CHILD ONLINE PROTECTION NATIONAL STRATEGY FRAMEWORK FOR THE REPUBLIC OF SUDAN

DECEMBER 2016

CONTENTS

"Online risks and illicit content are concepts that are increasingly common in Sudan as the usage of ICTs and the Internet increases. As the ICT sector landscape evolves, we have seen the migration of traditional voice revenue to data services which are being driven by the rise of social media and other broadband services; criminal and unethical activities are also shifting online. Children may be exposed to these vices at early an early age and this poses a great danger, in that Sudan's cultural values and identity in this information society are at risk of erosion.

The Republic of Sudan is therefore taking steps to develop collaboration with international stakeholders to build capacity and learn international best practices on Child Online Protection (COP). The establishment of a coherent National Child Online Protection strategy and awareness programme to protect both child and adults from online vulnerabilities will take into account the role of different stakeholders and existing initiatives within Sudan."

ACKNOWLEDGEMENTS

This framework has been developed and prepared with the support of the International Telecommunication Union, the guidance of the Sudanese National Telecommunications Corporation, and the assistance of the following contributing authors and experts (listed in descending alphabetical order):

• Yomna Omran (MCIT, Egypt)

• Rouda Alamir Ali (ITU)

• Amelia Gowa (ITU consultant)

We wish to thank the contributing support team, authors, experts and the workshop participants for their time, enthusiasm, insight and dedication to this exercise.

GLOSSARY

Constituents	agencies/community to which the activities in the strategy framework are directed
Stakeholders	agencies/bodies that are directly involved in strategy
COP	Child Online Protection
CRC	Convention on the Rights of the Child
ECPAT	End Child Prostitution, Pornography and Trafficking of children for sexual purposes
GCA	Global Cybersecurity Agenda
GSMA	GSM Association
ICMEC	International Centre for Missing and Exploited Children
ICT	Information and Communication Technology
ICSE DB	International Child Sexual Exploitation image database
ITU	International Telecommunication Union
IWF	Internet Watch Foundation
MCIT	Ministry of Communications and Information Technology
TPRA	Telecommunications and Post Regulation Authority

UNICEF	United Nations Children's Fund
UNODC	United Nations Office on Drugs and Crime

EXECUTIVE SUMMARY

In order to develop a comprehensive strategy based on local empirical data, TPRA, under the guidance of the ITU, undertook a local assessment amongst stakeholders in Sudan. The intent of the local assessment was to ascertain the level of exposure, awareness and available mitigation measures currently in existence within Sudan.

The purpose of the local assessment would ideally be to serve as a point of reference in assessing the usage patterns of ICTs and the potential risks especially amongst children within the country, and inform more insightful recommendations and action items to form the strategy.

In order to address the issues posed by exploitation of children on the Internet, TPRA with the support of the ITU organised a Child Online Protection (COP) National Strategy Workshop with a primary objective to develop a sustainable Action Plan to be implemented in the country, subject to revision, amendment and redeployment after a certain period of time as stipulated in a consensus by the stakeholders.

Following the COP Strategy Framework Workshop, national stakeholders will work to consolidate existing initiatives through execution of specialised action plans pledged by each entity, and conduct meetings to further follow-up on said actions.

As a preamble, this report provides a current state assessment in the Republic of Sudan, based on the information given by the stakeholders:

- TPRATelecommunications and Post Regulation Authority (TPRA)
- National Information Center (NIC)
- Prosecutor of Criminal Investigations (Ministry of Justice)
- Prosecutor of Family and Child Protection (Ministry of Justice)

- National Council for Child Welfare (NCCW)
- Ministry of Education (Management of educational planning and management of student activity management training)
- Family and Child Protection Unit (Ministry of Interior)
- E-Crime Police (Ministry of Interior)
- Sudan National Broadcasting Corporation (SNBC)
- Sudanese Coalition for Education for All (SCEFA)
- Journalists for Children Society
- Center for Civil Society Studies (MDA)
- Non-Governmental Organization and Society in Sudan (NGO)
- Telecommunication Operators (Zain, MTN, Canar, and Sudatel)
- Sudan University for Science and Technology (SUST)
- El-Ahfad University for Women Education

The stakeholders widely acknowledged that there should be actions to promote child safety online at the national level, taking into consideration the main shortcomings at the national level and the developments at the international level. Therefore, the Strategy Framework and hence the Action Plan developed is based on the five work areas (pillars) of the Child Online Protection initiative i.e. Legal Measures, Technical and Procedural Measures, Capacity Building, Organisational Structures and International Cooperation.

*full list of stakeholders to be provided by TPRA to include any other representatives that are not on the above list.

Part 1 – CURRENT STATE ASSESSMENT

Sudan adopted the ITU Initiative on the Child Online Protection (COP) within the Global Cybersecurity Agenda (GCA) framework. The National Committee for Child Online Protection was established by an administrative decree issued by Her Excellency Dr. Tahni Abddal, Minister of the Information and Communication Technology. TPRA – its role dating back to 2012 - has committed itself to a comprehensive approach, and plays an executive role in this committee along with other members from relevant government authorities, the private sector and NGOs to form an advisory group to facilitate the planning of programs and projects related to the initiative.The first meeting held at the TPRA Tower in December 2015, following which a committee meeting to formulate an action plan was incorporated in April 2016. The main areas as outlined in the brief that sought to be addressed include:

Exchange of information between the members engaged in the field of COP to inform the adequate planning of future phases.

Enhance constant communication between the stakeholders on the latest facts, information, and trends that will contribute to the implementation of programs for the protection of children in Sudan from the dangers of the Internet.

Conduct studies, questionnaires and surveys to identify the risks and trends.

Develop general guidelines and identify the appropriate channels to disseminate the information.

Follow up with best practice by attending conferences and seminars held at local or international levels in order to raise awareness, ways to combat cybercrime, and contribute to these forums.

Planning for positive alternatives of protection whilst using ICTs and prevention of abuse of the same, and the dissemination of the culture of community.

The general framework for COP in Sudan includes many mechanisms, strategies, policies, plans and programs. We found that many national mechanisms for the protection of childhood in Sudan and many different institutions whose functions and responsibilities are to fulfill the rights of the child, each in its field in terms of nature of work, powers and competencies. There are various institutions working in the field of legislation and ratification of international and regional instruments and their compatibility with national laws. There are also institutions working to monitor the implementation of laws on children and other direct intervention to protect the rights of children from violations and the most important mechanisms are: national Council for Child Welfare, Child Courts, Child Prosecutions, Family and Child Protection Police, Human Rights Commission, Advisory Council for Human Rights, National Commission on International and Humanitarian Law, Unit for Combating Violence against Women and Children, Office of Disarmament, Demobilization and Reintegration The National Council for Persons with Disabilities, the Cyber Crime Prosecution, the Telecommunication and Post Regulatory Authority (TPRA) and related government institutions.

Complaints and reporting of violations:

1. **Child Support Line 9696**

The child or any member of his/her family or any member of the community may file a complaint if there is any violation of the rights of the child. Article 84/1 of the Children's Act provides that any person with reasonable cause to believe that there is a loss of the rights of any child may inform the nearest official authority.

Regarding the means of reporting violations, the law states in Article 85 that a Hotline or any other means of communication shall be established under this Law to receive communications, claims and complaints for any violation of any of the rights of the child, and the Family and Child Protection Police should establish a center to receive communications and coordinate with the concerned authorities for interventionThe Family and Child Protection Police Hotline (6969) Free Toll - was established in 2009 to receive complaints. The Family and Child Protection Department of the State of Khartoum seeks to upgrade and develop the line to provide

the best services for children. The telephone line is available 24 hours a day, The line responds to all cases of violence, neglect and abuse against children

The number of calls received by Child Support Line 9696 in 2015 was (4483).

2. **Center of complaints and inquiries (5050) in (TPRA)**

The Center receives inquiries and complaints from all over Sudan on the short number 5050, reported to the regulatory body of communications in Sudan (TPRA)

Complaints that are received by the Center include: (Failure to activate the service or its disconnecting by mistake - misleading advertising - fraud messages - complaints of inconvenience - complaints of information networks and social networks - cyber bullying - pornographic content on the Internet - cybercrime - extortion - Impersonate - Scandal - SMS complaints - account theft) and in 2017, the Center received 3503 calls and in 2018 the number of 614 calls to 1/5/2018.

Statistics of Internet Complaints Facts:The Sudan CERT dealt with 624 cyber crime incident such as: (Email scam - Evidence expert – Forensics – Fraud - Illegal Information – Impersonate - Impersonate:: Facebook – Junk – Malware – Offense – Phishing – Scandal through:(YouTube/Email and Facebook) – Spy - Technical consulting - Theft crimes Threat - Violation of privacy - WhatsApp Cases – filtering – information – media - web defacement) during the year 2017

On the other hand direct complain could be reported to (TPRA) through the following methods:

1. Telephone: +2491871711442. E-mail: complaint@tpra.gov.sd – filtering@tpra.gov.sd – contact@cert.gov.sd

3. Via post box 2869

In order to achieve the strategy of COP, the Telecommunication and Post Regulatory Authority(TPRA) has mobilized the child protection partners in Sudan from the government institutions, the private sector and civil society organizations to work

together to implement the initiative program in accordance with the directives of ITU. The first meeting of the partners of the Child Protection Initiative was held in December 2015 and the meetings continued periodically to reach a clear vision in this regards.

This initiative works to protect children from the risks of the Internet and to raise awareness of the positive side of Internet use, as well as the exchange of information among the members of the initiative in the area of child protection on the Internet and planning future stages, as well as conducting studies and planning positive alternatives. **COP initiative sub-committees:**

Further, the Sudan COP initiative comprises of sub-committees namely: Legal measures, Education and capacity building, Media, Research and studies, and Technical and procedural measures. Each sub-committee maintains a list of action items to be fulfilled under the guidance and support of the relevant agencies within the main committee. Aside from Research and studies, and Education and capacity building, the rest of the sub-committees exhibit considerable progress in execution of their action items. Listed below are the accomplishments of the afore-mentioned sub-committees.

1. Legal measures

1.1Current situation:

1. Created integrated legal system to combat against the online crimes related to the children.
2. E-crime law 2007 version has been updated with new article (to indicate a clear article against online children abuse).
3. The new version of E-crime Law for 2016 currently addresses many acts relating to the protection of children online and Electronic Crimes.
4. Raised legal awareness amongst policy makers.

Developed specialized training programs for law enforcement agencies.**1.2 Situation analysis:**

Framework for the Protection of Children from Violence:

Sudan is one of the first countries to ratify the International Convention on the Rights of the Child in 1990 and without reservations to any article. It also ratified the additional protocols in 2004 (Optional Protocol to the Convention on the Rights of the Child on child trafficking, child prostitution, child pornography and the Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflicts). It also ratified the African Charter on the Rights and Welfare of the Child in 2007.

Article 27 (3) of the Interim Constitution of 2005 states that all rights and freedoms enshrined in the international human rights conventions, covenants and agreements ratified by the Republic of the Sudan are an integral part of this document.

The enactment of the Children's Act 2010 is a major achievement in the field of children's rights in Sudan. It is one of the most important legislation that deals mainly with the treatment and organization of child protection and welfare in Sudan. It also came in line with the Convention on the Rights of the Child and the other international obligations and covenants of Sudan relating to children's issues. Article 5 (1) of the Constitution states that the provisions of this law shall be guided by the principles and provisions of the Transitional Constitution of the Republic of Sudan of 2005 and the ratified international conventions and protocols, as stated in Article 5 (2) This law guarantees the protection of children from all forms and types of violence, harm, inhuman physical ,moral, and sexual mistreatment, neglect or exploitation).

Chapter 9 of the Children's Law is intended to prohibit the exploitation of children in prostitution, pornography and forced labor. Article 45 states that the perpetrator of the crime is a person who:

(A) abducts, sells or transfers a member or members of any child
(B) Rapes, harasses or sexually abuses any child.
(C) Produces, distributes, publishes, imports, exports, displays, sells or possesses any child pornography
(D) Uses any child for the purpose of sexual activities for reward or any form of remuneration,
(E) Encourages or depicts by any means any child exercising a real practice or simulating explicit sexual activities or depicting sexual organs of any child to satisfy sexual desire.

The Child Act has introduced deterrent penalties for a number of violations of violence against children. Article (86) provides that any person who violates the provisions of:

(F) Article 45 (a) shall be punishable by death or imprisonment for a term not exceeding twenty years with a fine.
(G) Article 45 (b) shall be punishable by death or imprisonment for a term of twenty years with a fine.
(H) Articles 45 (c), (d), (e), (f) and 46 (1) shall be punishable by imprisonment not exceed fifteen years' and a fine.
(I) Article 46 (2) shall be punishable by imprisonment for a term not exceeding twenty years and a fine.
(J) Articles 45 and 46 In addition to imprisonment and fines, seizure and confiscation of property such as those used to commit or facilitate the committing of the crime and the closure of buildings used in the committing of such offenses. The Court may allocate a portion of the fine to the affected as compensation

Article 33 of the Child Act bans the publication, display, circulation, photocopying, or possession of any visual or audiovisual works or works of art related to the child, addressing his /her instincts or make attractive his behavior contrary to the values and traditions of society. Which would encourage him/ to delinquency. The law also regulates the viewing of shows according to the provisions of Article 34 (1) It is strictly forbidden for children to enter cinemas, watch clubs and other entertainment places during the school day, and their entry is prohibited only with their parents or those who raise them (2) The regulations shall determine the organization of monitoring performances for children in cinemas, viewing clubs and public places, and the responsibility of the directors and supervisors of such places and the establishment of such performances and officials responsible for public input , and the irregularities imposed on the violators of those responsible. In addition to its text on the declaration of prohibited offers as states in Article (35), directors of cinemas, viewing clubs and similar public places must advertise in a clear place, in both Arabic and English languages, and by all the means of advertising available on offers that children are prohibited from viewing.

With regard to the right of the child victim to rehabilitation and reintegration, the Child Act stipulates in article 47/1 that the Ministry must take appropriate measures to achieve physical and psychological rehabilitation and social reintegration of a child who is the victim of any form of neglect, exploitation, abuse or torture Or any form of cruel, inhuman or degrading treatment or punishment or armed conflict.(2) Reintegration and rehabilitation must be carried out in an environment that promotes the child's health, respect for him/herself and his/her dignity.

The Law of Literary and Artistic Works of 2001, which prohibits offensive material and states, according to Article 15, the prohibited works which may not be imported, entered, published, printed, circulated or dealt with in any of the following cases (violation of religious values or public morals, abuse of the beliefs, customs or religions, color , sex, to the glorification , preference of one sex over another, or the conflict with state policy and national security).

E crime Law incriminate (1) Whoever produces, prepares, sends, stores or promotes through the information network or a computer or the like, any content that is Indecent or inconsistent with public order or morality, shall be punished by imprisonment for a term not exceeding five years or by a fine or both. 2. Any person who provides or facilitates intentionally or negligently through the information network or a computer or the like to access content that is dishonest or inconsistent with public order or morality shall be punishable by imprisonment for a term not exceeding four years or by a fine or both. The law shall impose the penalty if the act is committed to an juvenile (3) If the act referred to in paragraphs (1) and (2) is referred to an juvenile punishable by imprisonment for a term not exceeding seven years or by a fine or both.

Any person, who creates, publishes or uses a website, a computer or the like to facilitate or promote programs or ideas inconsistent with public order or morality, Shall be punished by imprisonment for a term not exceeding three years or by a fine or both.

As part of the protection of children against all forms of violence, the State has prepared in 2011 the National Plan to address violence against children in order to establish and develop a comprehensive system for the protection of children against all forms of violence, which is consistent with and complementary to the various sectors working in the area of child protection.

In response to the comprehensive recommendations of the United Nations Secretary-General's Study on Violence against Children in the World in October 2006, in which one of its recommendations states that all States should develop a multifaceted and systematic framework to respond to violence against children integrated into national planning processes.

2. In the framework of the legislative development for the protection of children online, the Council of Ministers approved the draft law against the crime of informatics for the year 2018 This law was devoted a complete chapter of electronic crimes against children and works to keep abreast of the huge technological development in the field of communications and information technology and the emergence of modern crimes committed by programs And techniques. The provisions of Chapter VI on cybercrime against children and minors states that:(35) Any person who uses the information or communication network or any means of information or applications to threaten or intimidate any child, deception or minor to intentionally carry out or abstain from doing any act shall be punished by imprisonment for a term not exceeding six years or a fine.
3. (36) Any person who uses the information or communications network or any means of information or applications to produce, promote, distribute, obtain, display or sell any child pornography or any programs or ideas or inconsistent with public order or morality related to children, To imprisonment for a term not exceeding ten years and a fine.
4. (37) Any person who uses the information or communications network or any means of information and applications to kidnap or entice any child or minor to sell him/her, transfer or use any of its members for the purposes of paid or unpaid sexual activities or Forced labor, inciting to commit suicide or committing any crime shall be punishable by life imprisonment and a fine.
5. (38) Anyone who uses the information or communications network or any of the information or applications to promote child prostitution, adultery or child sodomy, or any obscene acts, or to display pictures, videos or any material for children in Indecent situations, or exposes children or minors to watch electronic or similar sites or applications containing pornographic, obscene or Indecent material, shall be punished by imprisonment for a term not exceeding ten years and with a fine.
6. 39(1) Any person who uses the information network or communications or any means of information or applications in the promotion of drugs, liquor, any intoxicating or other psychotropic substances, or explaining the way of using or manufacturing to children or minors shall be punished by imprisonment for a period not exceeding Ten years and a fine, and may be punished with flogging. 2) Anyone who creates or manages any site, page or application for the purpose of promoting, facilitating gambling or the playing gambling with children or minors, or facilitating that or inciting, others shall be liable to imprisonment for a term not exceeding two years and a flogging or fine.

1.3 Challenges within the laws :

- Absence of laws, regulations and rules governing the Internet cafes
- Absence of the necessary control mechanisms on Internet cafes in case of use by children
- Absence of a hotline to report cases of crimes against children on the Internet
- Absence of rules and controls for ownership of the SIM Cards (determining a specific age to own SIM's)
- How to treat children from addiction to Internet use delinquent children are hackers of important and sensitive websites
- The cyber bullying phenomenon in schools, homes and public places
- Absence of legal information about the safe use of the Internet, cybercrime

2 Media:

1. **2.1Current situation:**Prepared materials for safe use of technology and Internet.
2. Encouraged private sectors, civil society and the media to support the COP initiative.
3. Launched a channel on Social Media for purposes of sharing knowledge and experiences.
4. Involved all interested parties to create environment for open dialogue on the issues related to COP.
5. Coordinated with the Ministry of Education to raise awareness about child abuse via the Internet.

2.2 Challenges in the media:

1. Lack of budgets required to meet the expenditure on media production.
2. Lack of family interest in the culture of safe use of the Internet
3. How to create meaningful and attractive content for children about the dangers of the negative use of the Internet
4. Raising awareness of the family and the com

3. Technical and Procedural Measures:

3.1Current situation:

1. Established and approved the COP Initiative in Sudan since 2012.

2. Instituted Internet filtering system for safety of Sudanese community.
3. Developed a COP website.[1]
4. Launched awareness program and supporting publications.
5. Produced animation movies for children related to Internet safety, and broadcasted on TV channels and social networking sites.
6. Published an educational magazine containing illustrative animations.
7. Motivated the telecom operators to adopt technological solutions to protect children.
8. Encouraged the establishment of a hotline or email to facilitate reporting crimes against children and any type of child abuse.
9. Prepared for the COP workshop in collaboration with the ITU, engaged all stakeholders and interested parties.

3.2 Challenges in the framework of technical solutions

1. Knowing the age of the Internet Browser.
2. Balancing between privacy and safety.
3. Reducing the time of software or technical solutions.
4. Registering the connection SIM's with ID and stopping the random sale of SIM's.
5. Limiting the service of internet Shared Access for users.
6. Organizing free periods provided by telecommunications companies for the use of the Internet.

[1] www.cert.sd/cop

4 Research and studies:

4.1Current situation:

1. Study the the social impact of the Internet on Internet cafe users-MDA
2. A study on the impact of the Internet on youth-MDA
3. Study on the Children Internet Usage in Sudan –Sudan-CERT

4.2 Challenges in research and studies

4. Lack of funding for spending on research on the protection of children on the Internet, which is reflected negatively on the scarcity and lack of research in the field.
5. The difficulty of obtaining accurate information due to the use of traditional data collection methods.
6. Lack of qualified staff in the field of data collection in modern ways(e.g. focusing groups).
7. How to extract new knowledge into pre-existing data to determine the age of the Internet user.
8. How to formulate the integration process between the Research and Studies Committee and the other four subcommittees.
9. Studying the status of the preacher and the important segments of the society on the use of the Internet.

5.Educational & Capacity Building:

5.1Current situation:

1. To adopting a COP week to educate the community, individuals and encourage them to develop their skills in the field of safe use of the Internet for children.
2. Lunch a ToT program and workshop on the safe use of the Internet.
3. Prepare awareness courses and conferences in schools in cooperation with the Ministry of Education.
4. Conducting training courses for teachers in the Ministry of Education and the Federal Ministry of Health for all the states of Sudan on the ToT programTrain the Trainer Program (TOT) - Train E-crime police investigators., Prosecutors and Judges – school Teacher
5. Training of students in the Primary (3893) students in Khartoum State
6. Promote security awareness throughout the State Provide information related to Security
7. Training course for trainers (TOT) for teachers of Primary schools in different states of Sudan (number 50) at the Ministry of Education.
8. Publish Student Book for Internet Safety.
9. Publish Teacher Book for Internet Safety.

5.2 Challenges in Educational & Capacity Building

1. Include the methodology of safe and positive use of the Internet in educational curricula in all educational stages.
2. The proliferation of mobile phones among school students.
3. Lack of awareness of children in schools using the Internet safely.
4. Lack of enlightenment sessions of the law of e-crimes and dissemination among members of the community.
5. Weak capacity of social centers and other institutions to support, rehabilitate and reintegrate victims into society.
6. Lack of assessment and analysis of gaps in capacity building within institutions to measure awareness level.
7. Absence of guidance material on the protection of children on the Internet for people with disabilities (in the sign language for people with hearing disabilities and the program of vision for people with visual disabilities).
8. The weakness of the media ,religious and community leaders in COP.
9. Lack of interest in enlightening the technical community and industry actors in their role in COP.

The SWOT(Strength-Weakness-Opportunity –Threats) analysis:

Strength:

- ✓ A strong commitment from the National Telecommunications Cooperation to protect children online.
- ✓ The existence of effective national partners.
- ✓ The existence of local, regional and international experiences.
- ✓ A partnership between government agencies and civil society organizations.
- ✓ Cooperation with telecommunications companies to protect children online.
- ✓ The existence of a legal framework to protect children from violence.
- ✓ The existence of mechanisms and centers for reporting and complaints.
- ✓ The existence of a number of national experts in the field of child protection on the Internet.
- ✓ The existence of a number of civil society organizations working in the field.

Weaknesses

- Poor community supervision
- The lack of precise information about child victims of exploitation through the Internet
- Parliament has not yet passed the bill to combat cyber crimes (2018)
- Poor awareness of the society in general and among children in particular
- The weak capabilities of investigating the crimes of children exploitation through the Internet
- Easy access of children to SIM cards (sales are not limited to user's age)
- Poor dissemination of the culture of spreading the safe use of the Internet in schools

Opportunities

- Sudan's commitment to the international and regional conventions.
- The existence of the transitional constitution, which stipulates that any agreement ratified by the Sudan is an integral part of the Constitution.
- Membership of Sudan in many international and regional agencies and organizations.
- The existence of mechanisms to protect children from violence(s/p?).
- The existence of the Child Act 2010(s/p?).
- The existence of a sophisticated law to combat cybercrime.
- Opportunities for technical and material support.
- Establishment of a national committee for the protection of children online(s/p?).
- The existence of international and regional cooperation in the field of child protection on the Internet.

Threats

- Lack of funding for raising awareness.
- The grwoing number of pornographic sites and the growing phenomenon of pornography.

- Growing of the exploitation of children from abroad and the publishing of child pornography and sexuality internally.

The Strategic Vision:

Secure a safe use for children online so as to have a protective environment for children

General Objectives:

Develop legislations to protect children online

- Raising the awareness all segments of soceity for the children safe use of the Internet
- Development of filtering software and the creation of modern technical means to protect children online
- Integrating educational materials into the curriculum on the safe use of the Internet
- Capacity building of staff in the relevant bodies

Strengthening partnerships and sharing experiences locally, regionally and internationally

Conduct studies and research related to children's use of the Internet

Policies:

- Adopting a policy based on the best interests of children
- Coordination of efforts among concerned partners

- Development and innovation in technology to play a better role in protecting children online
- Seeking to raise the capacity of personnel in the field
- Review and reform laws

Areas of the Strategy

1. The of laws and legislation
2. The Media
3. The Technical and Procedural
4. The Research and studies
5. The Education and capacity building

1. The of laws and legislation

Programs and projects are developed in this area according to the following objectives:

- Develop a strong legislative framework to protect children on the Internet
- Strengthen child protection mechanisms on the Internet
- Building the capacity of the judiciary
- Harmonization of national laws and legislations with international conventions and agreements
- Strengthen child protection mechanisms on the Internet
- acceptance of electronic and cyber evidence in cybercrime for children
- Building the capacity of personnel in the relevant judicial bodies dealing with cybercrime against children
- Establish a hotline to report cases of children's cyber crimes.

- Setting age-related controls (using the national number) to access children online.
- Establish mechanisms to prevent delinquent children from hacking and sabotaging some websites.
- Dissemination of legal culture for the safe use of the Internet
- Creating an integrated legal system to combat child abuse cyber crimes
- Establishing systems, programs and mechanisms for regional and international cooperation in the fields of exchange of information, collection and preservation of evidence, arresting and extradition of suspects, and controlling international coordination and cooperation to combat cybercrime.
- Setting conditions for the license to open Internet cafes to enhance control of these cafes.
- Providing technical tools that assist law enforcement agencies in the analysis and detection the criminals.

2. Media

Programs and projects are set in this area according to the following objectives:

- ✓ Increase the information space in the multimedia that addresses the positive use of the Internet
- ✓ Creation of modern means to deliver an attractive and purposful information message
- ✓ Enlightening about the importance of legislation and laws that protect children from exposure to cybercrime
- ✓ creating media content that is attractive to the child
- ✓ Formation of a team of children as trainers responsible for Mass media and awareness by selecting a group of students and training them to become ambassadors of the safe Internet, using the National Child Parliament
- ✓ Utilizing Islamic preaching platforms in places of worship to raise awareness of the dangers of the negative use of the Internet
- ✓ Benefiting from sports, cultural and younth clubs local committees and various organizations
- ✓ Organizing discussions panel, awareness programs and community dialogues for parents (Design brochures - designed for this purpose)
- ✓ Promoting the child's right to access knowledge and encourging a culture of safe use of the Internet
- ✓ In addition to the previous awareness of methods (houses of worship - clubs etc ...) employ media through interactive programs and direct dialogues
- ✓ Organizing media platforms and hosting public figures to discuss the dangers of the negative use of the Internet
- ✓ Increase the program space that addresses the dangers of the negative use of the Internet through:

- Diversification of means of delivery of media messages
- Encouraging producers to produce targeted and favourble programs for children on the about positive internet use
- Organizing competitions and sponsoring talents

The Technical and Procedural

Programs and projects are developed in this area according to the following objectives:-

- ✓ The creation of modern technical means to block restricted websites and redirect them to a page with positive and secure content.
- ✓ Design and development of filtering softwares.
- ✓ Retain Internet access log files.
- ✓ Developing a system for the reliability of access to Internet services and linking it to the national number.
- ✓ Encouraging industrial initiatives private sector to create technical solutions for protection.
- ✓ Exchange of technical expertise and integration with systems developed regionally
- ✓ Encouraging industrial initiatives to create technical solutions for protection.
- ✓ Create groups on social networks that bring together children and educational psychologists for guidance and problem solving.
- ✓ Sponsor talent and encourage children and young people to create technical solutions that help in protection and security

esearch and studies:

Programs and projects are developed in this area according to the following objectives:

- ✓ Know the trends of children's use of the Internet (eg time spent online and sites visited to identify children's risks on the Internet)
- ✓ Know the position of parents to monitor the activities of their children online
- ✓ Studying the positive indicators of secure Internet patterns usage demonstrated by both parents and children
- ✓ Collect statistics on children's use of the internet in Sudan
- ✓ Evaluating the efficiency and effectiveness of blocking and filtering systems in Sudan
- ✓ Evaluating the effectiveness of training programs and awareness campaigns
- ✓ Study and compile best practices from other countries
- ✓ Training cadres on the use of modern methods of data collection through intensive training workshops
- ✓ Use of data mining techniques available in telecommunications companies to access new knowledge

- ✓ Coordinate with all subcommittees to determine each committee's problems and require studies or research

Education and capacity building

Programs and projects are developed in this area according to the following objectives:

- ✓ Incorporate the method of safe and positive use of the Internet in school curricula.
- ✓ Innovation attractive applications to satisfy the desires of children, so inventing modern techniques to block restricted sites and redirect the child's attention to the secure content
- ✓ Raising awareness of children in schools
- ✓ Capacity-building for various stakeholders
- ✓ Launch of the teacher training program in the method of safe and positive use of the Internet
- ✓ Preparing awareness sessions for children and conferences in schools in cooperation with the Ministry of Education.
- ✓ Establishment of an association (ICT) for teachers in schools to promote the issue of students protection online.
- ✓ The use of extra-curricular activities to raise awareness about the negative use of the Internet
- ✓ Training judges, prosecutors and police in child protection trends on the Internet and cybersecurity in general, including the use of digital evidence and mutual legal assistance
- ✓ Capacity-building of social centers and other relevant institutions in supporting, rehabilitating and reintegrating victims into society
- ✓ Provide internal and external training for child protection ambassadors online
- ✓ Evaluating and analyzing gaps in capacity building within each educational institution to measure the level of awareness
- ✓ Providing guidance materials on the protection of children on the Internet for people with disabilities (in the sign language for people with hearing impairments and the program of optics for people with visual disabilities)
- ✓ Building the capacity of the media and religious and community leaders in the protection of children online

Part 2 - THE FRAMEWORK

SECTION 1 – Organizational Structures - A Sound Research Base and Monitoring Framework

Good organisational structures need to be in place at national level in order to facilitate the development of Internet safety infrastructures. Overarching structures can be established in legislation and by governments but good structure, process, and collaboration is also essential at ground level where national agencies must work together to address online child abuse and children's needs. Here, research plays an essential role in informing framework development and evaluating the impact of new measures. Hiring professionals in the area can be expensive, but research can be built into the programmes in a way that measuring impact can be done within the right context, inexpensively. There might exist policy frameworks and programmes concerning the use of ICT's, but there should ideally be a specific focus or chapter on online child safety or, if it already exists, given a higher profile.

RECOMMENDATIONS

- Regular coordination of the main committee and sub-committees; procedures of the stakeholder groups should be transparent for better accountability.
- The capabilities of the reporting facilities should be enhanced to also collaborate with other relevant government agencies, law enforcement and industry; to include training and provision of protection for both adults and children reporting illegal content online.

- National online child victim support council with specific one-stop support centres within the different states of Sudan for child online victims could be established to include specialised personnel such as counsellors, child psychologists, rehabilitation officers, police officers (investigators, prosecutors) and legal advisors.
- Establish an ICT Teachers association for educators in schools to advance the issue of online child protection and productive use of ICTs as well as to enhance skills and competencies amongst ICT teachers and students.
- It is recommended to define strategies that focus on vulnerable children who are outside the regular school system or identified as being disadvantaged/special needs.
- It is recommended to continue to carry out ICT surveys and related studies to gauge the level of awareness and preparedness to mitigate risks to children online.

ACTION PLAN

- Create Terms of Reference for the committee and sub-committees.
- Periodic research and data collection has to be carried out to determine trends, positive and negative experiences, and significant changes within the landscape of the country. Categorical emphasis should be given to contemporary Internet access points i.e. hotspots, cybercafés, community centers, libraries, school ICT clubs and post offices. Possible topics could include:
    - Online usage trends of children (e.g. time spent online, websites visited, popular games played, programs engaged)
    - Online risks faced (from the viewpoint of the children themselves)
    - Attitude of parents towards monitoring their children's activities online

- Study the positive indicators of Internet security patterns exhibited by both children and parents
- Collect statistics on the children Internet usage in Sudan
- Evaluate the efficiency and effectiveness of blocking and filtering systems in Sudan
- Evaluate the effectiveness of training programs and awareness campaigns
- Study and compilation of best practices from other countries

- To create a roadmap for training and capacity building programmes for various stakeholders e.g.:
  - All levels of law enforcement officers (strategic, operational and tactical): to train police officers and build investigative capacity
  - Magistrates and judges: trends of child online protection and cybersecurity in general including use of digital evidence and mutual legal assistance.
  - Teachers, parents, counsellors and care-givers: building capacity to deal with trends, threats, risks and issues that children face online.
  - Social centers, victim support units and other institutions involved in victim support, rehabilitation and reintegration.
  - The technical community, industry players and media on their roles in advocating and promoting the rights of children online.

SECTION 2 – Capacity Building - Raising Awareness

The term capacity building has been used in wide variety of contexts. In the context of this document, it refers to the need to capitalise, build upon and enhance existing skills and knowledge through the provision of useful information regarding sources, research, training and possible funding sources to enable the development of local child Internet safety development programs.

An effective awareness raising strategy has to be based upon robust research which provides a clear understanding of what children and young people are doing online and the risks that they face. Moreover, an effective awareness raising campaign should take into account the local cultural situation and use a variety of means to reach target audiences. It should empower and educate and is an essential tool in capacity building.

RECOMMENDATIONS

- Each stakeholder should have a child protection policy.
- Develop age-appropriate programmes for different target groups, including vulnerable and disadvantaged groups.
- Conduct assessments and gap analysis of the capacity building within each educational institution to gauge level of awareness and preparedness to pass on the required values to students.
- Religious leaders to participate in online safety awareness drives and campaigns. Definitions of harmful content to be included in sensitization of the religious groups. Develop critical skills for young people using the religious groups.
- To provide guidance on online safety principles for vulnerable and marginalized groups and people with special needs, in collaboration with NGOs.

- Integrate ICT safety programs with national, regional and internationally recognized days to create more involvement and awareness. Create a social calendar on relevant days.
- Promote positive content for better empowerment of children and parents on the Internet through various available channels.
- It is also recommended to continue to raise the awareness of public authorities and policy on the topic of child online protection.

ACTION PLAN

- To integrate positive and safe use of the Internet within the educational curriculum classroom.
- To adopt a COP week to educate the community, individuals and encourage them to develop their skills in the field of safe use of the Internet for children.
- Launch a Train the Trainers program and workshop for teachers on the safe use of the Internet.
- Prepare awareness courses and conferences in schools in cooperation with the Ministry of Education.Develop updated training programs for children:
    - Children in primary schools;
    - Children in secondary schools;
    - Youth in informal education system;
    - Youth that are not connected to neither formal nor informal education system;
    - Children in remote areas;
    - Children in private schools; and
    - Children in semi-private schools.

An ambassador program could be launched within these groups as an incentive for the children, to keep them more engaged.

- Set up training and awareness sessions for parents.
- Launch training programs amongst Religious institutions.
- Provide technical training to the key members of civil society to include training the trainer toolkits, guidelines and material on online safety. The guidelines and material will:
    - Include an index or glossary of common terms and trends;
    - Be translated into Arabic.
- Establish focus groups amongst different age and target groups to test pilot awareness campaign programs.
- Develop a comprehensive capacity building program and plan to deliver relevant COP awareness, sensitization and operational information to policy makers from multiple ministries, government agencies and other organizations. This should cover strategic, operational and tactical roles that will be required for implementation.

SECTION 3 – Legal Measures

A strong and comprehensive child protection legislative framework is an essential component of any national framework addressing Internet safety. Although the focus is upon online protection, a good and reasonable approach would be the introduction of new complementing provisions to already existing legislation.

RECOMMENDATIONS

- Bring to the attention of policy makers and all stakeholders that child abuse in the online environment is not only related to child pornography/ child sexual abuse material, but also other aspects, namely: data protection and privacy of minors, use of commercial services online, online advertising targeting minors, juvenile liability, victims' assistance, liability of adults and guardians, safeguard of minors from being prosecuted, etc.
- Harmonize the national provisions to the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography and Budapest standards.
- Include other forms of sexual exploitation such as grooming, virtual pornography, live streaming, cyberbullying, stalking, sex tourism, along with their proper definitions.
- Ensure proper procedures to attend a child when he/she is a perpetrator in the form of psychiatric expertise, special police proceedings, and special court proceedings.
- Harmonize law so that extradition is allowed, and eliminate double criminality.
- Curriculum to include segment on knowledge of legal structures and regulations.

ACTION PLAN

- Propose a new regulation for the Internet Cafe license, and impose fines on violators.
- Ensure that child online offenders and victims are included in the police child diversion chart.
- Establish mechanisms to make further assessments of the legal and policy situation at national level with regard of all aspects of child abuse online.
- The assessment should contain analytical analysis and take into account regional instruments and initiatives in order to propose harmonised amendments to the existing legislation in respect of human rights and fundamental CRC principles.

SECTION 4 – International Cooperation and Implementation

A collaborative approach aimed at building consensus at the global level shall be part of any legal framework for protecting children in cyberspace. Given the international nature of cybercrime and of child exploitation, the COP strategy recognises that online child abuse is a global crime that requires international collaboration.

Global commitments have been made to protect children in the online and offline environments. A high level international cooperation and data sharing, therefore, is a fundamental step to be taken in this collaborative approach. The benefits are clear: a cooperation network allows countries to exchange and receive updated information in a mutual advantageous relation.

International law enforcement in the child Internet abuse area has developed considerably in recent years but barriers to effectiveness include the preponderance of a small number of well-resourced policing units in industrialised countries leading the way and considerable differences in domestic law. Essential international law enforcement is essential in combating Internet child abuse given the global nature of the offending behaviour and good international links should be established at local level.

Sudan International and Regional Relations current status:

Sudan is an active member of international and regional organizations and unions, for example, the International Telecommunication Union (ITU) , the Arab Organization for Communications and Information Technology (AICTO), the African Telecommunications Union (ATU) and is a permanent member of the Permanent Arab Communications Committee.

Sudan-CERT is a member of a number of organizations including OIC-CERT and Africa-CERT, among other CERTs committees. It also has signed several memorandums of understanding (MOU) with a number of friendly countries. There is a multilateral international partnership to address cyber threats (Empact provides emergency response resources to facilitate identification of threats and exchange of resources to assist member states).

RECOMMENDATIONS

- Further build synergies with international actors, such as COP Partners, to learn from best practices and receive guidance from international stakeholders.
- In coordination with COP partners, establish a series of regional and global gatherings related to COP to allow for collaboration and exchange of knowledge and national 'trends and experiences'. The benefit of gathering with countries with similar cultural values is to allow for open dialogue.

- Collaborative strategies with relevant private sector stakeholders and civil society for purposes of capacity building, assistance in updating initiatives, resource acquisition, research and data collection.
- Establish regional and international coordination for research purposes e.g. regional and international academia bodies.

ACTION PLAN

- Develop an international partnership framework for strategic, operational and tactical enforcement of the COP strategy that will be beneficial to the Republic of Sudan.
- To establish collaboration with regional and international academia for research purposes and resource acquisition. Begin with regional universities, and build up to international ones.
- Share regional case studies with the national law enforcement agencies to demonstrate the procedures and practices across stakeholders and interagency cooperation so that practical methods can be discussed and possibly incorporated into the framework. Additionally, highlight and categorise online issues that have translated to offline situations.

- Identify and prioritize high level champions to ensure accountability.

Examples of collaboration strategies:

- IWF: to improve the capability and functionality of reporting of illegal content in Sudan. Different activities that could be carried out to this effect would include an analysis of existing infrastructure, training on general functions and codes of practice especially regarding how the information is collected and processed in accordance with the legal structures.
- Interpol: is the lead international police agency for combating online crimes against children. They are pivotal in terms of spreading awareness, best practices, enabling and facilitating the sharing of information between police forces worldwide.Sudan would benefit from co-operation with the International Child Sexual Exploitation image database, managed by Interpol (ICSE DB). This constitutes a powerful intelligence and investigative tool that allows specialized investigations to share data internationally with police forces.
- ECPAT: capacity building initiatives on the impact of Internet cafes on the youth community, legal structures on child prostitution, pornography and trafficking.
- GSMA: research engagement on how young people use and benefit from mobile technology; supporting mobile operators in developing proactive measures to protect children; Mobile Alliance against Child Sexual Abuse Content - a voluntary initiative to fight illegal child abuse content.
- Insafe: incorporation of Safer Internet Day into national awareness campaigns and roadmap.
- ICMEC: capacity building for law enforcement and introduction to the chapters and working mechanisms of the Financial Coalitions against Child Pornography.
- UNODC: capacity building for law makers and law enforcement.

- UNICEF: research and capacity building to enhance understanding of children's use of ICTs, risk opportunities, gaps and challenges. (This could be coordinated with the UNICEF regional office in the Arab region.)

**this list is not in any way definitive or conclusive to all possible areas of engagement with international partners and experts.

SECTION 5 – Technical and Procedural Measures - Working with Industry

The act of "going online" means that technology is being used. Whether accessing the Internet, communicating with a friend using social media technology is involved and this means that a certain amount of protection can be provided by default. This can be put in place on behalf of the users and it is possible to prevent the user from removing some of the protection.

All stakeholders have a key role to play here. Industry can develop sophisticated controls which are easy for the end user to implement, regulatory bodies can insist that certain safeguards are in place, particularly for younger users, but ultimately, someone needs to check that they are being used effectively.

National governments clearly have a role to play and will be able to regulate for specifics which recognise the cultural identity of their country, but the other bodies such as the European Commission and the United Nations also take a lead in developing policies and recommendations for good practice.

The parents have a role to play and parental controls are another approach to technical measures that can be implemented.

RECOMMENDATIONS

- It is important to deliver trainings for government agencies, law enforcement, civil society and educators to establish relevant technical expertise.
- Encourage further technical research, multi-sectorial engagements.
- Encourage innovation and development with specific focus on the following:

- Child participation
- Academia involvement
- Industry initiatives

ACTION PLAN

- Relevant government agencies and industry to encourage creative and impactful innovations from the public on finding more technical solutions for COP.
- Organize technical champions and run technical workshops on topics like e-commerce and related fraud.
- Establish clear reporting structures (CERT, hotline, helplines, education authorities)
- A clear deployment or compliance plan to be provided with regards to Internet cafes, operators and all upstream providers.

Child Online Protection Strategy

work plan

2018-2020

Child Protection Strategy Online work plan 2018-2020													
Areas	**Objectives**	**Main Interventions**	**Time period**										
			2018				**2019**				**2020**		
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
	1.Develop a strong legislative framework to protect children online	1.1 Holding consultative sessions on ESCWA study												
		1.2 Follow-up of the law of combating the crimes of informatics for the year 2018												
		1.3 Prepare and approve a new rule to regulate the license of Internet cafes to enhance the control of these cafes												

Laws and legislations		1.4 Adopting the means that lead to the acceptance of electronic evidence in the cyber crime of children												
		1.4 Work to include delinquent and victims children on the Internet in the Family and Child Protection Unit -Ministry of Interior												
	2.Strengthening child protection mechanisms on the Internet	2.1 Develop and increase the hotline capacity of **9696**												
		2.2 Increase the number of branches of the units , prosecutors and child courts in the states of Sudan												
		2.3 Provide necessary support to family and child protection units												
	3. Building the capacity of the judiciary.	3.1 Provision and adoption of an forensic evidence lab												
		3.2 Special training sessions for judges, prosecutors and the police on all matters related to												

		information crime against children and ways of protecting them on the Internet												
		3.3 Building the capacity of the relevant judicial bodies in dealing with cybercrime against children												
		3.4 Develop the capacity of law enforcement agencies to analyze and detect the criminals.												
		3.5 Providing opportunities for participation and external training and sharing experiences in the field of cybercrime												
	4. Disseminate legal culture for the safe use of the Internet	4.1 Providing legal information on the safe use of the Internet, cybercrime and peer to peer cybercrime												
		4.2 Issuing monthly reports on child cyber crimes												
	1.Raise awareness of	1.1 Design a meaningful and attractive slogan for the strategy of protecting children online												

Mass Media	the safe use of the Internet for children	1.2 To form a team of children of the Child Parliament and train them to become ambassadors for the safe use of Internet and work in awareness raising												
		1.3 Holding seminars, lectures and family dialogues on the safe use of the Internet and its effects												
		1.4 Encourage and motivate students of the Universities to create attractive and targeted messages to protect children online												
		1.5 Production of creative messages and short films to raise awareness through social media and various media												
		1.6 Establish intensive media campaigns to define the numbers **9696** and **5050**												
	2.Increasing awareness of child protection	2.1 Issuing weekly messages in a newspaper and increasing the number of media programs dealing with the risks of the negative use of the internet												

	online	2.2 Preparation of competitions for media awards for the best programs to educate children on ways on the safe use of the internet.												
		2.3 Sponsoring for attractive mass media programs and introducing awareness spaces for child protection on the Internet												
		2.4 Adopt a week to educate the local community in protecting children from internet risks												
	1. Encourage initiatives to create technical solutions to protect children online	1.1 Announcement of competitions to promote innovation in child protection technology on the Internet with a focus on child participation, academic participation and industrial initiatives												
		1.2. Develop child-specific communication SIMs' and age-related controls for children's access to the calling SIM's and for children's access to the Internet												

Technical Solutions		1.3. Establish a mechanism to determine the extent of child pornography and its harmful impacts on children's behavior												
		1.4Establish groups on social networks that bring together children and educational psychologists for guidance and problem solving												
		1.5 Save log files to the Internet and create a monthly archive of all logins for Internet sites												
		1.6 Provide huge storage capacity and a periodic archiving system for ISPs												
		1.7 Exchange of technical expertise and integration with systems developed regionally and internationally												
	2. Design and development of filtering software.	2.1 Open channels of communication with software companies												
		2.2 Follow-up development and updating of the systems of filtering websites to contribute to the protection of children from												

		abusive sites												
		2.3 Modify the page blocking and filtering websites and linking them to a number of sites with positive content												
	1 - The preparation of studies and theoretical and practical research on the cyber delinquency of children	1.1 Prepare a study on the delinquency of children and develop solutions based on information, results and outputs of these studies												
		1.2Prepare a study on trends of children's use of the Internet (eg time spent on the Internet, visited sites, popular games played, and programs to be involved)												
		1.3 Study positive indicators of Internet security patterns demonstrated by both children and parents												
	2. Conducting	2.1 Study the risks faced by children online (from the perspective of children themselves)												

Researches And studies	questionnaires and studies of the risks that children face on the Internet	2.2 Collection of statistics on children's use of the Internet in Sudan												
		2.3 Study and compile best practices from other countries												
	3. Evaluation of activities and programs	3.1 Evaluate the efficiency and effectiveness of blocking and filtering systems in Sudan												
		3.2 Evaluation of capacity-building and training programs												
		3.3 Evaluation of the mass media work and awareness campaigns												
Education and Capacity Building	1. Include a safe and positive use of the Internet in school curricula.	1.1 Preparation of a safe and positive use of the Internet in school curricula in cooperation with the Ministry of Education												
		1.2 Launch of the teacher training program												

	2. Raising awareness of children in schools	2.1 Preparation of awareness sessions for children and conferences in schools in cooperation with the Ministry of Education.												
		2.2 Establish an information and communication technology (ICT) association for teachers in schools to promote the issue of child protection on the Internet students.												
		2.3. To employ extracurricular activities to raise awareness about the positive use of the Internet												
		3.1 Evaluate and analyze gaps in capacity-building within each educational institution to measure the level of awareness and willingness to convey the values required for students												
		3.2 Training of judges, prosecutors and police in child protection trends on the Internet and cybersecurity in general, including												

	3. Capacity building for various stakeholders	the use of digital evidence and mutual legal assistance												
		3.3 Train teachers, parents and caregivers with trends, threats, risks and issues faced by children on the Internet												
		3.4 Capacity building Social centers and other relevant institutions in supporting, rehabilitating and reintegrating victims into society												
		3.5 Training of mass media and community leaders in advocating for the protection of children online												
		3.6 Train children in the safe use of the Internet												
		3.7 Enlighten the technical community and industry actors with their roles in promoting child protection on the Internet.												
		3.8 Provide internal and external training for child online protection ambassadors												

		3-9 training religious leaders to participate in awareness campaigns on the safe use of the Internet												
		3.10 Provide guidance materials for people with disabilities on the protection of children on the Internet (in the sign language for people with hearing impairments and the program of optics for people with visual disabilities)												
		3.11 Provide technical training to civil society organizations, including training of trainers and guidelines on Internet safety.												

ANNEX A

TERMS OF REFERENCE (TOR) FOR STAKEHOLDERS OF COP FRAMEWORK

NO	STAKEHOLDER	TERMS OF REFERENCE (TOR)
1.	Telecommunications and Post Regulation Authority (TPRA)	Which is responsible for the implementation of the strategy to follow through its various departments and coordination with the rest of the partners. The Department of Communication Services, which receives complaints (5050) and responsible for the filtering system, coordinating with the ISP's.
2.	Sudan-Cert	Increasing the security efficiency of the entities that use ICT and protect them from cybercrime. Provide advice to citizens and various agencies in information security before and after the occurrence of any E-crime or electronic incident, as well as tracking electronic criminals and hand the evidence to the judiciary.
3.	National Council for Child Welfare (NCCW)	To formulate policies, plans and programs related to childhood in the framework of the state policy and coordination with different levels of government in the field

		of child care and to raise awareness of children's issues and to devise ways and means to mobilize them to take initiatives to address the various issues of childhood.
4.	E-Crimes Police	Investigation of cases related to cybercrime as well as tracking electronic criminals and handing them to legal entity under existing laws.
5.	Family and Child Protection Unit (Ministry of Interior)	Conducting investigations into violations committed against children, providing social and psychological support, raising awareness, carrying out research and studies on the causes of violence and violations, and providing a telephone line for free assistance to children (9696) to respond immediately to complaints and communications on the one hand and solve some problems by telephone by providing advice and guidance by social workers.
6.	Prosecutor of Family and Child Protection (Ministry of Justice)	Supervise investigations into children's cases and charge for crimes committed against children or by them and initiate prosecution before children's courts.
7.	Court of Family and Child Protection (Ministry of Justice)	Consider the cases brought before it by the prosecution, the social service office or the caregivers with regard to child

		victims of violations and cases referred to them by children who are delinquent from other courts.
8.	Ministry of Education	Working with the National Center for Curriculum and Educational Research (Bakht al-Ruda) of the Ministry of Education to include the safe use of the Internet in curricula. And working with departments of different stages to raise awareness of the safe use of the Internet and the training of children and teachers.
9.	Prosecution of Information Crimes (Ministry of Justice)	Investigation of cases related to cybercrime.
10.	Ministry of Health	Coordinating with the Department of Women and Child Welfare and the units of medical services and psychological and social rehabilitation as well as the implementation of community awareness activities.
11.	Unit for combating violence against women and children	Coordinating and working to raise awareness and conduct research on the phenomenon of violence against women and children.

12.	Communication Companies	Exchange experiences and develop technical solutions to protect children online and provide financial and technical support.
13.	Sudan National Broadcasting Corporation (SNBC)	Campaigns and advocacy campaigns.
14.	Non-Governmental Organization and Society in Sudan (NGO)	Raising awareness, training and media work.
15.	Academic circles	Field of research, studies and training.
16.	Community and religious committees	Enlightenment and raising awareness.
17.	Children and ambassadors protect children online	Enlightenment and raising awareness.
18.	National Information Center	The Center is responsible for the national network of the state and the feild of information systems and standard programs and raising awareness of information to citizens. The center works in various axes such as infrastructure, applications, standards and promotion of the information industry. The

		Center also actively participates in the development of national strategies for the information industry.
19.	ISPs: Zain, MTN, Canar, Sudatel	Have community responsibilities built on the foundation of active participation and contribution to the welfare and benefits of our community. Their contributions reached various vital sectors including: Health, Education, Youth and Sport. In addition to filtering system in the framework of COP.

ANNEX B

DEFINITIONS OF KEY CONCEPTS OF COP

Introduction: This section provides a list of resources where definitions of key concepts on COP are available. It should be noted that: 1. Particular resources dedicated to COP concepts are hard to find, most resources identified are for cybersecurity concepts in general; 2. For some broadly defined concepts, such as "solicitation of children for sexual purposes" or "harmful online content", they appear in different forms amongst related concepts in various resources. For example, "harmful online content" in one glossary may appear in related concepts such as "inappropriate content, illegal content for children" in other glossaries.

Part I. The following links are that for some resources which include significant number of definitions of key concepts on COP

1. **USLegal.com**http://definitions.uslegal.com/c/child-online-protection-act/

USLegal.com is the legal destination site for consumers, small business, attorneys, corporations, and anyone interested in the law, or in need of legal information, products or services. It provides definitions of legal terms that appeared in the U.S. federal or state law.

2. **eSafe Glossary by Salford City Council, Salford City, UK** http://www.salford.gov.uk/d/salford-esafety-glossary-jan2012.pdf

3.**ThinkUknow program**http://www.thinkuknow.org.au/site/inappropriatecontent.asp

ThinkUKnow is an Internet safety program delivering interactive training to parents, care-givers and educators through schools and organizations across Australia, using a network of accredited trainers from its partner agencies.

4. **Parentsprotect**http://www.parentsprotect.co.uk/cyberbullying.htm

The Parentsprotect website contains information and resources which aim to raise awareness about child sexual abuse, answer questions and give adults the information, advice, support and facts that they need to help protect children.

5. **NetSmartz Workshop**http://www.netsmartz.org/Cyberbullying

NetSmartz Workshop is an interactive, educational program of the National Centre for Missing & Exploited Children (NCMEC) that provides age-appropriate resources to help teach children how to be safer on- and offline.

6. **Enough Is Enough**http://www.internetsafety101.org/glossaryofterms.htm

Enough Is Enough (EIE), a non-partisan, non-profit organization, emerged in 1994 as the national leader on the front lines to make the Internet safer for children and families. The link above is to their internet safety glossaries, which includes definitions of several COP concepts.

7. **Cybersmart Program**http://www.cybersmart.gov.au/glossary.aspx

Cybersmart is a national cybersafety and cybersecurity education program managed by the Australian Communications and Media Authority (ACMA), as part of the Australian Government's commitment to cybersafety. The link above is to their internet safety glossaries, which also includes various definitions of interest.

Part II. Definitions of key concepts on COP from different resources:

- ✓ **Child sexual abuse material:**

1. **Child sexual abuse material** consists of a recording, usually in still or video form, which depicts a child engaged in explicit sexual activity.UNODC Study on the Effects of ICTs on the Abuse and Exploitation of Children
2. Offences relating to the production, sale and possession of child pornography (generally described as **child abuse material**) are contained in the Classification of Computer Games and Images Act 1995 Criminal Code (Child Pornography and Abuse) Amendment Bill 2004, State of Queensland, Australia.

3. **Child abuse material**means material that depicts or describes, in a way that reasonable persons would regard as being, in all the circumstances, offensive: (a) a person who is, appears to be or is implied to be, a child as a victim of torture, cruelty or physical abuse, or (b) a person who is, appears to be or is implied to be, a child engaged in or apparently engaged in a sexual pose or sexual activity (whether or not in the presence of other persons), or (c) a person who is, appears to be or is implied to be, a child in the presence of another person who is engaged or apparently engaged in a sexual pose or sexual activity, or (d) the private parts of a person who is, appears to be or is implied to be, a child. Crimes Amendment (Child Pornography and Abuse Material) Bill 2010 State of New South Wales, Australia.
4. **Child abuse images:** images of children reflecting abuse – sometimes incorrectly referred to as 'child pornography'. Salford City Council, Salford City, UK, eSafe Glossary

✓ **Cyber-enticement**

1. **Cyber-enticement** refers to the persuading, soliciting, coaxing, enticing, or luring by words, actions or through communication on the Internet or any electronic communication, any minor for the purpose of engaging in sexual conduct. UNODC Study on the Effects of ICTs on the Abuse and Exploitation of Children
2. **Child enticement** means conduct, or an attempt or conspiracy to commit such conduct, constituting criminal sexual abuse of a minor, sexual exploitation of a minor, abusive sexual contact of a minor, sexually explicit conduct with a minor, or any similar offense under federal or state law. Mass.gov, the Official Website of the Attorney General of the State of Massachusetts, USA
3. **Cyber-enticement** is child enticement through the use of the InternetIT Law Wiki.

4. **Child enticement** means an act or conduct, or an attempt or conspiracy to commit such conduct that would constitute a criminal sexual offense against a child under state or federal laws. USLegal.com

✓ **Solicitation of children for sexual purposes**

1. **Solicitation of children for sexual purposes** refers to an intentional proposal, through information and communication technologies, by an adult, to meet a child who has not reached the age of majority set in domestic law, for the purpose of committing sexual abuse or producing child pornography where this proposal has been followed by material acts leading to such a meeting**.** UNODC Study on the Effects of ICTs on the Abuse and Exploitation of Children

✓ **Grooming**

1. **Grooming** refers to a series of acts that facilitate cyber-enticement such as actions deliberately undertaken with the aim of befriending and establishing an emotional connection with a child, in order to lower the child's inhibitions in preparation for sexual activity with the child. UNODC Study on the Effects of ICTs on the Abuse and Exploitation of Children
2. **Grooming** is when a person tries to 'set up' and 'prepare' another person to be the victim of sexual abuse.NetSafe program, New Zealand
3. **Online grooming** is when an adult makes online contact with someone under the age of 16 with the intention of engaging in sexual abuse. ThinkUKnow program, Australia
4. **Grooming** is a word used to describe how people who want to sexually harm children and young people get close to them, and often their families, and gain their trust. Parentsprotect website, UK

5. **Grooming:** the actions undertaken by a paedophile to befriend and establish an emotional connection with a child, in order to lower the child's inhibitions in preparation for sexual abuse and/or rape. Paedophiles may initiate online conversations (e.g. in chat rooms) with likely victims to extract information about location, interests, hobbies and sexual experiences. Salford City Council, Salford City, UK, eSafe Glossary
6. **Child grooming** refers to an act of deliberately establishing an emotional connection with a child to prepare the child for child abuse. Child grooming is undertaken usually to carry out sexual abuse and other child exploitation like trafficking of children, child prostitution or the production of child pornography. Currently child grooming occur through the use of internet.USLegal.com
7. **Grooming:** Refers to the techniques sexual predators use to get to know and seduce their victims in preparation for sexual abuse. **Enough Is Enough (a child online protection NGO)**

✓ **Cyber-harassment**

1. **Cyber-harassment** commonly refers to the intimidation, repeated or otherwise, of one individual by another or by a group, perpetrated through or utilizing electronic means. UNODC Study on the Effects of ICTs on the Abuse and Exploitation of Children
2. **Cyber-harassment** refers to online harassment. Cyber harassment or bullying is the use of email, instant messaging, and derogatory websites to bully or otherwise harass an individual or group through personal attacks. Cyber harassment can be in the form of comments made in chat rooms, sending of offensive or cruel e-mails, or even harassing others by posting on blogs or social networking sites. Cyber harassment is often difficult to track as the person responsible for the acts of cyber harassment remains anonymous while threatening others online. This usually applies to school-age children. USlegal.com

✓ **Cyber-stalking**

1. **Cyber-stalking** is characterized by a repetitive aspect to the conduct and is often understood as a course of action that involves more than one incident perpetrated through or utilizing electronic means that causes distress, fear or alarm. UNODC Study on the Effects of ICTs on the Abuse and Exploitation of Children
2. **Cyber-stalking:** refers to the use of information and communication technology, particularly the internet, to harass an individual, group of individuals or organization. Salford City Council, Salford City, UK, eSafe Glossary
3. **Cyber-stalking** refers to the act of threatening, harassing, or annoying someone through multiple email messages with the intention of placing the recipient in fear that an illegal act or an injury will be inflicted on the recipient, his/her family or household. USlegal.com
4. **Cyber-stalking:** Methods individuals use to track, lure, or harass another person online. Enough Is Enough (a child online protection NGO)

✓ **Cyberbullying**

1. **Cyberbullying** is bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites. What makes cyberbullying different and possibly more dangerous/risky? Cyberbullying can happen 24/7. There is no cut-off when it comes to cyberbullying. A child can be cyberbullied day and night. It's hard to pinpoint or track who the bullies are. Being online offers bullies anonymity and they can post or share hurtful material without being worried about the consequences. Everything is permanent online. Hurtful content is hard to delete online as copies can be reproduced or uploaded.UNODC Study on the Effects of ICTs on the Abuse and Exploitation of Children

2. **Cyberbullying** is the use of information and communication technologies to support the deliberate, repeated and hostile behaviour, by an individual or group, which is intended to harm.

   ThinkUKnow program, Australia

3. **Cyberbullying** is just what it sounds like - bullying through Internet applications and technologies such as instant messaging (IM), social networking sites, and cell phones.

   NetSmartz Workshop

4. **Cyberbullying** refers to bullying over electronic media, usually through instant messaging and email. It may involve repeated harm threats, sexual remarks, and insulting speech. Cyber-bullies may publish personal contact information of victims and even assume their identity and publish material in their name for the purpose of defaming or ridiculing.

   Salford City Council, Salford City, UK, eSafe Glossary

5. **Cyberbullying** refers to any harassment that occurs via the internet, cell phones or other devices. Communication technology is used to intentionally harm others through hostile behaviour such as sending text messages and posting ugly comments on the internet.

   USlegal.com

6. **Cyberbullies/cyberbullying:** Wilful and repeated harm inflicted through the medium of electronic text, typically through e-mails or on websites (e.g., blogs, social networking sites).

   Enough Is Enough (a child online protection NGO)

✓ **Harmful online content**

1. **Harmful online content** is a very broad category that includes any online material that has the ability to negatively influence children. Examples include online pornography and especially sexual abuse material; violent video games; websites that espouse racial or ethnic hatred; and commercial sites that seek to swindle youth or steal their identities. UNODC Study on the Effects of ICTs on the Abuse and Exploitation of Children

2. **Inappropriate Content for Children:** In many ways the Internet is like a gigantic library; both have content to teach and entertain. And similar to the content in a library, not all Internet content is appropriate for children. Libraries create children's and young adults' sections in order to help youths (and their parents) identify which materials are appropriate for them. On the Internet, however, all of the content may be equally accessible; websites about ponies and websites featuring pornography are both a click away.

   NetSmartz Workshop

3. **Illegal content:** online content which is illegal under national legislation. The most common types of such content are images of sexual abuse of children, illegal activity in chat rooms (e.g. grooming), online hate and xenophobia websites.

   Salford City Council, Salford City, UK, eSafe Glossary

4. **Harmful content:** pictures, texts, documents, etc. whose content is capable of causing harm, e.g. images depicting violence are unsuitable and damaging for children and minors.

   Salford City Council, Salford City, UK, eSafe Glossary

In collaboration with

For

The Republic of Sudan