Child Sexual Exploitation (ICSE) database (INTERPOL) making it the first among countries in Africa to connect to INTERPOL. Information collected from the designed reporting platform can be further analysed on INTERPOL to speed up investigations.

6.4 System Design, Development, and Testing

Agile development methodology was used to develop the system. It consists of 5 basic processes as shown as listed below:

1. Planning
2. Requirements Gathering
3. Design
4. Development
5. Testing

To establish the desirable system features from the users and key stakeholders, interviews and questionnaires were used to collect data. Based on the data collected and analysed, functional and non-functional requirements were outlined. The conceptual modelling where the different actors, attributes and relationships are defined was done to visualize the system. Further use case diagrams, sequence diagrams and the wireframe designs were used to design and visualise the system.

Flutter framework (Flutter Developers Community, 2022), Dart programming language (Dart Development Community, 2022) and Figma (Figma Development Community, 2022) were used in the system development for both the web and mobile application. Firebase Real Time Database (Google Developers, 2022) was used for the database design and information storage.

The developed system is an online platform that is both web and mobile based accessible by the general public to report any instances of child online abuse. In addition, from the reports made, some statistics of the numbers, types of online abuse reported and resourceful links on the subject of online child abuse are also provided for public awareness. The platform is also used by the Law enforcement agencies to receive, review and investigate the reported cases of online child abuse. Since reporters can attach evidence in the form of images while reporting, the Law Enforcement Agencies can use this evidence material during their investigations. Evidence attached can be further analysed other forensics tools or even on Interpol or other more sophisticated child online abuse platforms.

6.5 Effectiveness of the System in Reporting Online Child Abuse

The systems effectiveness in resolving the problem of reporting and maintaining a record of online child abuse was evaluated by selecting a subset of intended systems users and stakeholders to evaluate how the system worked. The intended system users included the general public (who would report crimes) and law enforcement personnel (who would receive, review and act on the reported crimes). The feedback obtained from the sampled users reflected that the system worked as intended and that the users were satisfied as shown on the detailed results discussed on Table 5-1, Table 5-2 and Table 5-3.

CHAPTER 7: CONCLUSIONS AND RECOMMENDATIONS

7.1 Conclusions

Online abuse of children is rampant worldwide. This has been aggravated by the increased use of technology in education aimed at developing the children's interest in technology from an early age. Further, the ongoing COVID-19 pandemic necessitated virtual learning and teaching in many countries. Children, having now been pushed to the virtual platforms ought to be protected from any harm that they may encounter while online. Furthermore, if such harm has been realized by a child, reporting of the same and seeking justice for the child and punishment for the criminal should be made easier for anyone. Reporting such offenses helps in the investigation, retrieval and removal of any online content that might continue harming the child's welfare in future.

To facilitate this process, the system developed will aid in the reporting of online abuse cases by any party who is privy to any form of online child abuse. As the developed system allows for anonymous reporting, the reporters will not be required to disclose their identity, making more users comfortable to report any case. The system developed also provides statistics of online abuse prevailing in the country and links to informative sites on the topic of online child abuse. This feature will help the public as an invaluable source of information and knowledge.

7.2 Recommendations

The developed system should be adopted by the law enforcement agencies e.g. the police units or the Department of Criminal Investigations (DCI) children's section. On adoption, the system should be publicised to widen its user base and consequently the number of reported cases. Its adoption will allow easy reporting of online offenses by the citizens and also facilitate the process of investigation. Citizens will be enabled to conveniently give tips on any ongoing online crime against children.

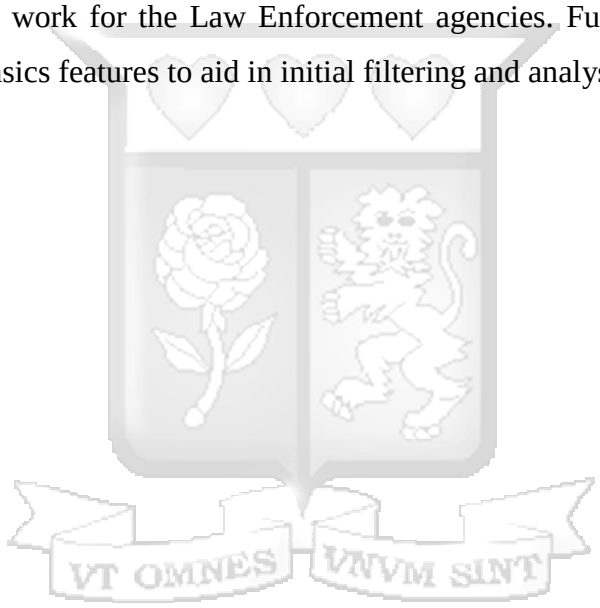
The system can be implemented centrally by the DCI, while the admin roles are allocated to individual police stations or units. Cases related to a specific area can be assigned to police units or officers in the affected area for ease of investigation especially in cases where they also point to offline abuse too.

Consolidated online child abuse Intelligence can be used for strategic decision making regarding the training and reinforcement of the officers and agencies that handle children's protection.

7.3 Future Work

In the future, the system can be improved to provide more reports, educational material and informative tips for the users. Willing reporters who give their identity could also be enabled to track or receive updates on reported cases. Developing a USSD option for reporting will help in widening the coverage of people from all over, including the rural population, where many people own feature phone.

The system has no way of eliminating false reporting by the public. This is a feature that can be developed to better the system. At the moment, the only assumed deterrence to false reporting is the possibility of tracking down the source of the false report and punishing the one responsible, which would mean more work for the Law Enforcement agencies. Further, the system can be enhanced to include forensics features to aid in initial filtering and analysis of attached evidence.



REFERENCES

African Union. (2019). *African Charter on the Rights and Welfare of the Child | African Union*. Au.Int/En/Treaties/African-Charter-Rights-and-Welfare-Child. https://au.int/en/treaties/african-charter-rights-and-welfare-child

Akbar, Z., Putri, T., & Aisyawati, M. (2020). CYBERBULLYING: DEFINITION AND MEASUREMENT IN ADOLESCENT – LITERATURE REVIEW. *Humanities & Social Sciences Reviews*, *8*, 18–26. https://doi.org/10.18510/hssr.2020.843

Allan, L. (2022, February 8). *Online Abuse | Different types, effects, signs, avoiding & reporting*. CPD Online College. https://cpdonline.co.uk/knowledge-base/safeguarding/online-abuse/

Andrews, D., Alathur, S., Chetty, N., & Kumar, V. (2020). Child Online Safety in Indian Context. *2020 5th International Conference on Computing, Communication and Security (ICCCS)*, 63–77. https://doi.org/10.1109/ICCCS49678.2020.9277038

Ben-Ze'ev, A. (1981). J.J. Gibson and the ecological approach to perception. *Studies in History and Philosophy of Science*, *12*, 107–139. https://doi.org/10.1016/0039-3681(81)90016-9

Centre to Counter Child Exploitation. (2018). *Report abuse | ACCCE*. https://www.acccе.gov.au/report

Communications Authority of Kenya. (2020). *KE-CIRT – Communications Authority of Kenya*. https://ke-cirt.go.ke/

Communications Authority of Kenya. (2021). About KE-CIRT. *Communications Authority of Kenya*. https://ca.go.ke/industry/cyber-security/about-ke-cirt/

Communications authority of Kenya. (2021). Sector Statistics Report Q4 2020-2021. *Communications Authority of Kenya*. https://www.ca.go.ke/document/sector-statistics-report-q4-2020-2021/

Cooper, K., Quayle, E., Jonsson, L., & Svedin, C. G. (2016). Adolescents and self-taken sexual images: A review of the literature. *Computers in Human Behavior*, *55*, 706–716. https://doi.org/10.1016/j.chb.2015.10.003

Dart Development Community. (2022). *Dart overview*. Dart. https://dart.dev/overview.html

Directorate of Criminal Investigations. (2020). *Anti-Human Trafficking & Child Protection Unit(AHTCPU).* ANTI-HUMAN TRAFFICKING & CHILD PROTECTION UNIT(AHTCPU). https://www.cid.go.ke/index.php/sections/investigationunits/anti-human-trafficking-child-protection-unit-ahtcpu.html

DQ Institute, G. S. for D. I. (2021). *Check Out the Best Countries for Child Online Safety | DQ Institute*. https://www.dqinstitute.org/child-online-safety-index/

ECPAT. (2021). *ECPAT Resources Archive*. ECPAT International. https://www.ecpat.org/resources/

ECPAT International. (2021). ECPAT International—What we do. *ECPAT International*. https://www.ecpat.org/what-we-do/

Figma Development Community. (2022). *Figma: The collaborative interface design tool.* Figma. https://www.figma.com/

Flutter Developers Community. (2022). *Flutter—Build apps for any screen*. //flutter.dev/

Google Developers. (2022). *Firebase Realtime Database | Store and sync data in real time*. Firebase. https://firebase.google.com/products/realtime-database

Governor, J. P. (2021). *State of Illinois | Online Child Abuse Neglect Reporting: Home*. https://dcfsonlinereporting.dcfs.illinois.gov/

Hamilton-Giachritsis, C., Hanson, E., Whittle, H., Alves-Costa, F., & Beech, A. (2020). Technology assisted child sexual abuse in the UK: Young people's views on the impact

of online sexual abuse. *Children and Youth Services Review*, *119*, 105451. https://doi.org/10.1016/j.childyouth.2020.105451

Hanson, E. (2017). The Impact of Online Sexual Abuse on Children and Young People: Impact, Protection and Prevention. In *Online Risk to Children: Impact, Protection and Prevention: First Edition* (pp. 97–122). https://doi.org/10.1002/9781118977545.ch6

Internet Society. (2021). *Learning*. https://learning.internetsociety.org

Interpol. (2019, May 20). *Kenya first African country to connect to the International Child Sexual Exploitation database*. https://www.interpol.int/en/News-and-Events/News/2019/Kenya-first-African-country-to-connect-to-the-International-Child-Sexual-Exploitation-database

INTERPOL. (2021). *International Child Sexual Exploitation database*. https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

ISO/IEC JTC 1, Information technology, SC 27, IT Security techniques. (2012, July). *ISO/IEC 27032:2012(en), Information technology—Security techniques—Guidelines for cybersecurity*. ISO/IEC 27032:2012(En) Information Technology — Security Techniques — Guidelines for Cybersecurity. https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

ISPCAN. (2016, October). *4.21-Expert Paper The Recovery and Reintergration of Children.pdf*. Ecpat.Org. https://www.ecpat.org/wp-content/uploads/2016/10/4.21-Expert-Paper-ISPCAN.pdf

ITU. (2020). *Guidelines for policy-makers on Child Online Protection 2020*. International Telecommunications Union. https://www.itu-cop-guidelines.com/policymakers

KAACR, K. A. for A. of C., & ECPAT International. (2019). *Sexual Exploitation of Children in Kenya Submission for the Universal Periodic Review of the Human Rights situation in Kenya* (UPR third cycle 2017 – 2021; 35 Th Session (January 2020)). Human Rights Council.

Kenya Film Classification Board (KFCB). (2021). *Home | Kenya Film Classification Board (KFCB)*. https://kfcb.go.ke/

Children Act, No 8 of 2001 (2001). http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ChildrenAct_No8of2001.pdf

Sexual Offenses Act, 3 of 2006 (2006). https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---ilo_aids/documents/legaldocument/wcms_127528.pdf

Counter Trafficking in Persons Act, 8 of 2010 18 (2010). http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/Counter-TraffickinginPersonsAct_No8of2010.pdf

Computer Misuse and Cybercrimes Act, No 5 of 2018 (2018). http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf

Data Protection Act, No. 24 of 2019 49 (2019). http://www.kenyalaw.org/kenya_gazette/gazette/notice/206587/

Kenya National Bureau of Statistics, K. (Ed.). (2019a). *2019 Kenya population and housing census: Vol. III*. Kenya National Bureau of Statistics. https://www.knbs.or.ke/?page_id=3142

Kenya National Bureau of Statistics, K. (2019b). *2019 Kenya Population and Housing Census Volume IV: Distribution of Population by Socio-Economic Characteristics: Vol. IV*.

Kenya National Bureau of Statistics. https://www.knbs.or.ke/download/2019-kenya-population-and-housing-census-volume-iv-distribution-of-population-by-socio-economic-characteristics/

Livingstone, S., & Smith, P. K. (2014). Annual Research Review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry, 55*(6), 635–654. https://doi.org/10.1111/jcpp.12197

Lynn, R. (2021). *What is FDD in Agile?* Planview. https://www.planview.com/resources/articles/fdd-agile/

May-Chahal, C., Dodd, S., Palmer, E., & Milan, S. (2018). *Rapid Evidence Assessment: Characteristics And Vulnerabilities Of Victims Of Online Facilitated Child Sexual Abuse And Exploitation.*

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence Chapter 1: Cyber-dependent crimes. *Home Office Research Report 75, Chapter 1: Cyber-dependent crimes*, 35.

Ministry of Labour and Social Protection. (2018). *NPA-against-SEC-Kenya-2018-2022.pdf.* Anppcan.Org. http://www.anppcan.org/wp-content/uploads/2014/11/NPA-against-SEC-Kenya-2018-2022.pdf

Miraz, M. H., Ali, M., Excell, P. S., & Picking, R. (2018). Internet of Nano-Things, Things and Everything: Future Growth Trends. *Future Internet, 10*(8), 68. https://doi.org/10.3390/fi10080068

Missouri Department of Social Services. (2021). *Online System for Child Abuse & Neglect Reporting (OSCR)*. Missouri Department of Social Services. https://apps.dss.mo.gov/OnlineCanReporting/default.aspx

National Centre for Missing and Exploited Children. (2020, December 11). *Exploted Children Statistics*. About NCMEC. https://www.missingkids.org/footer/media/keyfacts

National Council for Children's Services. (2017). *National Council for Children's Services*. http://www.childrenscouncil.go.ke/

Victim Protection Act, 17 of 2014 (2014). https://statelaw.go.ke/wp-content/uploads/2020/11/Victim-Protection-Act-17-of-2014.pdf

NCCS, N. C. for C. S. (2017). *Child Help line*. National Council for Children Services. http://www.childrenscouncil.go.ke/child-help-line.html

NIST, N. I. of S. and T. (2019, February 8). *Cyber Security basics, Glossary* [Text]. NIST. https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary

Norman, D. A. (1988). *The psychology of everyday things* (1st ed.). New York : Basic Books. https://hal.archives-ouvertes.fr/hal-00692043

Pyżalski, J. (2012). From cyberbullying to electronic aggression: Typology of the phenomenon. *Emotional and Behavioural Difficulties*, *17*(3–4), 305–317. https://doi.org/10.1080/13632752.2012.704319

Quayle, E. (2016). *Researching online child sexual exploitation and abuse: Are there links between online and offline vulnerabilities?* 48.

Quayle, E. (2020). Prevention, disruption and deterrence of online child sexual exploitation and abuse. *ERA Forum*. https://doi.org/10.1007/s12027-020-00625-7

Quayle, E., & Koukopoulos, N. (2019). Deterrence of online child sexual abuse and exploitation. *Policing*, *13*(3), 345–362. https://doi.org/10.1093/police/pay028

Sarre, R., Lau, L. Y.-C., & Chang, L. Y. C. (2018). Responding to cybercrime: Current trends. *Police Practice and Research*, *19*(6), 515–518. https://doi.org/10.1080/15614263.2018.1507888

South West Grid for Learning, Swg. (2020, October 2). *What is Online Safety? | SWGfL*. Online Safety. https://swgfl.org.uk/online-safety/what-is-online-safety/

The Public Prosecutor's Office, BEE SECURE, & ECPAT Luxembourg. (2021). *Childprotection.lu*. The Luxembourg Website for Reporting Child Sexual Exploitation. https://www.childprotection.lu/?lang=en#home

UN Human rights, Office of the High Commissioner, O. (2021). *OHCHR | Convention on the Rights of the Child*. https://www.ohchr.org/en/professionalinterest/pages/crc.aspx

UNICEF (Ed.). (2017). *Children in a digital world*. UNICEF.

UNODC, U. N. O. on D. and C. (2022). *Cybercrime*. United Nations : Office on Drugs and Crime. //www.unodc.org/unodc/en/cybercrime/index.html

Wangamati, C. K., Yegon, G., Sundby, J., & Prince, R. J. (2019). Sexualised violence against children: A review of laws and policies in Kenya. *Sexual and Reproductive Health Matters*, *27*(1), 16–28. https://doi.org/10.1080/26410397.2019.1586815

WeProtect Global Alliance. (2021). *Protecting children from sexual exploitation and abuse online 2—WeProtect Global Alliance*. https://www.weprotect.org/

Wittes, B., Poplin, C., Jurecic, Q., & Spera, C. (2016, May 11). Sextortion: Cybersecurity, teenagers, and remote sexual assault. *Brookings*.

https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/

Wolak, J., Finkelhor, D., & Mitchell, K. J. (2012). *Trends in Law Enforcement Responses to Technology-facilitated Child Sexual Exploitation Crimes: The Third National Juvenile Online Victimization Study (NJOV-3)*. 5.

World Health Organization, Department of Gender, W. and H., World Health Organization, & Injuries and Violence Prevention Department. (2003). *Guidelines for medico-legal care for victims of sexual violence.* World Health Organization. https://apps.who.int/iris/bitstream/handle/10665/42788/?sequence=1

APPENDICES

Appendix I: Interview Guide

Interview guide for staff working in institutions dealing with children.

1. Have you ever encountered any online child abuse cases in your institution?
   - Yes
   - No

2. What kind of online abuse content was it?

   - Cyber bullying
   - Cyber Grooming
   - Cyber Stalking
   - Violence
   - Possession and distribution of online child sexual abuse material (CSAM)
   - Production of online child sexual abuse material (CSAM)
   - Solicitation of sexual content (images & conversation) from children
   - Sexting
   - Sharing sexual content
   - Others (Specify)

3. If yes, please give some estimates of approximately how many you encounter e.g., in a month.
   - None
   - Below 5
   - 6 to 10
   - more than 10

4. Please select what applies to you below:

   - My institution receives reports of online child abuse cases
   - My institution reports cases of online child abuse to another institution

5. If you receive reports of online child abuse cases, how are they reported to you?
   - Verbally (people walk to make their reports)
   - On call (we have a known phone number used to make reports)
   - Online (we have an online platform for this)
   - All the above

6. If you report cases of online child abuse to another institution, please explain how you report them?
    - Verbally (people walk to make their reports)
    - On call (we have a known phone number used to make reports)
    - Online (we have an online platform for this)
    - All the above

7. What are the procedures/ measures in place for tackling online child abuse cases that are reported or that occur in your institution?
    - I don't know of any
    - We report to department manager
    - We report to the nearest police station
    - We report to the child help line
    - We provide guidance and counselling to the victim (s) without reporting

8. Do you think the procedures/ measures mentioned above are the most appropriate?
    - Yes
    - No

9. What would you change in the above-mentioned measures/ procedures?

10. Do you maintain the statistics of the reported/ received cases?
    - Yes
    - No

11. What do you use this information for? Do you share this information with other people/ institutions? If yes, which institutions and for what purpose do you share this information with them?
    - Yes
    - No

12. Do you think an online system to report/ receive reports of online child abuse cases would help the reporting and investigation process? (Yes or No) Please explain your response.
    - Yes
    - No

13. What desirable features would you want such an online child abuse reporting system to have?
    - Ease of use.
    - Ability to report anonymously.

- Ability to track the action taken on any reported case.
- Usable on mobile devices (phone, Tablet, etc.).
- Identity protection for victims and suspected offenders.
- Provides statistics of reported cases in the country.
- Others (Please specify) [ ]

14. Please share any comment or concern regarding child online sexual abuse that you may have?

[ ]

Appendix II: Questionnaire

Questionnaire used to collect information about online child sexual abuse reporting procedures and the suitability of an online reporting system.

1. Have you ever encountered any instance, case or online content that could be classified as online child abuse content?
   - Yes
   - No

2. What kind of online abuse content was it?

   - Cyber bullying
   - Grooming
   - Stalking
   - Violence
   - Possession, and distribution of Child Sexual Abuse Material (CSAM)
   - Solicitation of sexual content (images & conversation) from children
   - Sexting
   - Sharing sexual content
   - Other…

3. If yes, what step did you take?
   - Report to the nearest police station
   - Call child help line
   - Post on DCI page
   - I did not know what to do

4. Are you aware of the child help line or the child abuse hotline (116)?
   - Yes
   - No

5. Have you ever made use of this helpline?
   - Yes
   - No

6. If yes, did you get assistance?
   - Yes
   - No

7. Would you report any online child abuse via an online system? (Yes/ No) Please give a reason for your answer.

- Yes
- No

8. What desirable features would you want such a system to have?
   - Ease of use.
   - Ability to report anonymously.
   - Ability to track the action taken on any reported case.
   - Usable on mobile devices (phone, Tablet, etc.).
   - Identity protection for victims and suspected offenders.
   - Provides statistics of reported cases in the country.
   - Others (Please specify)

Appendix III: System Functionality Evaluation form for Reporters

System Functionality Evaluation form - Reporter	Yes	No
Ease of use		
Ability to report anonymously		
Ease of attaching evidence		
Identity protection for victims and suspected offenders		
Usable on mobile devices (phone, tablet, etc.)		
Provides statistics of reported cases in the country		

Appendix IV: Research Ethical Approval

Strathmore UNIVERSITY

13th August 2021

Ms Maingi Eunice,
eunice.maingi@strathmore.edu

Dear Ms Maingi,

RE: A National System for Reporting and Keeping Record of Child Online Offences and Offenders

This is to inform you that SU-IERC has reviewed and **approved** your above **SU-master's** research proposal. Your application reference number is **SU-IERC1098/21.** The approval period is **13th August 2021 to 12th August 2022.**

This approval is subject to compliance with the following requirements:

i. Only approved documents including (informed consents, study instruments, MTA) will be used
ii. All changes including (amendments, deviations, and violations) are submitted for review and approval by SU-IERC.
iii. Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to SU-IERC within 48 hours of notification
iv. Any changes, anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to SU-IERC within 48 hours
v. Clearance for export of biological specimens must be obtained from relevant institutions.
vi. Submission of a request for renewal of approval at least 60 days prior to expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days upon completion of the study to SU-IERC.

Prior to commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology, and Innovation (NACOSTI) https://research-portal.nacosti.go.ke/ and obtain other clearances needed.

Yours sincerely,

for: Dr Virginia Gichuru,
Secretary; SU-IERC

STRATHMORE UNIVERSITY INSTITUTIONAL ETHICS REVIEW COMMITTEE (SU-IERC)
13 Aug 2021
TEL: +254 (0)70303400
P.O BOX 59857-00200
NAIROBI-KENYA

Cc: Prof Fred Were,
Chairperson; SU-IERC

Ole Sangale Rd, Madaraka Estate. PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034000
Email admissions@strathmore.edu www.strathmore.edu

Appendix V: Similarity Check Report

Similarity report summary

Ouriginal by Turnitin

Document Information

Analyzed document	A System for Reporting Online Child Abuse and Offenders -122719.pdf (D143013243)
Submitted	8/17/2022 4:10:00 PM
Submitted by	
Submitter email	eunice.maingi@strathmore.edu
Similarity	4%
Analysis address	library.strath@analysis.urkund.com